

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2017年6月22日(22.06.2017)



(10) 国際公開番号

WO 2017/104106 A1

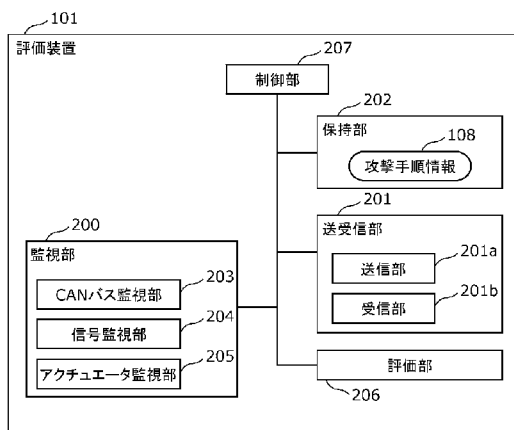
- (51) 国際特許分類:
G06F 21/57 (2013.01) B60R 16/02 (2006.01)
- (21) 国際出願番号: PCT/JP2016/004892
- (22) 国際出願日: 2016年11月16日(16.11.2016)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2015-243433 2015年12月14日(14.12.2015) JP
特願 2016-201242 2016年10月12日(12.10.2016) JP
- (71) 出願人: パナソニック インテレクチュアル
プロパティ コーポレーション オブ アメリ
カ (PANASONIC INTELLECTUAL PROPERTY
CORPORATION OF AMERICA) [US/US]; 90503 カ
リフォルニア州トーランス, スイート 20
0, マリナー アベニュー 20000 Califor
nia (US).
- (72) 発明者: 中野 稔久 (NAKANO, Toshihisa); 〒
5718501 大阪府門真市大字門真 1006 番地パ
ナソニック株式会社内 Osaka (JP). 安齋 潤 (AN
ZAI, Jun). 若林 徹 (WAKABAYASHI, Tohru). 南
公男 (MINAMI, Kimio).
- (74) 代理人: 徳田 佳昭, 外 (TOKUDA, Yoshiaki et al.);
〒5718501 大阪府門真市大字門真 1006 番地
パナソニック株式会社内 Osaka (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保
護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA,
BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN,
CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG,
ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL,
IN, IR, IS, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK,
LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,
MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH,
PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK,
SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保
護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW,
MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユー
ロパ (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨー
ロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC,
MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR),
OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM,
ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告 (条約第 21 条(3))

(54) Title: EVALUATION DEVICE, EVALUATION SYSTEM, AND EVALUATION METHOD

(54) 発明の名称: 評価装置、評価システム及び評価方法



- 101 Evaluation device
108 Hacking sequence information
200 Monitoring unit
201 Transceiver unit
201a Transmission unit
201b Receiving unit
202 Retaining unit
203 CAN bus monitoring unit
204 Signal monitoring unit
205 Actuator monitoring unit
206 Evaluation unit
207 Control unit

(57) Abstract: Provided is an evaluation device (101) which is connected to a bus which a plurality of electronic control units uses in communication in an electronic control system, and which carries out an evaluation relating to the security of the electronic control system. The evaluation device (101) comprises: a retaining unit (202) which retains hacking sequence information (108) which indicates the content of a plurality of frames and an order of transmission; a transmission unit (201a) which transmits the plurality of frames to the bus in the order of transmission which the hacking sequence information indicates; a monitoring unit (200) which monitors an actuator unit which is controlled by one of the plurality of electronic control units; and an evaluation unit (206) which carries out an evaluation on the basis of the result of the monitoring by the monitoring unit (200) when the plurality of frames is transmitted to the bus by the transmission unit (201a).

(57) 要約: 電子制御システムにおいて複数の電子制御ユニットが通信に用いるバスに接続され、電子制御システムのセキュリティに関する評価を行う評価装置 (101) は、複数のフレームの内容及び送信順序を示す攻撃手順情報 (108) を保持する保持部 (202) と、攻撃手順情報 (108) が示す送信順序で複数のフレームをバスに送信する送信部 (201a) と、複数の電子制御ユニットのいずれかにより制御されるアクチュエータ部について監視する監視部 (200) と、送信部 (201a) により複数のフレームがバスに送信される際における監視部 (200) の監視結果に基づいて評価を行う評価部 (206) とを備える。

明 細 書

発明の名称： 評価装置、評価システム及び評価方法

技術分野

[0001] 本開示は、車載ネットワークシステム等の電子制御ユニットが通信を行う電子制御システムのセキュリティ（攻撃耐性等）に関する評価を行う技術に関する。

背景技術

[0002] 近年、自動車には多数の電子制御ユニット（ECU：Electronic Control Unit）が配置され、ECUをつなぐ車載ネットワークには、例えばISO 11898-1で規定されているCAN（Controller Area Network）規格等が用いられる。車載ネットワークに対する攻撃としては、攻撃者が車内の情報端末に無線通信でアクセスし、情報端末のプログラムを不正に書き換えてその情報端末から車載ネットワークに対して任意のCANメッセージを送信し、車載ECUにつながるアクチュエータを運転者の意図に反して制御するような攻撃が知られている。自動車の運転自動化等に向けて、車載ECU自体がV2X（車車間通信（V2V：Vehicle to Vehicle）及び路車間通信（V2I：Vehicle to Infrastructure））等の無線通信の機能を搭載する状況になれば、情報端末と同様に、V2Xに対応するECUのプログラムが不正に書き換えられ、攻撃に利用され得る。攻撃対策の評価手法については、現状ではまだ研究が少ないが、例えば、非特許文献1には、単体の車載ECUにデータを送信してその応答に注目することで不具合（プログラミング間違いによるバグの混入等）を見つけるファジング手法が開示されている。

先行技術文献

非特許文献

[0003] 非特許文献1：松本勉、小林優希、土屋遊、吉田直樹、森田伸義、萱島信、「車載ECUに対するCAN経由のファジング手法」、SCIS 2015、2015年1月20日

発明の概要

[0004] 本開示の一態様に係る評価装置は、電子制御システムにおいて複数の電子制御ユニットが通信に用いるバスに接続され、当該電子制御システムのセキュリティに関する評価を行う評価装置であって、複数のフレームの内容及び送信順序を示す攻撃手順情報を保持する保持部と、前記攻撃手順情報が示す送信順序で前記複数のフレームを前記バスに送信する送信部と、前記複数の電子制御ユニットのいずれかにより制御されるアクチュエータ部について監視する監視部と、前記送信部により前記複数のフレームが前記バスに送信される際における前記監視部の監視結果に基づいて前記評価を行う評価部とを備える評価装置である。

[0005] また、本開示の一態様に係る評価システムは、バスを介して通信する複数の電子制御ユニットを備える電子制御システムのセキュリティに関する評価を行う評価システムであって、複数のフレームの内容及び送信順序を示す攻撃手順情報を保持する保持部と、前記攻撃手順情報が示す送信順序で前記複数のフレームを前記バスに送信する送信部と、前記複数の電子制御ユニットのいずれかにより制御されるアクチュエータ部について監視する監視部と、前記送信部により前記複数のフレームが前記バスに送信される際における前記監視部の監視結果に基づいて前記評価を行う評価部とを備える評価システムである。

[0006] また、本開示の一態様に係る評価方法は、バスを介して通信する複数の電子制御ユニットを備える電子制御システムのセキュリティに関する評価を行う評価方法であって、複数のフレームの内容及び送信順序を示す攻撃手順情報を保持し、前記攻撃手順情報が示す送信順序で前記複数のフレームを前記バスに送信し、前記複数のフレームが前記バスに送信される際に、前記複数の電子制御ユニットのいずれかにより制御されるアクチュエータ部について監視し、前記監視による監視結果に基づいて前記評価を行う評価方法である。

[0007] 本開示によれば、複数のECUから構成される電子制御システムの攻撃耐

性（電子制御システムに施されたセキュリティ対策技術が攻撃を適切に防御できるか否か等）について評価することが可能となる。

図面の簡単な説明

[0008] [図1]図 1 は、実施の形態 1 に係る評価システムの概略構成を示す構成図である。

[図2]図 2 は、評価システムにおける評価装置の構成図である。

[図3]図 3 は、評価対象の電子制御システムにおけるアクチュエータ ECU の構成図である。

[図4]図 4 は、評価対象の電子制御システムにおける指示 ECU の構成図である。

[図5]図 5 は、評価対象の電子制御システムにおけるセキュリティ ECU の構成図である。

[図6]図 6 は、評価対象の電子制御システムにおけるシフト位置 ECU の構成図である。

[図7]図 7 は、評価装置の保持部が保持する攻撃手順情報の一例を示す図である。

[図8]図 8 は、評価システムの動作例 1 を示すシーケンス図である。

[図9]図 9 は、評価システムの動作例 1 を示すシーケンス図である。

[図10]図 10 は、評価システムの動作例 1 を示すシーケンス図である。

[図11]図 11 は、評価システムの動作例 2 を示すシーケンス図である。

[図12]図 12 は、評価システムの動作例 2 を示すシーケンス図である。

[図13]図 13 は、評価システムの動作例 3 を示すシーケンス図である。

[図14]図 14 は、評価システムの動作例 3 を示すシーケンス図である。

[図15]図 15 は、評価システムの動作例 3 を示すシーケンス図である。

[図16]図 16 は、評価システムの動作例 4 を示すシーケンス図である。

[図17]図 17 は、評価システムの動作例 4 を示すシーケンス図である。

発明を実施するための形態

[0009] （本発明の基礎となった知見）

非特許文献１の手法は、単体の車載ＥＣＵの不具合を見つけることはできても、車載ネットワークを形成する複数のＥＣＵで構成されるシステム（電子制御システム）を評価対象としてセキュリティ（評価対象に施されたセキュリティ対策技術が攻撃を適切に防御できるか否かという攻撃耐性等）に関する評価を行えるものではない。

[0010] そこで、本開示は、複数のＥＣＵから構成される電子制御システムを評価対象としてセキュリティに関する評価を行い得る評価装置を提供する。また、本開示は、複数のＥＣＵから構成される電子制御システムのセキュリティに関する評価を行い得る評価システム及びその評価のための評価方法を提供する。

[0011] 本開示の一態様に係る評価装置は、電子制御システムにおいて複数の電子制御ユニットが通信に用いるバスに接続され、当該電子制御システムのセキュリティに関する評価を行う評価装置であって、複数のフレームの内容及び送信順序を示す攻撃手順情報を保持する保持部と、前記攻撃手順情報が示す送信順序で前記複数のフレームを前記バスに送信する送信部と、前記複数の電子制御ユニットのいずれかにより制御されるアクチュエータ部について監視する監視部と、前記送信部により前記複数のフレームが前記バスに送信される際における前記監視部の監視結果に基づいて前記評価を行う評価部とを備える評価装置である。監視部は、送信部により複数のフレーム（例えばＣＡＮメッセージ）がバスに送信される際に（例えば、送信直後に、或いは、送信直前から送信直後に亘り）、アクチュエータ部について直接又は間接的に監視し得る。これにより、複数の電子制御ユニット（ＥＣＵ）から構成される電子制御システムを評価対象として、アクチュエータ部の駆動に係る攻撃への防御機能等といったセキュリティ機能の評価を行い得る。

[0012] また、例えば、前記複数の電子制御ユニットは、ＣＡＮ（Controller Area Network）プロトコルに従って前記バスを介して通信を行うこととしても良い。これにより、ＥＣＵ間でフレームの授受を行うためのＣＡＮに従うネットワークにおける攻撃耐性等の評価が可能となり得る。

- [0013] また、例えば、前記監視部は、前記アクチュエータ部についての前記監視として、前記複数の電子制御ユニットのうちの1つに前記アクチュエータ部を制御させるよう指示するための制御指示フレームが前記バスに送信されたことを検出し、前記評価部は、前記送信部により前記複数のフレームの1つ以上が前記バスに送信された後の一定期間内に、前記制御指示フレームが前記バス上で送信されたことが前記監視部により検出されたか否かに応じて評価結果が相違するように前記評価を行うこととしても良い。制御指示フレームは例えば電子制御システムで規定されたフレームのIDにより識別可能である。これにより、アクチュエータ部を制御するためのフレームがバスで授受される場合においてバスの監視により適切に電子制御システムを評価し得る。
- [0014] また、例えば、前記監視部は、前記アクチュエータ部についての前記監視として、前記複数の電子制御ユニットのうちの1つから前記アクチュエータ部に制御信号が入力されたことを検出し、前記評価部は、前記送信部により前記複数のフレームの1つ以上が前記バスに送信された後の一定期間内に、前記アクチュエータ部に前記制御信号が入力されたことが前記監視部により検出されたか否かに応じて評価結果が相違するように前記評価を行うこととしても良い。アクチュエータ部を制御するための制御信号は電子制御システムで規定されている。これにより、攻撃によってアクチュエータ部への制御信号が伝達されたか否かが確認できるので適切な評価が可能となり得る。
- [0015] また、例えば、前記監視部は、前記アクチュエータ部についての前記監視として、前記アクチュエータ部の動作を検出し、前記評価部は、前記送信部により前記複数のフレームの1つ以上が前記バスに送信された後の一定期間内に、前記アクチュエータ部が動作したことが前記監視部により検出されたか否かに応じて評価結果が相違するように前記評価を行うこととしても良い。これにより、攻撃によってアクチュエータ部が動作したか否かが確認できるので適切な評価が可能となり得る。
- [0016] また、例えば、前記アクチュエータ部は、アクチュエータを有し、前記監

視部は、前記アクチュエータ部の動作を、前記アクチュエータの動作で変化
する物理量の測定によって検出することとしても良い。これにより、攻撃に
よって実際にアクチュエータが動作したか否かが確認できるので適切な評価
が可能となり得る。

[0017] また、例えば、前記アクチュエータ部は、アクチュエータの動作を模擬す
るプログラムを実行するコンピュータを有し、前記監視部は、前記アクチュ
エータ部の動作を、前記コンピュータにおいて前記プログラムに関わる所定
データの変化を観測することによって検出することとしても良い。これによ
り、実際のアクチュエータを代替する模擬アクチュエータを用いる場合にお
いて攻撃耐性等の評価が可能となり得る。

[0018] また、例えば、前記攻撃手順情報は更に前記複数のフレームについての送
信間隔を示し、前記送信部は、前記攻撃手順情報が示す送信順序及び送信間
隔に従って前記複数のフレームを前記バスに送信することとしても良い。こ
れにより、複数のフレームの送信順序と送信間隔とで定まる攻撃方法に対す
る防御機能等の評価が可能となり得る。

[0019] また、例えば、前記評価部は、評価結果として前記電子制御システムに攻
撃耐性があるか否かを示す情報を出力することとしても良い。これにより、
評価装置の利用者等は、電子制御システムに攻撃耐性があるか否かを知り得
る。

[0020] また、例えば、前記送信部は、前記攻撃手順情報が示す送信順序で前記複
数のフレームを前記バスに送信する攻撃パターンを複数回繰り返し、前記評
価部は、前記攻撃パターンの繰り返しによる前記監視結果の変化の有無に応
じて評価結果が相違するように前記評価を行うこととしても良い。これによ
り、攻撃パターンの繰り返しに対する電子制御システムの攻撃耐性等につい
ての評価が可能となり得る。

[0021] また、本開示の一態様に係る評価システムは、バスを介して通信する複数
の電子制御ユニットを備える電子制御システムのセキュリティに関する評価
を行う評価システムであって、複数のフレームの内容及び送信順序を示す攻

