

(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
2020年1月9日(09.01.2020)



(10) 国際公開番号

WO 2020/008872 A1

(51) 国際特許分類:

G06F 21/55 (2013.01) G06F 11/07 (2006.01)
B60R 16/02 (2006.01) H04L 12/28 (2006.01)

(21) 国際出願番号: PCT/JP2019/