撃手順情報を保持する保持部と、前記攻撃手順情報が示す送信順序で前記複数のフレームを前記バスに送信する送信部と、前記複数の電子制御ユニットのいずれかにより制御されるアクチュエータ部について監視する監視部と、前記送信部により前記複数のフレームが前記バスに送信される際における前記監視部の監視結果に基づいて前記評価を行う評価部とを備える評価システムである。これにより、複数のECUから構成される電子制御システムにおけるアクチュエータ部の駆動に係る攻撃への防御機能等といったセキュリティ機能の評価を行い得る。

[0022] また、本開示の一態様に係る評価方法は、バスを介して通信する複数の電子制御ユニットを備える電子制御システムのセキュリティに関する評価を行う評価方法であって、複数のフレームの内容及び送信順序を示す攻撃手順情報を保持し、前記攻撃手順情報が示す送信順序で前記複数のフレームを前記バスに送信し、前記複数のフレームが前記バスに送信される際に、前記複数の電子制御ユニットのいずれかにより制御されるアクチュエータ部について監視し、前記監視による監視結果に基づいて前記評価を行う評価方法である。これにより、複数のECUから構成される電子制御システムを評価対象として、アクチュエータ部の駆動に係る攻撃への防御機能等といったセキュリティ機能の評価を行い得る。

[0023] また、例えば、前記複数の電子制御ユニットは、CAN (Controller Area Network) プロトコルに従って前記バスを介して通信を行い、前記評価方法は、前記複数のフレームの1つ以上が前記バスに送信された後の一定期間内に、前記複数の電子制御ユニットのうちの1つに前記アクチュエータ部を制御させるよう指示するための制御指示フレームが前記バスに送信されたことを検出したか否かに応じて、評価結果が相違するように前記評価を行うこととしても良い。これにより、CANに従う車載ネットワークシステム等の電子制御システムについて攻撃耐性等の評価が可能となり得る。

[0024] なお、これらの全般的又は具体的な態様は、システム、方法、集積回路、コンピュータプログラム又はコンピュータで読み取り可能なCD-ROM等

の記録媒体で実現されても良く、システム、方法、集積回路、コンピュータプログラム又は記録媒体の任意な組み合わせで実現されても良い。

[0025] 以下、実施の形態に係る評価システムについて、図面を参照しながら説明する。ここで示す実施の形態は、いずれも本開示の一具体例を示すものである。従って、以下の実施の形態で示される数値、構成要素、構成要素の配置及び接続形態、並びに、ステップ（工程）及びステップの順序等は、一例であって本開示を限定するものではない。以下の実施の形態における構成要素のうち、独立請求項に記載されていない構成要素については、任意に付加可能な構成要素である。また、各図は、模式図であり、必ずしも厳密に図示されたものではない。

[0026] （実施の形態１）

以下、自動車（車両）に搭載され、バスを介して通信する複数の電子制御ユニット（ＥＣＵ）を含んで構成される車載ネットワークシステム（電子制御システム）のセキュリティに関する評価を行う評価装置及び評価方法、並びに、電子制御システムと評価装置とを含む評価システムについて説明する。

[0027] [１．１ 評価システム１０の構成]

図１は、評価システム１０の概略構成を示す構成図である。評価システム１０は、同図に示すように、評価装置１０１と、電子制御システム１１とを含んで構成される。評価システム１０は、電子制御システム１１を評価対象として、電子制御システム１１の攻撃耐性（攻撃に対して防御を行うセキュリティ対策技術が適切に作用しているか否か等）について評価を行う。

[0028] 電子制御システム１１は、車載ネットワークシステムであり、車両内の制御装置、センサ、アクチュエータ（例えば電子制御可能にされたステアリング、アクセル、ブレーキ等）、ユーザインタフェース装置等の各種機器に接続されて、車内のバス（ＣＡＮバス）を介してフレームの送受信を行う複数の電子制御ユニット（ＥＣＵ）を含んで構成される車載ネットワークを備える。電子制御システム１１では、各ＥＣＵがフレームを授受して連携するこ

とで、例えば、先進運転者支援システム（A D A S : Advanced Driver Assistance System）の一機能である駐車支援機能、車線維持支援機能、衝突回避支援機能等の機能を実現する。

[0029] 車内には多数のセンサ、アクチュエータ、E C U等が含まれ得るが、ここでは説明の便宜上、一例として、電子制御システム11は、図1に示すように、アクチュエータE C U 102、指示E C U 103、セキュリティE C U 104、シフト位置E C U 105、車速E C U 106、及び、アクチュエータ107を備えるものとして説明する。ここでは、アクチュエータ107は、ステアリング、アクセル、ブレーキ等を代表して表したものであり、アクチュエータE C U 102も、ステアリング、アクセル、ブレーキ等の1つ又は複数を制御するE C Uを代表して表したものである。なお、各E C Uは、C A Nバス20を通信路としてC A N規格（プロトコル）に従って通信を行う。C A Nにおいてデータの伝送に用いられるフレームであるデータフレーム（C A Nメッセージとも称する）は、I D（メッセージI D）を格納するI Dフィールド、データを格納するデータフィールド等を含むように規定されている。

[0030] アクチュエータE C U 102は、アクチュエータ107（例えば、ステアリング、アクセル、ブレーキ等）と信号線で接続されると共に、C A Nバス20とも接続され、C A Nバス20を介して受信したC A Nメッセージに基づいてアクチュエータ107を制御する。

[0031] 指示E C U 103は、C A Nバス20に接続され、車両の状態等を示すC A Nメッセージを取得し、一定条件下でアクチュエータ107を制御させるための指示（例えばステアリング操作指示）を、C A NメッセージとしてアクチュエータE C U 102へ送信する。

[0032] セキュリティE C U 104は、C A Nバス20を常時監視（モニタリング）し、例えば不正なC A Nメッセージ（攻撃用のC A Nメッセージ）が流れていることを検知した場合に、そのC A Nメッセージを無効化する等の対処を行う。C A Nメッセージの無効化の方法としては、任意の方法を用いるこ

とができるが、例えば不正なCANメッセージに重畳させるように、CANプロトコルで規定されたエラーフレームを送信することで無効化し得る。

[0033] シフト位置ECU105及び車速ECU106は、これらを搭載する車両の状態を取得し、CANメッセージとしてCANバス20に送信する。シフト位置ECU105は、車両のシフトレバーのシフト位置に対応する変速ギアの状態（パーキング：P、リバース：R、ドライブ：D等）を示すCANメッセージを送信し、車速ECU106は、車速（車両の速度）を示すCANメッセージを送信する。

[0034] 評価装置101は、電子制御システム11（評価対象）に対して施されたセキュリティ対策技術の攻撃耐性を評価する装置である。評価装置101は、保持する攻撃手順情報108に基づいて、評価対象に対して攻撃（ハッキング）を仕掛け、攻撃への反応を観測するための監視（モニタリング）を行い、監視結果に応じた評価を行う。評価装置101による評価の一例としては、例えば、その攻撃に対する耐性の有無（攻撃或いは防御の成否）の判定が挙げられる。評価装置101は、監視として具体的には、CANバス20を流れるフレーム（メッセージ）の監視、アクチュエータ107への入力信号（つまりアクチュエータECU102の出力信号）の監視、及び、アクチュエータ107の挙動（動作）そのものの監視を行う。攻撃手順情報108は、攻撃を仕掛ける際の手順（送信すべきCANメッセージの種類、順序、タイミング、頻度等）を示す。

[0035] 以下、評価システム10の各構成要素について詳細に説明する。

[0036] [1. 2 評価装置101の構成]

図2は、評価システム10における評価装置101の構成図である。

[0037] 評価装置101は、図2に示すように、監視部200（CANバス監視部203、信号監視部204及びアクチュエータ監視部205）と、送受信部201（送信部201a及び受信部201b）と、保持部202と、評価部206と、制御部207とを含んで構成される。

[0038] 評価装置101は、例えば、プロセッサ（マイクロプロセッサ）、メモリ

等のデジタル回路、アナログ回路、通信回路、ハードディスク等を含む装置である。メモリは、ROM、RAM等であり、プロセッサにより実行される制御プログラム（ソフトウェアとしてのコンピュータプログラム）を記憶することができる。例えばプロセッサが、制御プログラム（コンピュータプログラム）に従って動作（各種回路の制御等）することにより、評価装置101は各種機能を実現することになる。なお、コンピュータプログラムは、所定の機能を達成するために、プロセッサに対する指令を示す命令コードが複数個組み合わせられて構成されたものである。

[0039] (1) 送受信部201

送受信部201は、通信回路等により実現される。送受信部201は、送信部201a及び受信部201bで構成される。送信部201aは、CANバス20に対してCANメッセージ（例えば、シフト位置、車速、或いは、ステアリング操作指示を示すデータフレーム等）を送信する。受信部201bは、CANバス20を流れるCANメッセージ（例えば指示ECU103が送信するステアリング操作指示を示すデータフレーム等）を受信する。

[0040] (2) 保持部202

保持部202は、メモリ、ハードディスク等の記憶媒体で実現され、評価装置101が評価対象の攻撃耐性等を評価するために仕掛ける攻撃の手順を示す攻撃手順情報108を記憶している。攻撃手順情報108は攻撃用の複数のフレーム（CANメッセージ）の送信順序等を示す。攻撃手順情報108の詳細については後に図7を用いて説明する。

[0041] (3) CANバス監視部203

CANバス監視部203は、例えばプログラムを実行するプロセッサ等により実現され、評価対象の電子制御システム11で複数のECUが接続されているCANバス20を監視する。CANバス監視部203は、具体的には受信部201bを介してCANメッセージを受信して、CANメッセージに含まれるデータの中身（ペイロード）を確認する。例えば、CANバス監視部203は、アクチュエータ107についての監視として、CANバス20

に接続された指示ECU103にアクチュエータ107を制御させるよう指示するための制御指示フレームがCANバス20に送信されたことを検出する。そしてCANバス監視部203は、例えば指示ECU103が送信する制御指示フレーム（ステアリング操作指示に関するデータフレーム）のデータフィールドの内容（駐車支援機能の有効／無効フラグ、ステアリング操舵角の指定等）を確認する。

[0042] (4) 信号監視部204

信号監視部204は、アクチュエータECU102がアクチュエータ107に対して信号線により送信した信号（アクチュエータ107への入力信号）を観測し、信号内容を確認する。信号監視部204は、例えば、アクチュエータECU102かアクチュエータ107かその間の信号線かに接続する通信回路、プログラムを実行するプロセッサ等により実現される。

[0043] (5) アクチュエータ監視部205

アクチュエータ監視部205は、アクチュエータ107を観測し、アクチュエータ107の挙動（動作）を確認する。アクチュエータ107の動作の確認は、アクチュエータ107がステアリングであれば回転量、アクセル或いはブレーキであれば変位量等の状態、変化の有無等の確認である。アクチュエータ監視部205は、例えば、アクチュエータ107が生じる物理現象（アクチュエータ107の動作で変化する物理量）を直接的又は間接的に測定するセンサ、プログラムを実行するプロセッサ等で実現される。

[0044] (6) 評価部206

評価部206は、プログラムを実行するプロセッサ等により実現される。評価部206は、監視部200（CANバス監視部203、信号監視部204及びアクチュエータ監視部205）での監視による確認結果に基づいて、電子制御システム11のセキュリティに関する評価を行う。具体的には、評価部206は、監視部200による確認結果の全部又は一部と、攻撃手順情報108に基づいてCANメッセージを送信するときの期待値とを比較し、攻撃が成功しているか否か（例えば攻撃に対する防御機能が適切に作動した

か否か)等を判定する。期待値は、攻撃結果として期待されるアクチュエータの挙動、攻撃結果として期待される、アクチュエータ107へ入力される制御信号、攻撃結果として指示ECU103が送信すると期待されるCANメッセージ(例えば制御指示フレーム)等であり、予め規定され得る。評価部206は、送信部201aにより攻撃手順情報108に基づく攻撃用のCANメッセージがCANバス20に送信される際(例えば送信直後の一定期間、或いは送信直前から送信直後まで等)における監視部200の監視結果に基づいて評価を行う。評価部206は、例えば、送信部201aにより攻撃手順情報108に示される攻撃用の複数のフレーム(CANメッセージ)の1つ以上がCANバス20に送信された後の一定期間内に、制御指示フレームがCANバス20上で送信されたことがCANバス監視部203により検出されたか否かを判定し、制御指示フレームが検出されたか否かに応じて評価結果が相違するように評価を行い得る。また評価部206は、例えば、攻撃用のCANメッセージの1つ以上がCANバス20に送信された後の一定期間内に、アクチュエータ107に、制御のための制御信号が入力されたことが信号監視部204により検出されたか否かに応じて評価結果が相違するように評価を行い得る。また、評価部206は、例えば、攻撃用のCANメッセージの1つ以上がCANバス20に送信された後の一定期間内に、アクチュエータ107が動作したことがアクチュエータ監視部205により検出されたか否かに応じて評価結果が相違するように評価を行い得る。

[0045] (7) 制御部207

制御部207は、プログラムを実行するプロセッサ等により実現され、監視部200、送受信部201、保持部202、及び、評価部206を管理、制御して評価装置101の機能を実現する。

[0046] [1. 3 アクチュエータECU102の構成]

図3は、アクチュエータECU102の構成図である。

[0047] アクチュエータECU102は、図3に示すように、送受信部301と、指示送信部302と、状態取得部303と、判定部304と、制御部305

とを含んで構成される。

[0048] アクチュエータ ECU 102 は、CAN バス 20 に接続された ECU である。ECU は、例えば、プロセッサ、メモリ等のデジタル回路、アナログ回路、通信回路等を含む装置である。メモリは、ROM、RAM 等であり、プロセッサにより実行される制御プログラムを記憶することができる。例えばプロセッサが、制御プログラム（コンピュータプログラム）に従って動作（各種回路の制御等）することにより、アクチュエータ ECU 102 は機能を果たす。

[0049] （１）送受信部 301

送受信部 301 は、CAN バス 20 に対して CAN メッセージを送信し、CAN バス 20 を流れる CAN メッセージを受信する。送受信部 301 は、例えば、シフト位置、車速、或いは、ステアリング操作指示を示す CAN メッセージを受信する。

[0050] （２）指示送信部 302

指示送信部 302 は、送受信部 301 を介して受信した CAN メッセージに基づき、アクチュエータ 107 に対して信号線で制御信号を送信する。制御信号は、例えば、ステアリングに対しては、回転角度等を示して回転等を指示する信号（ステアリング動作指示）であり、アクセル或いはブレーキに対しては、変位量（例えば踏み込み量）等を示して作動等を指示する信号である。

[0051] （３）状態取得部 303

状態取得部 303 は、アクチュエータ 107 と接続する信号線を介してアクチュエータ 107 の状態を取得する。状態取得部 303 が取得する状態は、例えば、アクチュエータ 107 がステアリングであれば回転角度、アクセル或いはブレーキであれば変位量（例えば踏み込み量）等である。

[0052] （４）判定部 304

判定部 304 は、送受信部 301 を介して受信した CAN メッセージに基づき、アクチュエータ 107 へ制御信号を送信するか否かを判定する。例え

ば、アクチュエータ１０７としてのステアリングへ指示する制御信号を出す場合には、判定部３０４は、送受信部３０１を介して受信したシフト位置、車速、ステアリング操作指示等の情報に基づいて、制御信号を出すか否かを判定し、制御信号で指定する制御量（回転角度等）を決定する。

[0053] （５）制御部３０５

制御部３０５は、送受信部３０１、指示送信部３０２、状態取得部３０３、及び、判定部３０４を管理、制御してアクチュエータＥＣＵ１０２の機能を実現する。

[0054] [１．４ 指示ＥＣＵ１０３の構成]

図４は、指示ＥＣＵ１０３の構成図である。

[0055] 指示ＥＣＵ１０３は、図４に示すように、送受信部４０１と、判定部４０２と、算出部４０３と、制御部４０４とを含んで構成される。

[0056] 指示ＥＣＵ１０３は、ＣＡＮバス２０に接続されたＥＣＵである。指示ＥＣＵ１０３のプロセッサが、メモリに記憶された制御プログラム（コンピュータプログラム）に従って動作することにより、指示ＥＣＵ１０３は機能を果たす。

[0057] （１）送受信部４０１

送受信部４０１は、ＣＡＮバス２０に対してＣＡＮメッセージを送信し、ＣＡＮバス２０を流れるＣＡＮメッセージを受信する。送受信部４０１は、例えば、ステアリング操作指示を示すＣＡＮメッセージを送信し、シフト位置或いは車速を示すＣＡＮメッセージを受信する。

[0058] （２）判定部４０２

判定部４０２は、送受信部４０１を介して受信したＣＡＮメッセージに基づき、アクチュエータＥＣＵ１０２へ制御指示（例えばステアリング操作指示を示す制御指示フレームであるＣＡＮメッセージ）を出すか否かを判定する。例えば、ステアリングを制御させるためにアクチュエータＥＣＵ１０２へ制御指示を出す場合、送受信部４０１を介して受信したＣＡＮメッセージが示すシフト位置、車速、或いは、駐車支援機能の開始に関する情報等から

、制御指示を出すか否かを判定する。ここでは、電子制御システム 11 において駐車支援機能の開始に関する情報を示す CAN メッセージは、例えば、CAN バス 20 に接続された、ユーザインタフェースを備える ECU（不図示）から送信されること等を想定している。その ECU は例えば車両の運転者の操作に応じて駐車支援機能の開始に関する情報を示す CAN メッセージを送信し得る。

[0059] (3) 算出部 403

算出部 403 は、送受信部 401 を介して受信した CAN メッセージに基づき、制御指示で指示すべき制御量（例えばステアリングの回転角度等）を算出する。

[0060] (4) 制御部 404

制御部 404 は、送受信部 401、判定部 402、及び、算出部 403 を管理、制御して指示 ECU 103 の機能を実現する。

[0061] [1. 5 セキュリティ ECU 104 の構成]

図 5 は、セキュリティ ECU 104 の構成図である。

[0062] セキュリティ ECU 104 は、図 5 に示すように、送受信部 501 と、CAN バス監視部 502 と、制御部 503 とを含んで構成される。

[0063] セキュリティ ECU 104 は、CAN バス 20 に接続され、攻撃に対処するセキュリティ機能（防御機能等）を備えた ECU である。セキュリティ ECU 104 のプロセッサが、メモリに記憶された制御プログラム（コンピュータプログラム）に従って動作することにより、セキュリティ ECU 104 は機能を果たす。

[0064] (1) 送受信部 501

送受信部 501 は、CAN バス 20 を流れる CAN メッセージを受信し、CAN バス監視部 502 の指示を受けて CAN バス 20 に、不正な CAN メッセージを無効化するためにエラーフレームを送信する。送受信部 501 は、例えば、シフト位置、車速、或いは、ステアリング操作指示を示す CAN メッセージを受信する。

[0065] (2) CANバス監視部502

CANバス監視部502は、複数のECUが接続されているCANバス20から送受信部501を介して受信したCANメッセージに含まれるデータの中身（ペイロード）を確認する。CANバス監視部502は、不正なCANメッセージ（つまり電子制御システム11において予め定められたルールに準拠していないCANメッセージ）が流れていることを確認した場合に、送受信部501を介してエラーフレームを送信する。

[0066] (3) 制御部503

制御部503は、送受信部501及びCANバス監視部502を管理、制御してセキュリティECU104の機能を実現する。

[0067] [1. 6 シフト位置ECU105、車速ECU106の構成]

図6は、シフト位置ECU105の構成図である。

[0068] シフト位置ECU105は、図6に示すように、送受信部601と、状態取得部602と、制御部603とを含んで構成される。車速ECU106も、シフト位置ECU105と同様の構成を備える。

[0069] シフト位置ECU105及び車速ECU106のそれぞれは、CANバス20に接続されたECUである。それぞれのECUのプロセッサが、メモリに記憶された制御プログラム（コンピュータプログラム）に従って動作することにより、それぞれのECUは機能を果たす。

[0070] (1) 送受信部601

送受信部601は、CANバス20に対してCANメッセージを送信し、CANバス20を流れるCANメッセージを受信する。

[0071] (2) 状態取得部602

状態取得部602は、センサ等から車両の状態を取得し、送受信部601を介してその取得した状態を示すCANメッセージを送信する。シフト位置ECU105における状態取得部602は、シフト位置を取得し、車速ECU106における状態取得部602は、車速を取得する。

[0072] (3) 制御部603

制御部 603 は、送受信部 601 及び状態取得部 602 を管理、制御して、シフト位置 ECU 105 或いは車速 ECU 106 の機能を実現する。

[0073] [1. 7 攻撃手順情報]

評価装置 101 の保持部 202 に保持される攻撃手順情報 108 の一例を図 7 に示す。図 7 の例では、攻撃手順情報 108 は、評価対象機能（攻撃対象とする電子制御システム 11 の機能）、攻撃のために送信すべき CAN メッセージ、その CAN メッセージのメッセージ ID、その CAN メッセージにおけるデータ内容（即ち他の ECU へ通知又は指示する内容）、その CAN メッセージの送信間隔、及び、送信順序を示す。

[0074] 図 7 の例の攻撃手順情報 108 は、駐車支援機能を攻撃対象とする場合については、ID（メッセージ ID）が 0x0123 である、シフト位置を通知する CAN メッセージにより、シフト位置が「リバース」であることを通知し、その後、ID が 0x0034 である、車速を通知する CAN メッセージにより、車速が「6 km/h」であること通知し、最後に、ID が 0x0256 である、ステアリング操作指示を示す CAN メッセージにより、ステアリングを右に 15 度回転させるためのフラグ「1」及びステアリング操舵角の指定「右旋回 15 度」のデータを送信すべきことを示す。このフラグは、駐車支援機能が有効か無効かを示す有効／無効フラグであり、「1」が有効であることを示し、「0」が有効でない（無効である）ことを示す。なお、図 7 の例は、一例に過ぎず、攻撃手順情報 108 の内容は、任意に定め得る。送信部 201a は、攻撃手順情報 108 が示す送信順序で複数の CAN メッセージを CAN バス 20 に送信することになる。また、攻撃手順情報 108 は、複数の CAN メッセージ間の送信間隔を規定したものであっても良く、この場合には、送信部 201a は、攻撃手順情報 108 が示す送信順序及び送信間隔に従って複数の CAN メッセージを CAN バス 20 に送信することになる。

[0075] なお、電子制御システム 11 では CAN バス 20 においてシフト位置、車速、或いは、ステアリング操作指示（駐車支援機能の有効／無効の状態）に

関するCANメッセージは、常に周期的に送信されている。ステアリングの操作が必要ない場合（駐車支援機能が働いていない場合）には、フラグが「0」の状態ステアリング操作指示（駐車支援機能の有効／無効の状態）に関するCANメッセージが周期的に送信され、ステアリングの操作が必要な場合（駐車支援機能を働かせる場合）には、フラグが「1」の状態に変えられたそのCANメッセージ（つまりステアリング操作指示を示すCANメッセージ）が周期的に送信される。

[0076] [1. 8 評価システム10の動作]

以下、上述した構成を備える評価システム10において、評価装置101により評価対象の電子制御システム11を、攻撃手順情報108に従って攻撃（CANメッセージの送信により攻撃）することで評価する動作について説明する。まず、セキュリティECU104を除去した状態（セキュリティECU104の導入前等）の電子制御システム11を評価対象として評価する動作例1及び動作例2を説明し、その後に、セキュリティECU104を有する状態（セキュリティECU104の導入後等）の電子制御システム11を評価対象として評価する動作例3及び動作例4を説明する。

[0077] [1. 8. 1 評価システム10の動作例1]

図8～図10は、セキュリティECU104を備えない状態の電子制御システム11を評価する評価システム10の動作（動作例1）を示すシーケンス図である。図8に示すシーケンス図は、図9に示すシーケンス図へ続く。図9に示すシーケンス図は、図10に示すシーケンス図へ続く。動作例1では、評価装置101が、攻撃によりアクチュエータECU102を誤認識させる例を示す。電子制御システム11ではシフト位置、車速、及び、ステアリング操作指示に関する各CANメッセージが、シフト位置ECU105、車速ECU106、或いは、指示ECU103により周期的に送信されている。

[0078] シフト位置ECU105は、現在のシフト位置（ドライブ：D）を示すCANメッセージをCANバス20へ送信し（ステップS801）、アクチュ

エータECU102は、CANバス20を流れているそのシフト位置を示すCANメッセージを受信する（ステップS802）。

[0079] 評価装置101は、例えばアクチュエータECU102におけるCANメッセージの定期処理用のバッファを上書きさせること等を狙って、CANバス20にシフト位置（ドライブ：D）を示すCANメッセージが流れた直後に、攻撃手順情報108に従って現在のシフト位置を詐称する偽のシフト位置（リバース：R）を示すCANメッセージをCANバス20へ送信する（ステップS803）。これにより、アクチュエータECU102は、CANバス20を流れているシフト位置を示すCANメッセージを受信して、現在のシフト位置がリバース：Rであると誤認識する（ステップS804）。

[0080] また、車速ECU106は、現在の車速（30km/h）を示すCANメッセージをCANバス20へ送信し（ステップS805）、アクチュエータECU102は、CANバス20を流れているその車速を示すCANメッセージを受信する（ステップS806）。

[0081] 評価装置101は、CANバス20に車速（30km/h）を示すCANメッセージが流れた直後に、現在の車速を詐称する偽の車速（0km/h）を示すCANメッセージをCANバス20へ送信する（ステップS807）。これにより、アクチュエータECU102は、CANバス20を流れている車速を示すCANメッセージを受信して、現在の車速が0km/hであると誤認識する（ステップS808）。

[0082] 指示ECU103は、現在、駐車支援機能が有効でないこと（フラグ：0）を示すCANメッセージをCANバス20へ送信し（ステップS901）、アクチュエータECU102は、CANバス20を流れている駐車支援機能の有効／無効の状態に関するCANメッセージを受信する（ステップS902）。

[0083] 評価装置101は、CANバス20に駐車支援機能が有効でないこと（フラグ：0）を示すCANメッセージが流れた直後に、現在、駐車支援機能が有効であること（フラグ：1）を示すCANメッセージをCANバス20へ

送信する（ステップS903）。これにより、アクチュエータECU102は、CANバス20を流れているその駐車支援機能の有効／無効の状態に関するCANメッセージを受信して、現在、駐車支援機能が有効であると誤認識し（ステップS904）、駐車支援機能の有効／無効の状態に関するCANメッセージ（つまり駐車支援機能が有効であるのでステアリング操作指示を示すCANメッセージ）に含まれるステアリングの操舵角の指定に基づきステアリングを動作させるための制御信号（ステアリング動作指示）を送信する（ステップS905）。そして、アクチュエータ107としてのステアリングは、受信した制御信号（ステアリング動作指示）に基づいて動作する（ステップS906）。以後の説明において、アクチュエータ107としてのステアリングをアクチュエータ107（ステアリング）と称する。

[0084] 評価装置101は、アクチュエータECU102がアクチュエータ107（ステアリング）へ送信した制御信号（ステアリング動作指示）を受信（監視）する（ステップS1001）。また、評価装置101は、アクチュエータ107（ステアリング）の挙動を確認（観測）する（ステップS1002）。評価装置101は、受信した制御信号、及び、確認したアクチュエータ107（ステアリング）の挙動を、攻撃の期待値と比較することにより、電子制御システム11のセキュリティの評価（攻撃の成否についての判定等）を行う（ステップS1003）。評価装置101は、例えば、受信した制御信号、及び、確認したアクチュエータ107（ステアリング）の挙動が、攻撃の期待値としての制御信号及び挙動となっている場合に攻撃が成功していると判定する。なお、評価装置101は、アクチュエータ107（ステアリング）へ入力される制御信号の監視結果と、アクチュエータ107（ステアリング）の挙動の確認結果とのうち一方のみを用いて攻撃の期待値に基づいて攻撃の成否についての判定等を行っても良い。

[0085] 評価装置101が、攻撃手順情報108に従った攻撃が成功していることを確認することで、例えば、その後に電子制御システム11に導入するセキュリティ対策技術（例えば、セキュリティECU104）の効果について評

価できるようになる。

[0086] [1 . 8 . 2 評価システム 1 0 の動作例 2]

図 1 1 及び図 1 2 は、セキュリティ ECU 1 0 4 を備えない状態の電子制御システム 1 1 を評価する評価システム 1 0 の動作（動作例 2）を示すシーケンス図である。図 1 1 に示すシーケンス図は、図 1 2 に示すシーケンス図へ続く。動作例 2 では、評価装置 1 0 1 が、攻撃により指示 ECU 1 0 3 を誤認識させる例を示す。

[0087] シフト位置 ECU 1 0 5 は、現在のシフト位置（ドライブ：D）を示す CAN メッセージを CAN バス 2 0 へ送信し（ステップ S 1 1 0 1）、指示 ECU 1 0 3 は、CAN バス 2 0 を流れているそのシフト位置を示す CAN メッセージを受信する（ステップ S 1 1 0 2）。アクチュエータ ECU 1 0 2 も、同様に CAN バス 2 0 を流れているそのシフト位置を示す CAN メッセージを受信する（ステップ S 1 1 0 3）。

[0088] 評価装置 1 0 1 は、CAN バス 2 0 にシフト位置（ドライブ：D）を示す CAN メッセージが流れた直後に、攻撃手順情報 1 0 8 に従って現在のシフト位置を詐称する偽のシフト位置（リバース：R）を示す CAN メッセージを CAN バス 2 0 へ送信する（ステップ S 1 1 0 4）。これにより、指示 ECU 1 0 3 は、CAN バス 2 0 を流れているシフト位置を示す CAN メッセージを受信して、現在のシフト位置がリバース：R であると誤認識する（ステップ S 1 1 0 5）。アクチュエータ ECU 1 0 2 も、同様に CAN バス 2 0 を流れているそのシフト位置を示す CAN メッセージを受信して、現在のシフト位置がリバース：R であると誤認識する（ステップ S 1 1 0 6）。

[0089] また、車速 ECU 1 0 6 は、現在の車速（30 km/h）を示す CAN メッセージを CAN バス 2 0 へ送信し（ステップ S 1 1 0 7）、指示 ECU 1 0 3 は、CAN バス 2 0 を流れているその車速を示す CAN メッセージを受信する（ステップ S 1 1 0 8）。アクチュエータ ECU 1 0 2 も、同様に CAN バス 2 0 を流れているその車速を示す CAN メッセージを受信する（ステップ S 1 1 0 9）。

- [0090] 評価装置101は、CANバス20に車速(30km/h)を示すCANメッセージが流れた直後に、現在の車速を詐称する偽の車速(0km/h)を示すCANメッセージをCANバス20へ送信する(ステップS1110)。これにより、指示ECU103は、CANバス20を流れている車速を示すCANメッセージを受信して、現在の車速が0km/hであると誤認識する(ステップS1111)。アクチュエータECU102も、同様にCANバス20を流れているその車速を示すCANメッセージを受信して、現在の車速が0km/hであると誤認識する(ステップS1112)。
- [0091] 評価装置101は、駐車支援機能を開始することを示すCANメッセージをCANバス20へ送信し(ステップS1201)、指示ECU103は、CANバス20を流れているその駐車支援機能の開始に関するCANメッセージ(駐車支援機能を開始することを示すCANメッセージ)を受信する(ステップS1202)。
- [0092] 続いて指示ECU103は、既に受信した偽のシフト位置及び車速が駐車支援機能を実行するための一定条件を満たすことから、駐車支援機能が有効であること(フラグ:1)を示すCANメッセージ(つまりステアリング操作指示を示すCANメッセージ)をCANバス20へ送信する(ステップS1203)。これにより、アクチュエータECU102は、CANバスを流れている駐車支援機能の有効/無効の状態に関するCANメッセージを受信して、現在、駐車支援機能が有効であると誤認識し(ステップS1204)、駐車支援機能の有効/無効の状態に関するCANメッセージ(ステアリング操作指示を示すCANメッセージ)に含まれるステアリングの操舵角の指定に基づきアクチュエータ107(ステアリング)へ制御信号(ステアリング動作指示)を送信する(ステップS1205)。そして、アクチュエータ107(ステアリング)は、受信した制御信号(ステアリング動作指示)に基づいて動作する(ステップS1206)。
- [0093] また、評価装置101は、指示ECU103がCANバスへ送信した駐車支援機能の有効/無効の状態に関するCANメッセージ(フラグ:1)を、

受信（監視）する（ステップS 1 2 0 7）。評価装置1 0 1は、受信した駐車支援機能の有効／無効の状態に関するCANメッセージの内容を、攻撃の期待値と比較することにより、電子制御システム1 1のセキュリティの評価（攻撃の成否についての判定等）を行う（ステップS 1 2 0 8）。評価装置1 0 1は、例えば、受信した駐車支援機能の有効／無効の状態に関するCANメッセージのフラグが、攻撃の期待値としてのフラグ値（1）となっている場合に、アクチュエータ1 0 7（ステアリング）を制御するための制御指示フレームを検出したと判定して、攻撃が成功していると判定する。

[0094] 評価装置1 0 1が、攻撃手順情報1 0 8に従った攻撃が成功していることを確認することで、例えば、その後に電子制御システム1 1に導入するセキュリティ対策技術（例えば、セキュリティECU 1 0 4）の効果について評価できるようになる。

[0095] [1 . 8 . 3 評価システム1 0の動作例3]

図1 3～図1 5は、セキュリティECU 1 0 4を備える状態（図1 参照）の電子制御システム1 1を評価する評価システム1 0の動作（動作例3）を示すシーケンス図である。図1 3に示すシーケンス図は、図1 4に示すシーケンス図へ続く。図1 4に示すシーケンス図は、図1 5に示すシーケンス図へ続く。動作例3では、評価装置1 0 1が、攻撃によりアクチュエータECU 1 0 2を誤認識させようと試みる例を示す。

[0096] シフト位置ECU 1 0 5は、現在のシフト位置（ドライブ：D）を示すCANメッセージをCANバス2 0へ送信し（ステップS 8 0 1）、アクチュエータECU 1 0 2は、CANバス2 0を流れているそのシフト位置を示すCANメッセージを受信する（ステップS 8 0 2）。

[0097] 評価装置1 0 1は、CANバス2 0にシフト位置（ドライブ：D）を示すCANメッセージが流れた直後に、攻撃手順情報1 0 8に従って現在のシフト位置を詐称する偽のシフト位置（リバース：R）を示すCANメッセージをCANバス2 0へ送信する（ステップS 8 0 3）。これにより、アクチュエータECU 1 0 2は、CANバス2 0を流れているシフト位置を示すCA

Nメッセージを受信して、現在のシフト位置がリバース：Rであると誤認識する（ステップS804）。

[0098] また、車速ECU106は、現在の車速（30km/h）を示すCANメッセージをCANバス20へ送信し（ステップS805）、アクチュエータECU102は、CANバス20を流れているその車速を示すCANメッセージを受信する（ステップS806）。

[0099] 評価装置101は、CANバス20に車速（30km/h）を示すCANメッセージが流れた直後に、現在の車速を詐称する偽の車速（0km/h）を示すCANメッセージをCANバス20へ送信する（ステップS807）。これにより、アクチュエータECU102は、CANバス20を流れている車速を示すCANメッセージを受信して、現在の車速が0km/hであると誤認識する（ステップS808）。

[0100] 指示ECU103は、現在、駐車支援機能が有効でないこと（フラグ：0）を示すCANメッセージをCANバス20へ送信し（ステップS901）、アクチュエータECU102は、CANバス20を流れている駐車支援機能の有効／無効の状態に関するCANメッセージを受信する（ステップS902）。

[0101] 評価装置101は、CANバス20に駐車支援機能が有効でないこと（フラグ：0）を示すCANメッセージが流れた直後に、現在、駐車支援機能が有効であること（フラグ：1）を示すCANメッセージをCANバス20へ送信する（ステップS903）。これに対して、セキュリティECU104は、評価装置101がステップS903でCANバス20へ送信した駐車支援機能の有効／無効の状態に関するCANメッセージを、不正なCANメッセージであると判定した場合に、エラーフレームを送信することでそのCANメッセージを無効化する（ステップS1401）。無効化されたCANメッセージの影響を受けないことから、アクチュエータECU102は、アクチュエータ107（ステアリング）107へ制御信号（ステアリング動作指示）を送信しない。このため、アクチュエータ107（ステアリング）は、

特に動作しない。

[0102] 評価装置101は、アクチュエータECU102がアクチュエータ107（ステアリング）へ制御信号（ステアリング動作指示）を送信していないことを確認し（ステップS1402）、アクチュエータ107（ステアリング）が動作していないことを確認し（ステップS1403）、それらが確認できた場合に防御（セキュリティ対策）が成功している（つまり攻撃が失敗している）と判定する（ステップS1501）。なお、評価装置101は、アクチュエータECU102がアクチュエータ107（ステアリング）へ制御信号を送信していないことの確認と、アクチュエータ107（ステアリング）が動作していないことの確認とのうち一方のみが確認できれば防御が成功していると判定する等、その一方のみを用いてセキュリティについての評価を行っても良い。

[0103] [1. 8. 4 評価システム10の動作例4]

図16及び図17は、セキュリティECU104を備える状態（図1参照）の電子制御システム11を評価する評価システム10の動作（動作例4）を示すシーケンス図である。図16に示すシーケンス図は、図17に示すシーケンス図へ続く。動作例4では、評価装置101が、攻撃により指示ECU103を誤認識させようと試みる例を示す。

[0104] シフト位置ECU105は、現在のシフト位置（ドライブ：D）を示すCANメッセージをCANバス20へ送信し（ステップS1101）、指示ECU103は、CANバス20を流れているそのシフト位置を示すCANメッセージを受信する（ステップS1102）。アクチュエータECU102も、同様にCANバス20を流れているそのシフト位置を示すCANメッセージを受信する（ステップS1103）。

[0105] 評価装置101は、CANバス20にシフト位置（ドライブ：D）を示すCANメッセージが流れた直後に、攻撃手順情報108に従って現在のシフト位置を詐称する偽のシフト位置（リバース：R）を示すCANメッセージをCANバス20へ送信する（ステップS1104）。これに対して、セキ

セキュリティECU104は、評価装置101がステップS1104でCANバス20へ送信したシフト位置（リバース：R）を示すCANメッセージを、不正なCANメッセージであると判定した場合に、エラーフレームを送信することでそのCANメッセージを無効化する（ステップS1601）。

[0106] また、車速ECU106は、現在の車速（30km/h）を示すCANメッセージをCANバス20へ送信し（ステップS1107）、指示ECU103は、CANバス20を流れているその車速を示すCANメッセージを受信する（ステップS1108）。アクチュエータECU102も、同様にCANバス20を流れているその車速を示すCANメッセージを受信する（ステップS1109）。

[0107] 評価装置101は、CANバス20に車速（30km/h）を示すCANメッセージが流れた直後に、現在の車速を詐称する偽の車速（0km/h）を示すCANメッセージをCANバス20へ送信する（ステップS1110）。これに対して、セキュリティECU104は、評価装置101がステップS1110でCANバス20へ送信した車速（0km/h）を示すCANメッセージを、不正なCANメッセージであると判定した場合に、エラーフレームを送信することでそのCANメッセージを無効化する（ステップS1602）。

[0108] 評価装置101は、駐車支援機能を開始することを示すCANメッセージをCANバス20へ送信し（ステップS1201）、指示ECU103は、CANバス20を流れているその駐車支援機能の開始に関するCANメッセージ（駐車支援機能を開始することを示すCANメッセージ）を受信する（ステップS1202）。

[0109] 続いて指示ECU103は、偽のシフト位置及び車速を受信していないので、駐車支援機能を実行するための一定条件が満たされないことから、駐車支援機能が無効であること（フラグ：0）を示すCANメッセージ（駐車支援機能の有効／無効の状態に関するCANメッセージ）をCANバス20へ送信する（ステップS1701）。これにより、アクチュエータECU10

2は、CANバスを流れている駐車支援機能の有効／無効の状態に関するCANメッセージを受信して、現在、駐車支援機能が無効であると認識し（ステップS1702）、アクチュエータ107（ステアリング）へ制御信号（ステアリング動作指示）を送信しない。

[0110] 評価装置101は、指示ECU103がCANバス20へ送信した駐車支援機能の有効／無効の状態に関するCANメッセージ（フラグ：0）を受信（監視）する（ステップS1703）。評価装置101は、受信した駐車支援機能の有効／無効の状態に関するCANメッセージの内容を、攻撃の期待値と比較することにより、電子制御システム11のセキュリティの評価（攻撃の成否についての判定等）を行う（ステップS1704）。評価装置101は、例えば、受信した駐車支援機能の有効／無効の状態に関するCANメッセージのフラグが、攻撃の期待値としてのフラグ値（1）となっていない場合に、アクチュエータ107（ステアリング）を制御するための制御指示フレームを検出しなかった判定して、防御（セキュリティ対策）が成功していると判定する。

[0111] （変形例）

以上のように、本開示に係る技術の例示として実施の形態1を説明した。しかしながら、本開示に係る技術は、これに限定されず、適宜、変更、置き換え、付加、省略等を行った実施の形態にも適用可能である。例えば、以下のような変形例も本開示の一実施態様に含まれる。

[0112] （1）上記実施の形態では、評価装置101がCANメッセージ（偽の情報を示すCANメッセージ）の送信により電子制御システム11を攻撃する例を示した。しかし、評価装置101は、いかなる方法を用いて攻撃を行っても良く、CANメッセージの送信以外の方法で攻撃を行っても良い。例えば、評価装置101は、評価対象の電子制御システム11における各種ECUと信号線で接続されるセンサのセンシング情報を偽の情報に差し替えてそのECUに誤認識させることとしても良い。

[0113] （2）上述の電子制御システム11では、各種ECU及びアクチュエータ

は、リアルな（実物としての）ＥＣＵ及びアクチュエータを想定して説明した。しかし、評価システム１０の評価対象としての電子制御システム１１における各種ＥＣＵは、リアルなＥＣＵ（例えば、評価ボード上で実装されたＥＣＵ、製品としてのＥＣＵ等）の代わりに、そのＥＣＵを模擬（シミュレート）する模擬ＥＣＵ（例えば、そのＥＣＵの機能、挙動等を模擬するソフトウェアを実行するコンピュータ等）であることとしても良い。同様に、評価対象の電子制御システム１１では、リアルなアクチュエータ（ステアリング、アクセル、ブレーキ等）の代わりに、そのアクチュエータを模擬する模擬アクチュエータ（例えば、アクチュエータの動作を模擬するシミュレーションソフトウェアを実行するコンピュータ等）を備えていても良い。即ち、評価システム１０の評価対象は、リアルなアクチュエータ及び模擬アクチュエータのいずれかであるアクチュエータ部を備える電子制御システムであれば良い。アクチュエータ部が模擬アクチュエータである場合においてはアクチュエータ部の観測を、アクチュエータ監視部２０５は例えばシミュレーションソフトウェアの出力機能等を利用してシミュレーションで用いられる各種パラメータを確認すること等で行っても良く、信号監視部２０４は例えばそのシミュレーションソフトウェアへ入力されるパラメータ等を確認すること等で行っても良い。即ち、アクチュエータ部が模擬アクチュエータである場合において監視部２００は、アクチュエータ部の動作を、コンピュータにおいてシミュレーションソフトウェア（プログラム）に関わる所定データ（例えばアクチュエータの動作で変化する物理量に対応したコンピュータの所定メモリ領域の内容或いは出力内容等）の変化を観測することによって検出しても良い。

- [0114] （３）上記実施の形態では、評価装置１０１が、ＣＡＮバス２０に接続された１つの装置である例を示したが、評価装置１０１は、攻撃手順情報１０８に従って攻撃用のＣＡＮメッセージを送信する送信装置と、ＣＡＮバス２０を流れるＣＡＮメッセージ、アクチュエータＥＣＵ１０２の出力する制御信号、アクチュエータ１０７の挙動等を監視する監視装置とに分離される等

、複数の筐体に分離された構成を備えても良い。

[0115] (4) 上記実施の形態では、評価システム10の評価対象として、CANバス20による車載ネットワークを備える電子制御システム11を例示したが、評価システム10で評価装置101が攻撃用のメッセージを送信したり監視の対象としたりするネットワークは、必ずしも車載ネットワークでなくとも良く、また、CANプロトコルによる通信が行われるCANバス20以外のネットワークであっても良い。例えば、評価システム10は、ロボット、産業機器等のネットワークその他のネットワーク通信システムを評価対象としても良い。また、CANプロトコルは、オートメーションシステム内の組み込みシステム等に用いられるCANOpen、或いは、TTCAN (Time-Triggered CAN)、CANFD (CAN with Flexible Data Rate) 等の派生的なプロトコルも包含する広義の意味のものと扱われるべきである。また、評価対象のネットワークシステムで、CANプロトコル以外の通信プロトコル、例えば、Ethernet (登録商標) や、MOST (登録商標)、FlexRay (登録商標)、LIN (Local Interconnect Network) 等を用いても良い。また、各種プロトコルに従ったネットワークを組み合わせた複合的なネットワークを含むシステムを評価対象として、評価装置101で、そのネットワークに対して攻撃及び監視を行うこととしても良い。

[0116] (5) 上記実施の形態では、評価装置101が、偽の情報を示すCANメッセージを送信する攻撃を行う例を示したが、この他に、シフト位置ECU105、車速ECU106、指示ECU103等が送信するCANメッセージの内容の一部をCANバス20上で改ざんすることで攻撃を行っても良い。

[0117] (6) 上述した評価装置101は、例えば車載ネットワークシステムの一部に相当する電子制御システム11を評価対象として攻撃することで評価しても良い。この場合には、評価対象に含まれない車載ネットワークシステムの部分(評価環境を構成する部分)を模擬するために、評価対象に含まれない車載ネットワークに定常状態で流れる正規のCANメッセージを送信しつ

つ、評価対象に対して攻撃を仕掛けることとしても良い。この場合において、例えば、評価対象におけるセキュリティECU104が、不正なCANメッセージを検知して無効化する場合に、関係のない正規のメッセージを無効化していないかを確認することで、評価対象を評価しても良い。また、不正なCANメッセージを検知して無効化する以外の攻撃対処のためのセキュリティ機能（CANメッセージへのメッセージ認証コード（MAC）付与やMAC検証等）が導入されている場合に、攻撃対処のために、定常状態の正規のCANメッセージの送受信に悪影響（大幅な通信遅延等）を及ぼしていないか等を確認することで、評価装置101は、評価対象を評価しても良い。

[0118] （7）評価装置101は、評価対象のセキュリティ（攻撃耐性等）についての評価として、防御をすり抜けた不正なCANメッセージの個数や割合に基づいて、攻撃耐性の有無の判定等といった評価を行うものであっても良い。なお、評価装置101は、攻撃耐性の有無を判定するために、不正なCANメッセージの個数や割合についての上限等を規定する閾値を用い得る。この閾値は、評価装置101に対して任意に設定可能にしても良いし、評価を繰り返し実施する場合において評価結果等に応じて変化（調整）し得るようにしても良い。また、評価装置101は、攻撃の成功率（成功の頻度等）を算定しても良い。このように評価装置101は、攻撃成否或いは防御成否の択一判定の他に、例えば複数の防御機能それぞれが作動するか否か或いはどの程度有効に作用したかについて評価しても良い。また、評価装置101では、送信部201aが、攻撃手順情報108が示す送信順序で複数のCANメッセージをCANバス20に送信する攻撃パターンを複数回繰り返し、評価部206が、攻撃パターンの繰り返しによる監視部200の監視結果の変化の有無に応じて評価結果が相違するように評価を行うこととしても良い。なお、評価装置101の評価部206での評価結果は、評価装置101によりメモリ等の記憶媒体に記録される他、評価装置101の外部に出力（例えば、評価結果の表示、評価結果を示す情報の送信等）され得る。例えば、評価部206は、評価結果として評価対象の電子制御システムに攻撃耐性があ

るか否かを示す情報を出力することとしても良い。

[0119] (8) 評価対象の電子制御システム 11 におけるセキュリティ ECU 104 を含むセキュリティ機能は、不正の検知に関するログ情報 (CAN メッセージの受信履歴等) を記録することとしても良く、この場合には、評価装置 101 は、そのログ情報と、その評価装置 101 が保持する、攻撃に関する期待値とを比較することで、攻撃が成功したか否かの判定或いは攻撃が成功した確率等の算出を行うことで、セキュリティについての評価を行うこととしても良い。

[0120] (9) 上記実施の形態では電子制御システム 11 はセキュリティ機能として、独立したセキュリティ ECU 104 を備え得ることとしたが、バスを介して通信する複数の ECU のうちの全部又は一部の ECU がセキュリティ機能を備えることとしても良い。また、複数の ECU がセキュリティ機能を分散して実現しても良い。

[0121] (10) 上記実施の形態では評価装置 101 が評価対象の電子制御システム 11 におけるバスに直接接続されている例を示したが、評価装置 101 と評価対象との間に、ゲートウェイ等の中継装置が介在しても良い。例えば、評価装置 101 が、ゲートウェイとの間で相互認証又は片方向認証を実施した上で攻撃用の CAN メッセージを送信することで、ゲートウェイにその CAN メッセージを CAN バス 20 へと転送させ、CAN バス 20 からの CAN メッセージを、ゲートウェイを介して取得する等により、評価対象のセキュリティ (攻撃耐性等) を評価することとしても良い。

[0122] (11) 評価装置 101 は、アクチュエータ監視部 205 でアクチュエータ 107 を観測する代わりに、アクチュエータ ECU 102 が CAN バス 20 へ送信するアクチュエータ 107 の状態通知 (ステアリングの現在の角度、アクセル又はブレーキの変位量、エンジンの回転数等) に係る CAN メッセージを監視することでアクチュエータ 107 の動作 (挙動) を間接的に確認しても良い。

[0123] (12) 上記実施の形態における評価装置 101 及び各種 ECU は、例え

ば、プロセッサ、メモリ等のデジタル回路、アナログ回路、通信回路等を含む装置であることとしたが、ディスプレイ、キーボード、マウス等の他のハードウェア構成要素を含んでいても良い。また、メモリに記憶された制御プログラムがプロセッサにより実行されてソフトウェア的に機能を実現する代わりに、専用のハードウェア（デジタル回路等）によりその機能を実現することとしても良い。例えば、評価装置101のCANバス監視部203、信号監視部204、アクチュエータ監視部205、送受信部201、保持部202、評価部206及び制御部207の各機能ブロックは、集積回路で実現され得る。また、例えば、アクチュエータECU102の送受信部301、指示送信部302、状態取得部303、判定部304及び制御部305の各機能ブロックは、集積回路で実現され得る。また、例えば、指示ECU103の送受信部401、判定部402、算出部403及び制御部404の各機能ブロックは、集積回路で実現され得る。また、例えば、セキュリティECU104の送受信部501、CANバス監視部502及び制御部503の各機能ブロックは、集積回路で実現され得る。また、例えば、シフト位置ECU105或いは車速ECU106の送受信部601、状態取得部602及び制御部603の各機能ブロックは、集積回路で実現され得る。

[0124] (13) 上記実施の形態における各装置（評価装置101、各種ECU等）を構成する構成要素の一部又は全部は、1個のシステムLSI（Large Scale Integration：大規模集積回路）から構成されているとしても良い。システムLSIは、複数の構成部を1個のチップ上に集積して製造された超多機能LSIであり、具体的には、マイクロプロセッサ、ROM、RAM等を含んで構成されるコンピュータシステムである。前記RAMには、コンピュータプログラムが記録されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、システムLSIは、その機能を達成する。また、上記各装置を構成する構成要素の各部は、個別に1チップ化されていても良いし、一部又は全部を含むように1チップ化されても良い。また、ここでは、システムLSIとしたが、集積度の違いにより、IC

、ＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩと呼称されることもある。また、集積回路化の手法はＬＳＩに限るものではなく、専用回路又は汎用プロセッサで実現しても良い。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Field Programmable Gate Array）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なりコンフィギュラブル・プロセッサを利用しても良い。更には、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行っても良い。バイオ技術の適用等が可能性としてあり得る。

[0125] （１４）上記各装置を構成する構成要素の一部又は全部は、各装置に脱着可能なＩＣカード又は単体のモジュールから構成されているとしても良い。前記ＩＣカード又は前記モジュールは、マイクロプロセッサ、ＲＯＭ、ＲＡＭ等から構成されるコンピュータシステムである。前記ＩＣカード又は前記モジュールは、上記の超多機能ＬＳＩを含むとしても良い。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、前記ＩＣカード又は前記モジュールは、その機能を達成する。このＩＣカード又はこのモジュールは、耐タンパ性を有するとしても良い。

[0126] （１５）本開示の一態様としては、例えば図８～図１７等に例示する処理手順の全部又は一部を含む評価方法であるとしても良い。例えば、評価方法は、ＣＡＮバス２０を介して通信する複数のＥＣＵを備える電子制御システム１１のセキュリティに関する評価を行う評価方法であって、複数のフレームの内容及び送信順序を示す攻撃手順情報１０８を保持し、攻撃手順情報１０８が示す送信順序で複数のフレームをＣＡＮバス２０に送信し（例えばステップＳ８０３、Ｓ８０７、Ｓ９０３、Ｓ１１０４、Ｓ１１１０、Ｓ１２０１）、複数のフレームがＣＡＮバス２０に送信される際に、複数のＥＣＵのいずれかにより制御されるアクチュエータ部（例えばアクチュエータ１０７）について直接又は間接的に監視し（例えばステップＳ１００１、Ｓ１００２、Ｓ１２０７）、監視による監視結果に基づいて評価（例えばＳ１００３、Ｓ１２０８）を行う評価方法である。また、本開示の一態様としては、こ

の評価方法に係る処理をコンピュータにより実現するコンピュータプログラムであるとしても良いし、前記コンピュータプログラムからなるデジタル信号であるとしても良い。また、本開示の一態様としては、前記コンピュータプログラム又は前記デジタル信号をコンピュータで読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD（Blu-ray（登録商標）Disc）、半導体メモリ等に記録したものとしても良い。また、これらの記録媒体に記録されている前記デジタル信号であるとしても良い。また、本開示の一態様としては、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしても良い。また、本開示の一態様としては、マイクロプロセッサとメモリを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記録しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するものとしても良い。また、前記プログラム若しくは前記デジタル信号を前記記録媒体に記録して移送することにより、又は、前記プログラム若しくは前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するものとしても良い。

[0127] （16）上記実施の形態及び上記変形例で示した各構成要素及び機能を任意に組み合わせることで実現される形態も本開示の範囲に含まれる。

産業上の利用可能性

[0128] 本開示は、電子制御システムに対して施されたセキュリティ対策技術が攻撃を適切に防御できるか否か等の評価を実施するために利用可能である。

符号の説明

- [0129] 10 評価システム
- 11 電子制御システム
- 20 CANバス
- 101 評価装置

102 アクチュエータECU
103 指示ECU
104 セキュリティECU
105 シフト位置ECU
106 車速ECU
107 アクチュエータ
108 攻撃手順情報
200 監視部
201, 301, 401, 501, 601 送受信部
201a 送信部
201b 受信部
202 保持部
203, 502 CANバス監視部
204 信号監視部
205 アクチュエータ監視部
206 評価部
207, 305, 404, 503, 603 制御部
302 指示送信部
303, 602 状態取得部
304, 402 判定部
403 算出部

請求の範囲

- [請求項1] 電子制御システムにおいて複数の電子制御ユニットが通信に用いるバスに接続され、当該電子制御システムのセキュリティに関する評価を行う評価装置であって、
- 複数のフレームの内容及び送信順序を示す攻撃手順情報を保持する保持部と、
- 前記攻撃手順情報が示す送信順序で前記複数のフレームを前記バスに送信する送信部と、
- 前記複数の電子制御ユニットのいずれかにより制御されるアクチュエータ部について監視する監視部と、
- 前記送信部により前記複数のフレームが前記バスに送信される際における前記監視部の監視結果に基づいて前記評価を行う評価部とを備える
- 評価装置。
- [請求項2] 前記複数の電子制御ユニットは、CAN (Controller Area Network) プロトコルに従って前記バスを介して通信を行う
- 請求項1記載の評価装置。
- [請求項3] 前記監視部は、前記アクチュエータ部についての前記監視として、前記複数の電子制御ユニットのうちの1つに前記アクチュエータ部を制御させるよう指示するための制御指示フレームが前記バスに送信されたことを検出し、
- 前記評価部は、前記送信部により前記複数のフレームの1つ以上が前記バスに送信された後の一定期間内に、前記制御指示フレームが前記バス上で送信されたことが前記監視部により検出されたか否かに応じて評価結果が相違するように前記評価を行う
- 請求項1又は2記載の評価装置。
- [請求項4] 前記監視部は、前記アクチュエータ部についての前記監視として、前記複数の電子制御ユニットのうちの1つから前記アクチュエータ部

に制御信号が入力されたことを検出し、

前記評価部は、前記送信部により前記複数のフレームの1つ以上が前記バスに送信された後の一定期間内に、前記アクチュエータ部に前記制御信号が入力されたことが前記監視部により検出されたか否かに応じて評価結果が相違するように前記評価を行う

請求項1～3のいずれか一項に記載の評価装置。

[請求項5] 前記監視部は、前記アクチュエータ部についての前記監視として、前記アクチュエータ部の動作を検出し、

前記評価部は、前記送信部により前記複数のフレームの1つ以上が前記バスに送信された後の一定期間内に、前記アクチュエータ部が動作したことが前記監視部により検出されたか否かに応じて評価結果が相違するように前記評価を行う

請求項1～4のいずれか一項に記載の評価装置。

[請求項6] 前記アクチュエータ部は、アクチュエータを有し、
前記監視部は、前記アクチュエータ部の動作を、前記アクチュエータの動作で変化する物理量の測定によって検出する

請求項5記載の評価装置。

[請求項7] 前記アクチュエータ部は、アクチュエータの動作を模擬するプログラムを実行するコンピュータを有し、

前記監視部は、前記アクチュエータ部の動作を、前記コンピュータにおいて前記プログラムに関わる所定データの変化を観測することによって検出する

請求項5記載の評価装置。

[請求項8] 前記攻撃手順情報は更に前記複数のフレームについての送信間隔を示し、

前記送信部は、前記攻撃手順情報が示す送信順序及び送信間隔に従って前記複数のフレームを前記バスに送信する

請求項1～7のいずれか一項に記載の評価装置。

- [請求項9] 前記評価部は、評価結果として前記電子制御システムに攻撃耐性があるか否かを示す情報を出力する
請求項1～8のいずれか一項に記載の評価装置。
- [請求項10] 前記送信部は、前記攻撃手順情報が示す送信順序で前記複数のフレームを前記バスに送信する攻撃パターンを複数回繰り返し、
前記評価部は、前記攻撃パターンの繰り返しによる前記監視結果の変化の有無に応じて評価結果が相違するように前記評価を行う
請求項1～9のいずれか一項に記載の評価装置。
- [請求項11] バスを介して通信する複数の電子制御ユニットを備える電子制御システムのセキュリティに関する評価を行う評価システムであって、
複数のフレームの内容及び送信順序を示す攻撃手順情報を保持する保持部と、
前記攻撃手順情報が示す送信順序で前記複数のフレームを前記バスに送信する送信部と、
前記複数の電子制御ユニットのいずれかにより制御されるアクチュエータ部について監視する監視部と、
前記送信部により前記複数のフレームが前記バスに送信される際における前記監視部の監視結果に基づいて前記評価を行う評価部とを備える
評価システム。
- [請求項12] バスを介して通信する複数の電子制御ユニットを備える電子制御システムのセキュリティに関する評価を行う評価方法であって、
複数のフレームの内容及び送信順序を示す攻撃手順情報を保持し、
前記攻撃手順情報が示す送信順序で前記複数のフレームを前記バスに送信し、
前記複数のフレームが前記バスに送信される際に、前記複数の電子制御ユニットのいずれかにより制御されるアクチュエータ部について監視し、

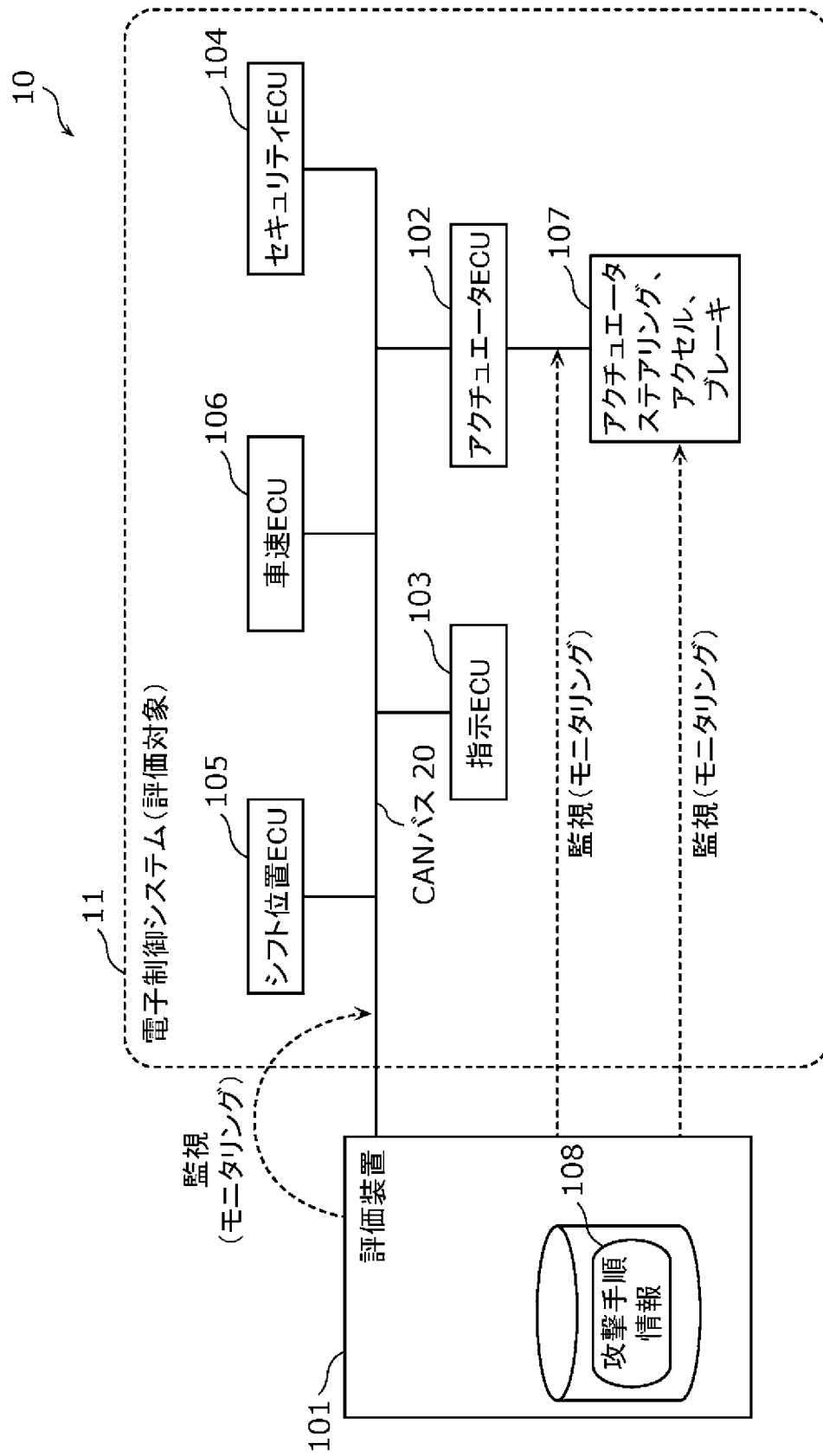
前記監視による監視結果に基づいて前記評価を行う
評価方法。

[請求項13] 前記複数の電子制御ユニットは、CAN (Controller Area Network) プロトコルに従って前記バスを介して通信を行い、
前記評価方法は、

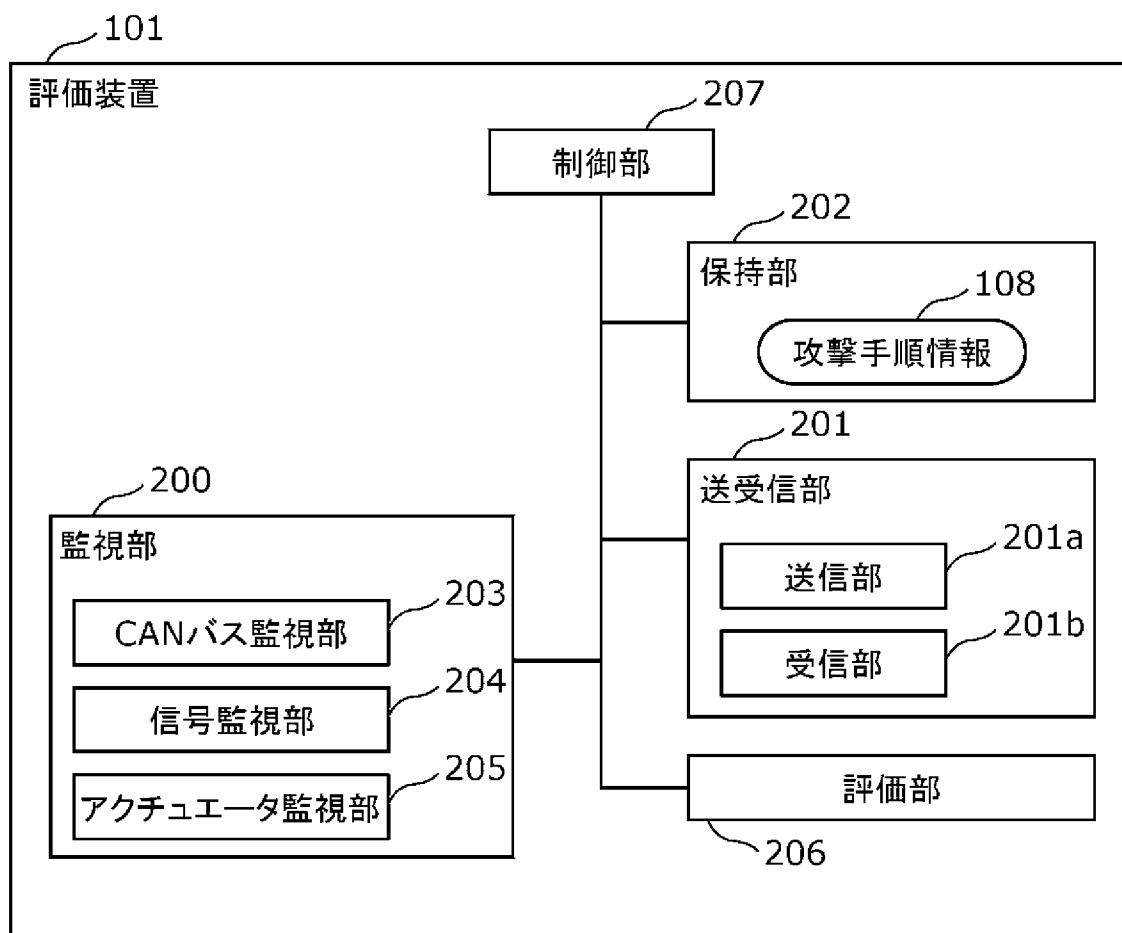
前記複数のフレームの1つ以上が前記バスに送信された後の一定期間内に、前記複数の電子制御ユニットのうちの1つに前記アクチュエータ部を制御させるよう指示するための制御指示フレームが前記バスに送信されたことを検出したか否かに応じて、評価結果が相違するように前記評価を行う

請求項12記載の評価方法。

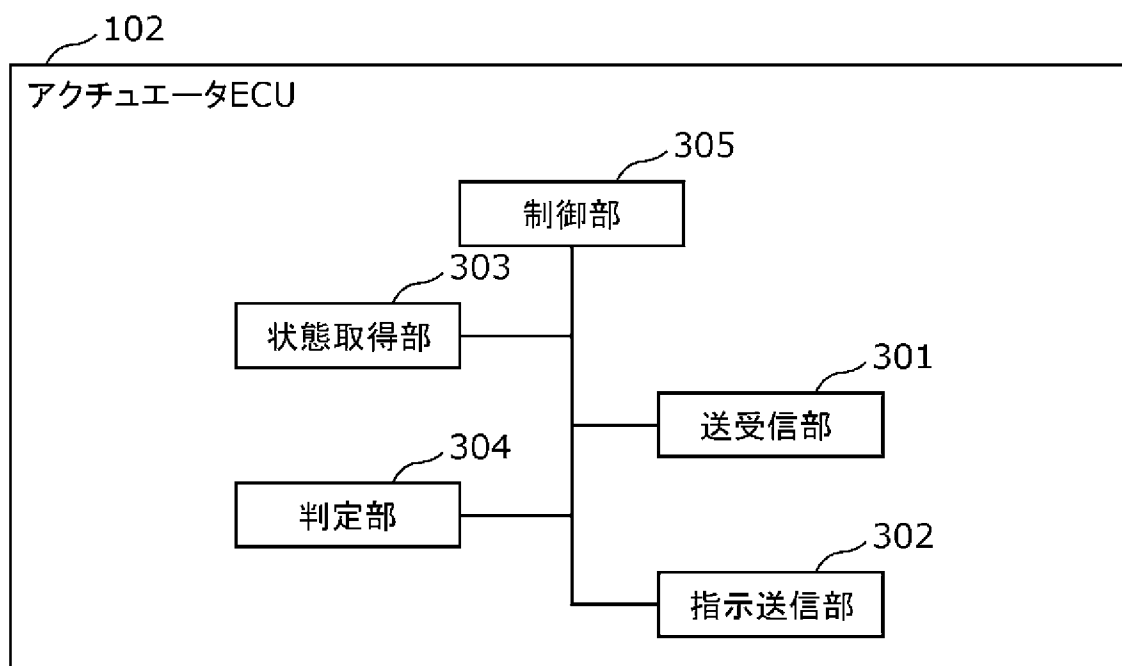
[図1]



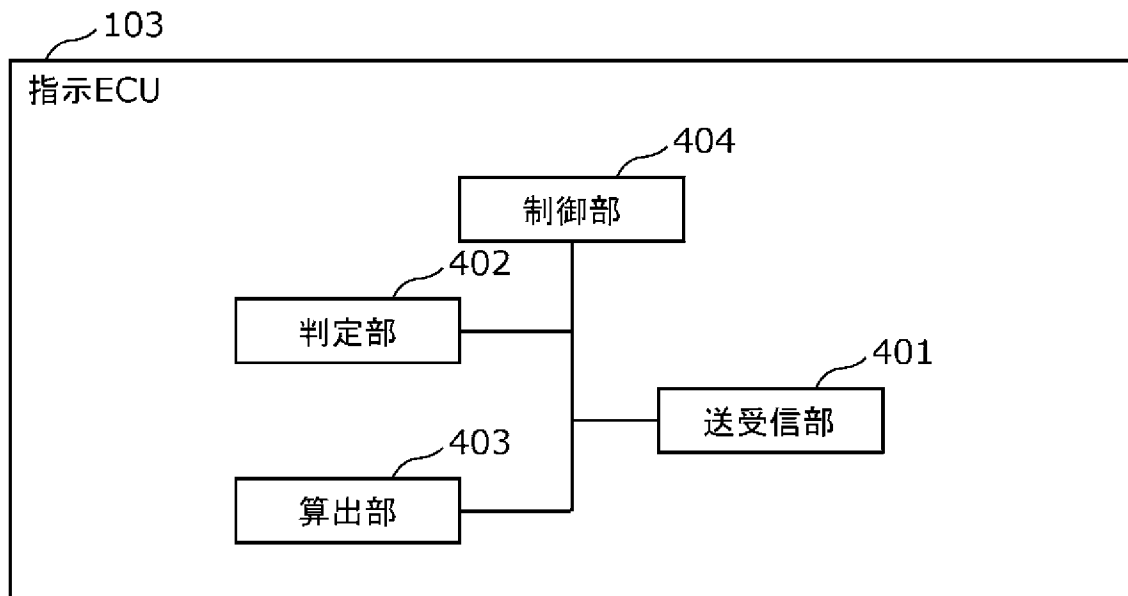
[図2]



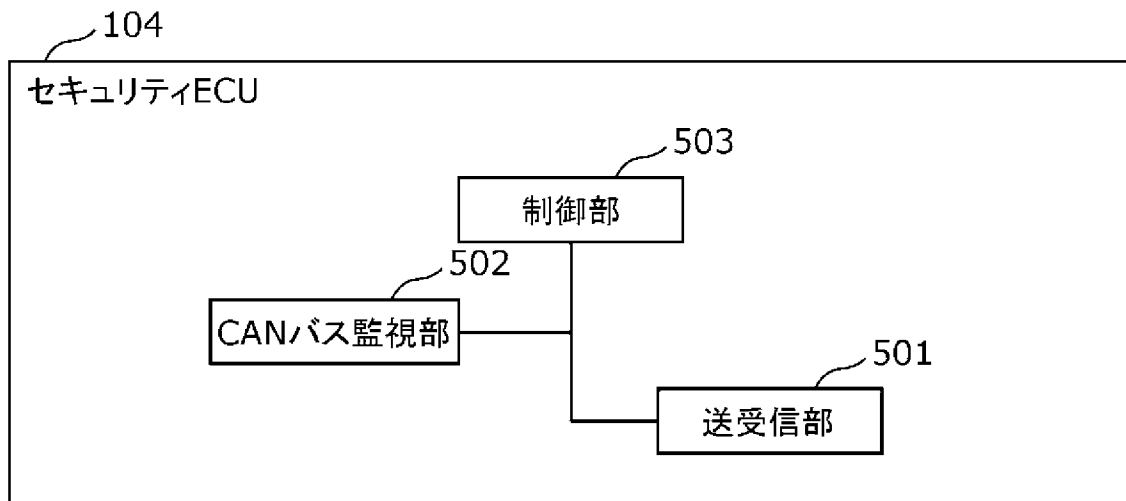
[図3]



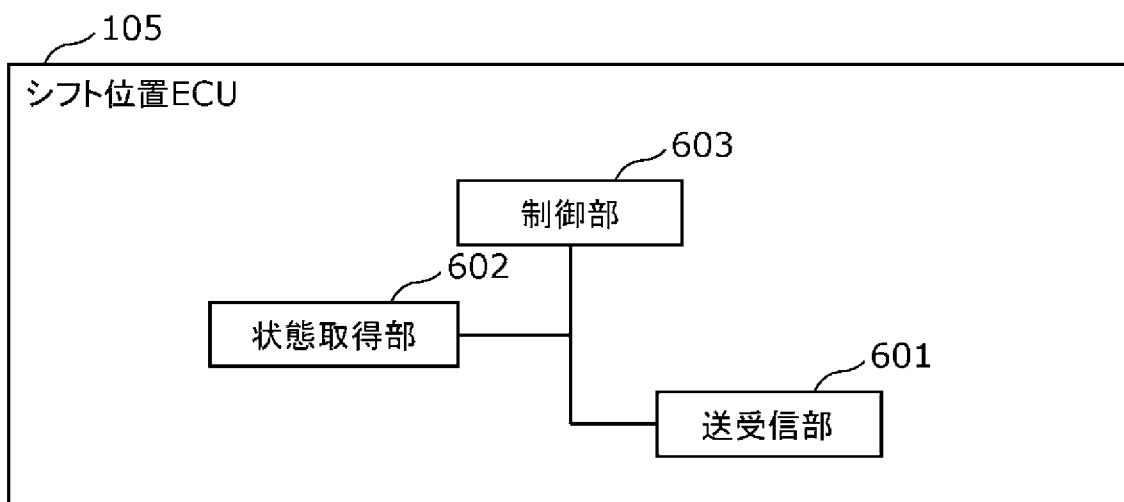
[図4]



[図5]



[図6]



[図7]

評価対象機能	送信メッセージ	メッセージID	データ内容	送信間隔	送信順序
駐車 支援機能	シフト位置	0x0123	"リバース"	20ms	1
	車速	0x0034	"6km/h"	20ms	2
	ステアリング 操作指示	0x0256	フラグ"1" "右旋回15度"	20ms	3
車線維持 支援機能	車速	0x0034	"70km/h"	10ms	1
	白線検知	0x0456	"逸脱"	10ms	2
	ステアリング 操作指示	0x0256	フラグ"1" "左旋回5度"	10ms	3
衝突回避 支援機能	車速	0x0034	"20km/h"	10ms	1
	障害物検知	0x0521	"障害物あり"	10ms	2
	ブレーキ 操作指示	0x0101	フラグ"1" "ブレーキ踏込"	10ms	3

Figure 1 is a block diagram of a vehicle control system. It shows several interconnected components: 101 (評価装置 - Evaluation Device), 102 (アクチュエータ ECU - Actuator ECU), 103 (指示ECU - Instruction ECU), 104 (車速ECU - Vehicle Speed ECU), 105 (シフト位置ECU - Shift Position ECU), 106 (アクチュエータ (ステアリング) - Actuator (Steering)), and 107 (アクチュエータ (ブレーキ) - Actuator (Brake)). The diagram illustrates the flow of control signals and data between these components, including a central processing unit (108) and various sensors (109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200). The diagram shows a complex network of control signals and data flow, with a central processing unit (108) and various sensors (109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200). The diagram shows a complex network of control signals and data flow, with a central processing unit (108) and various sensors (109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200). The diagram shows a complex network of control signals and data flow, with a central processing unit (108) and various sensors (109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200). The diagram shows a complex network of control signals and data flow, with a central processing unit (108) and various sensors (109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200). The diagram shows a complex network of control signals and data flow, with a central processing unit (108) and various sensors (109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200). The diagram shows a complex network of control signals and data flow, with a central processing unit (108) and various sensors (109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200). The diagram shows a complex network of control signals and data flow, with a central processing unit (108) and various sensors (109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200). The diagram shows a complex network of control signals and data flow, with a central processing unit (108) and various sensors (109, 110, 111, 112,

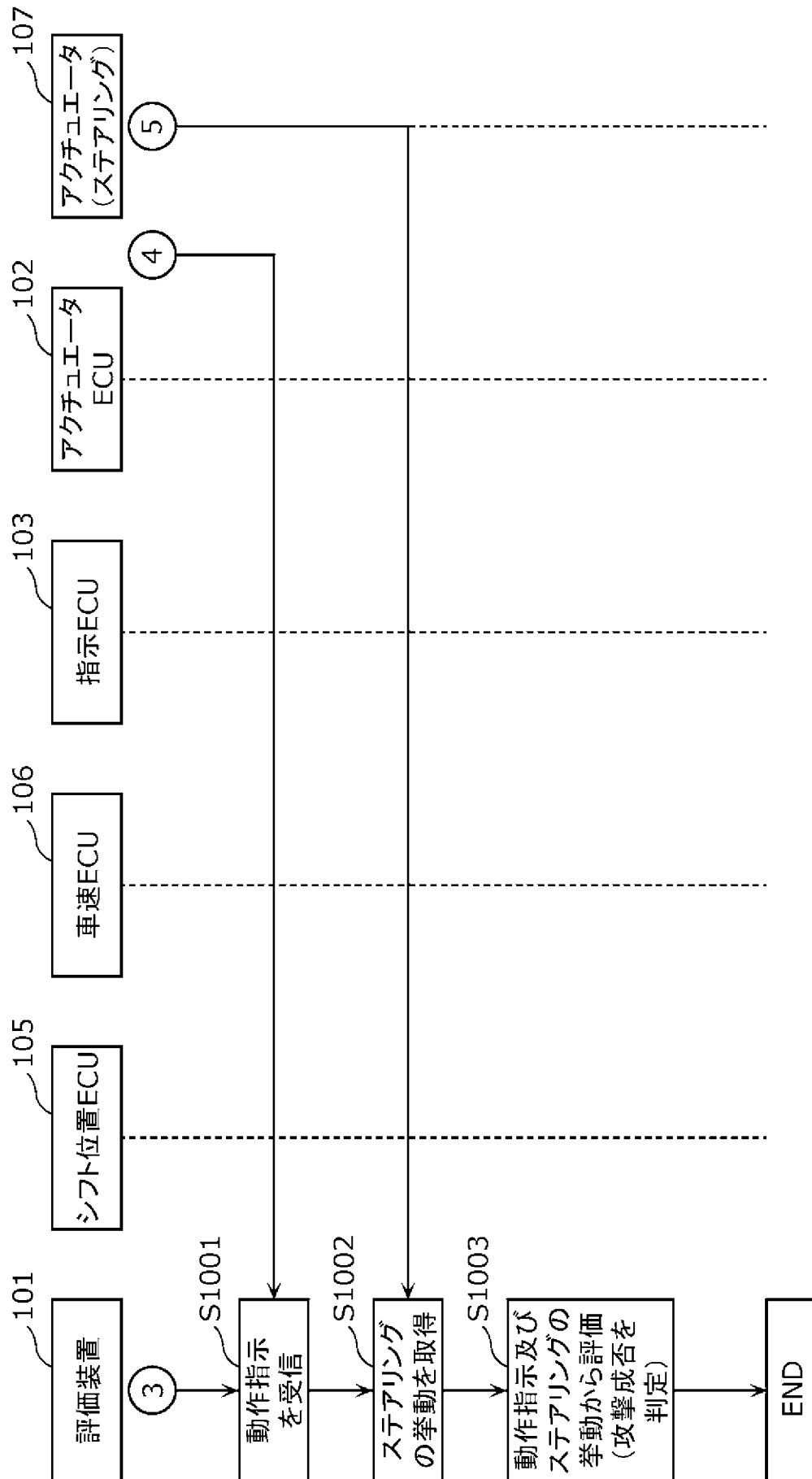
Figure 1 is a block diagram of a vehicle control system. The system includes the following components and their interconnections:

- 101: 評価装置 (Evaluation Device)**: Connected to 102 and 103 via dashed lines.
- 102: アクチュエータ ECU (Actuator ECU)**: Connected to 101, 103, and 107 via dashed lines.
- 103: 指示 ECU (Instruction ECU)**: Connected to 101, 102, and 106 via dashed lines.
- 106: 車速 ECU (Vehicle Speed ECU)**: Connected to 103 and 107 via dashed lines.
- 107: アクチュエータ (ステアリング) (Actuator (Steering))**: Connected to 102 and 106 via dashed lines.

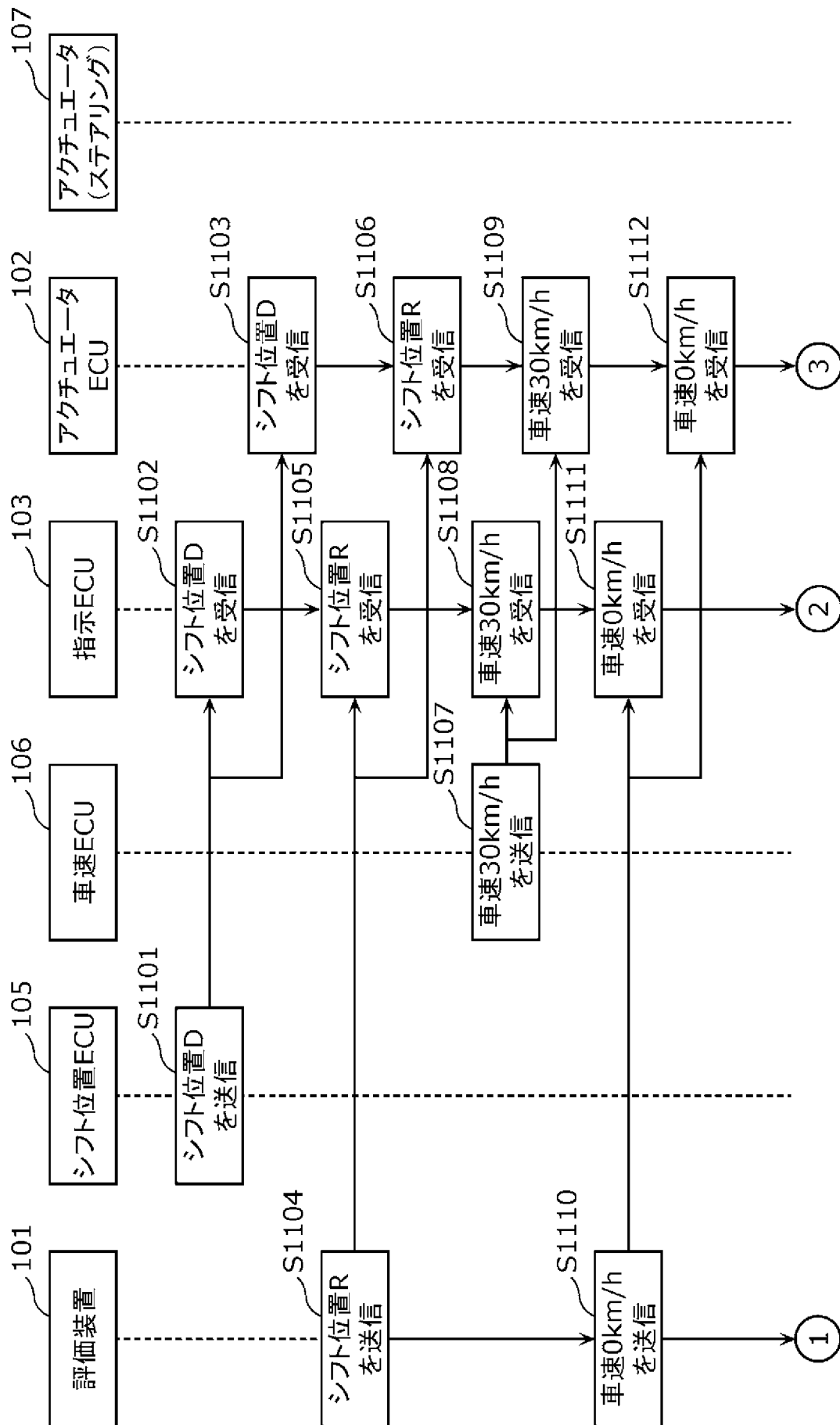
The system also includes a sequence of steps:

- 1**: 評価装置 (Evaluation Device) sends a signal (S903) to アクチュエータ ECU (Actuator ECU).
- 2**: アクチュエータ ECU (Actuator ECU) receives a signal (S902) from 指示 ECU (Instruction ECU).
- 3**: 評価装置 (Evaluation Device) sends a signal (S901) to 指示 ECU (Instruction ECU).
- 4**: ステアリング (Steering) receives a signal (S905) from 車速 ECU (Vehicle Speed ECU).
- 5**: ステアリング (Steering) receives a signal (S906) from アクチュエータ ECU (Actuator ECU).

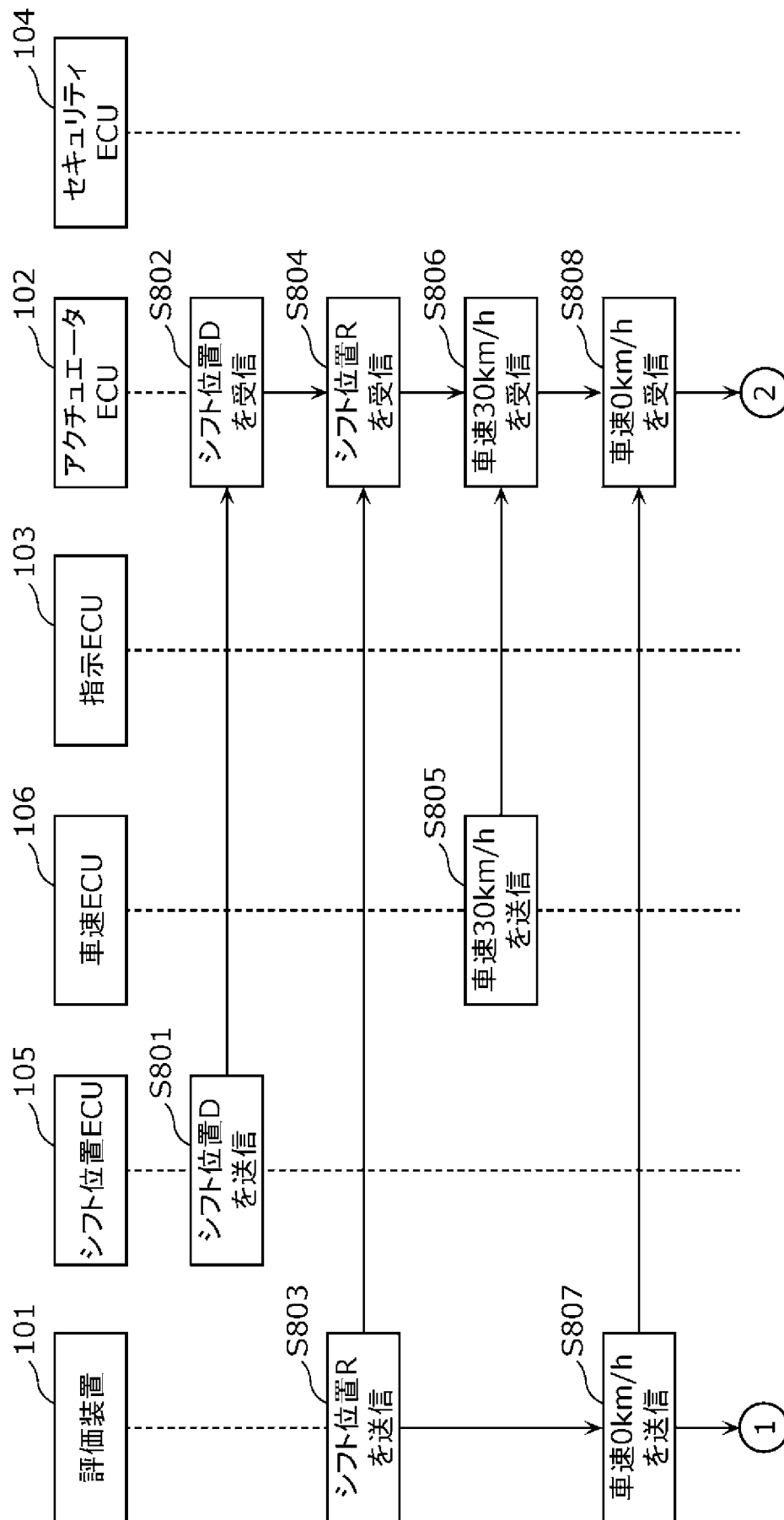
[図10]



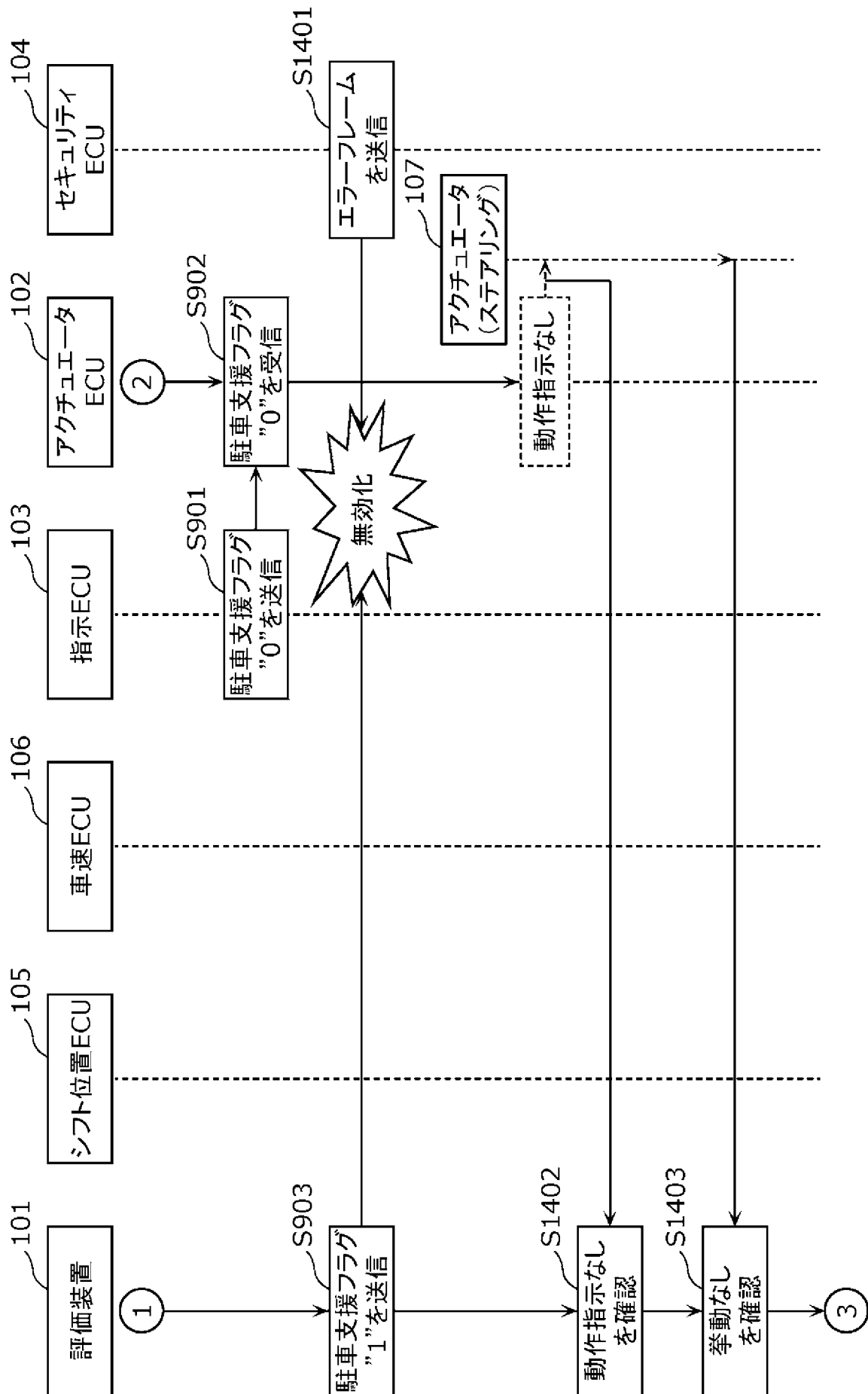
[図11]



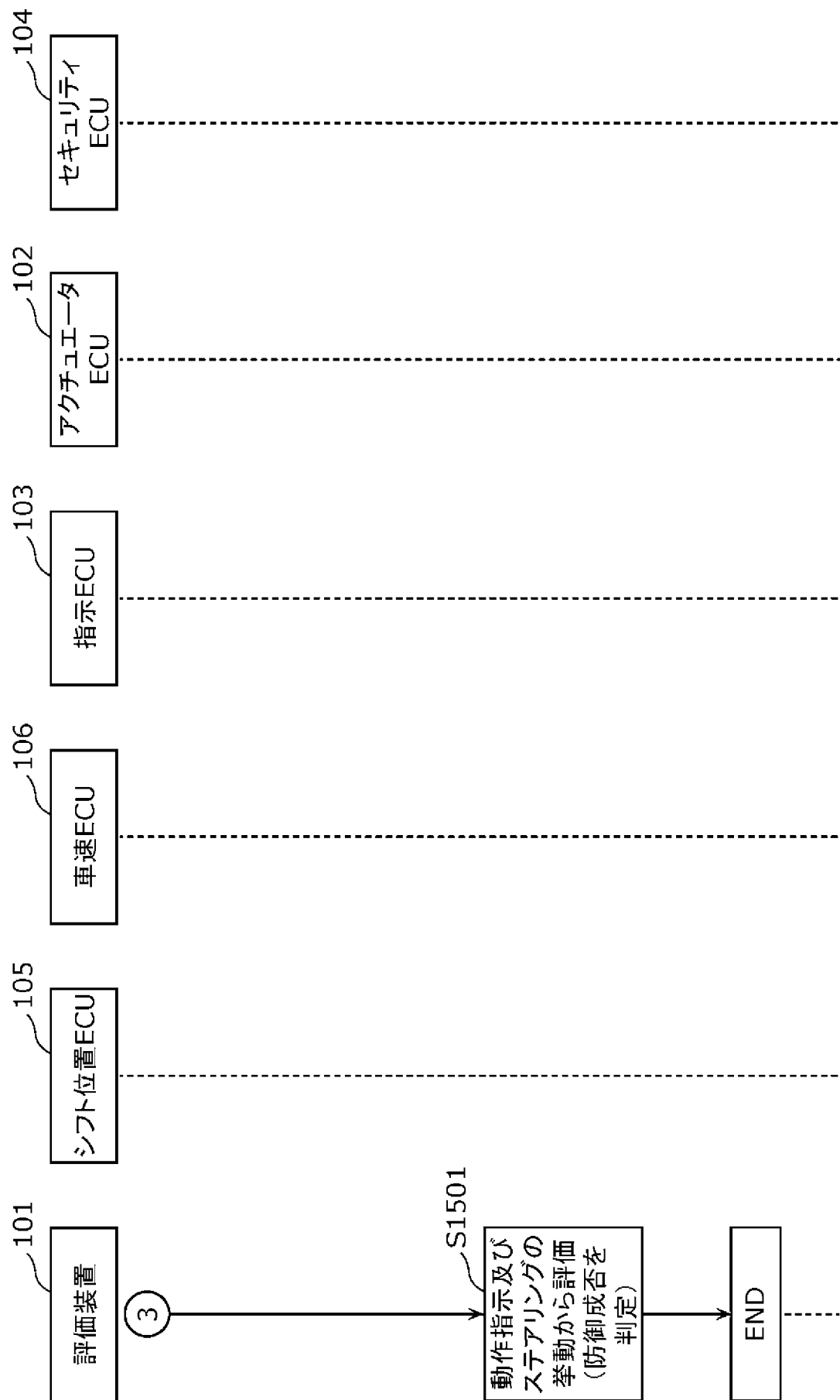
[図13]



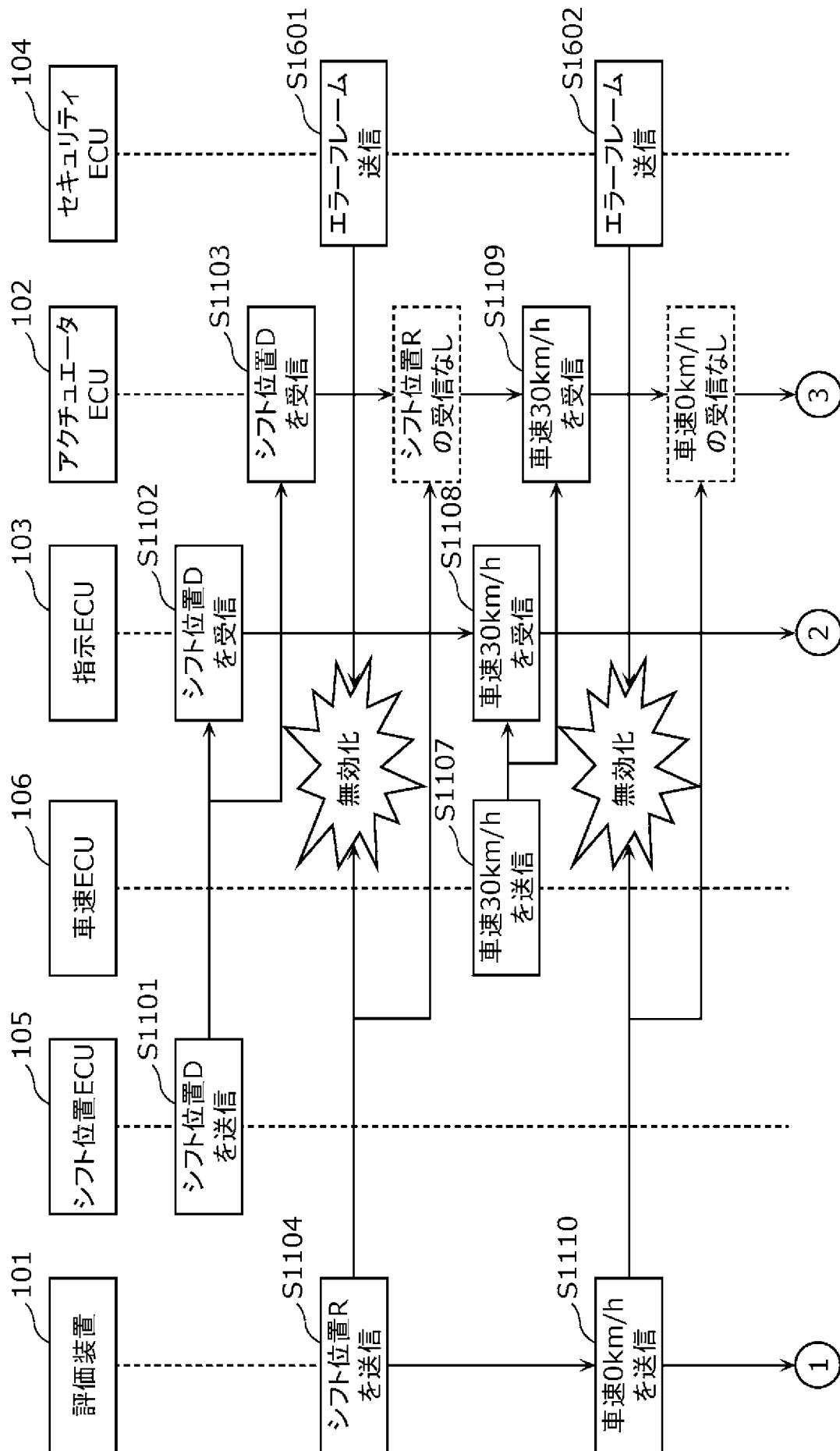
[図14]

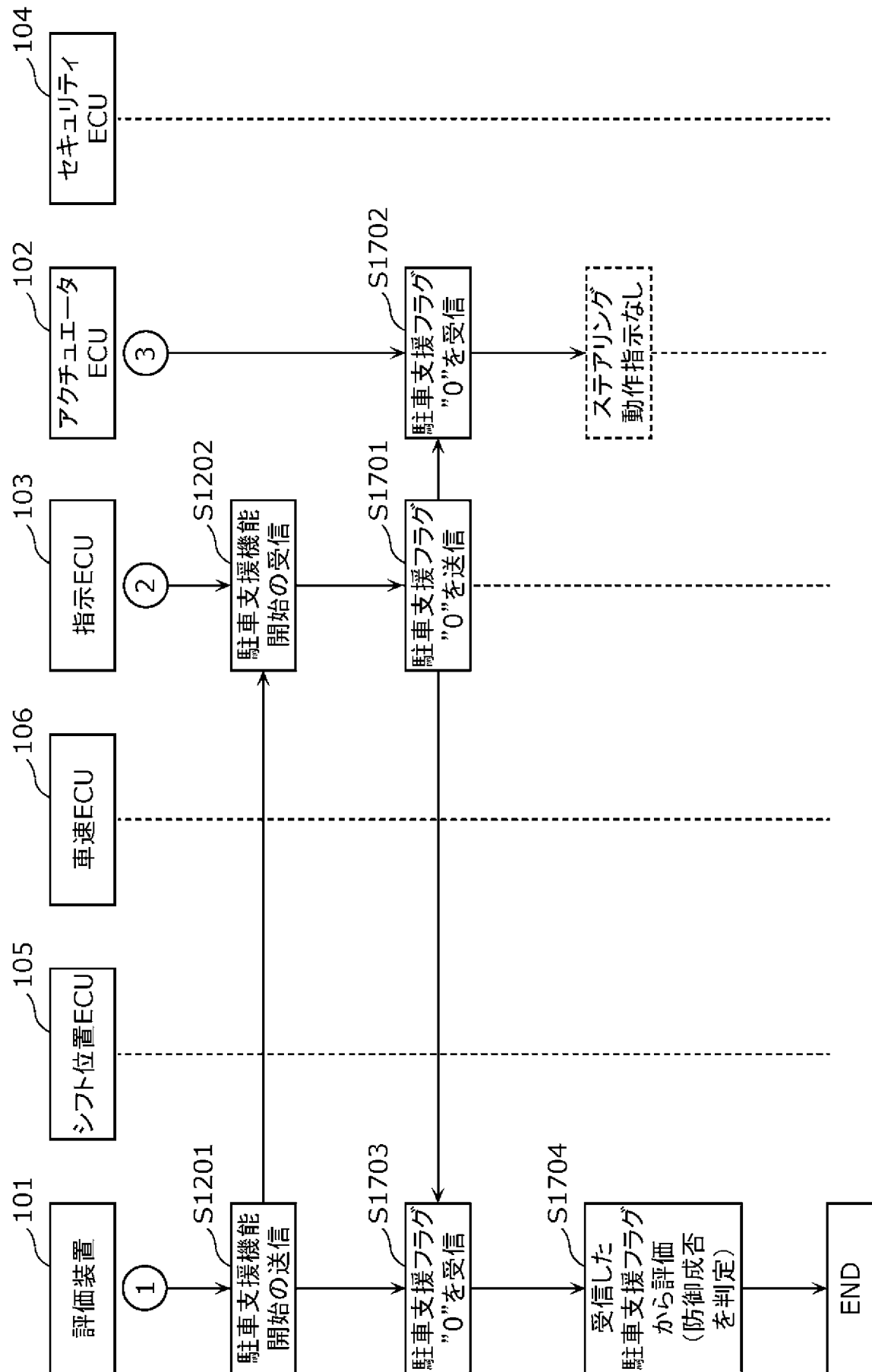


[図15]



[図16]





INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2016/004892

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/57(2013.01)i, B60R16/02(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F21/57, B60R16/02

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2016
Kokai Jitsuyo Shinan Koho	1971-2016	Toroku Jitsuyo Shinan Koho	1994-2016

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2015-114833 A (Mitsubishi Electric Corp.), 22 June 2015 (22.06.2015), paragraphs [0003], [0014] to [0026], [0044] (Family: none)	1-2, 8-12 3-7, 13
Y A	Takeshi KISHIKAWA, "Shasai Network o Hogo suru Security ECU no Teian: HW/SW Kyochō ni yoru Koshin Kano na CAN no Hogo Shuho to sono Hyōka", 2015 Symposium on Cryptography and Information Security SCIS2015 [CD-ROM] 2015 Symposium on Cryptography and Information Security Gaiyoshu, 23 January 2015 (23.01.2015), pages 1 to 8	1-2, 8-12 3-7, 13

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
05 December 2016 (05.12.16)

Date of mailing of the international search report
13 December 2016 (13.12.16)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. G06F21/57(2013.01)i, B60R16/02(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl. G06F21/57, B60R16/02

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2016年
日本国実用新案登録公報	1996-2016年
日本国登録実用新案公報	1994-2016年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y A	JP 2015-114833 A（三菱電機株式会社）2015.06.22, 段落 0003, 0014-0026, 0044（ファミリーなし）	1-2, 8-12 3-7, 13
Y A	岸川 剛, 車載ネットワークを保護するセキュリティECUの提案: HW/SW協調による更新可能なCANの保護手法とその評価, 2015年 暗号と情報セキュリティシンポジウム SCIS2015 [CD-ROM] 2015年 暗号と情報セキュリティシンポジウム概要集, 2015.01.23, pp.1-8	1-2, 8-12 3-7, 13

C欄の続きにも文献が列挙されている。

パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

05.12.2016

国際調査報告の発送日

13.12.2016

国際調査機関の名称及びあて先

日本国特許庁（ISA/J P）

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

児玉 崇晶

5S

3651

電話番号 03-3581-1101 内線 3546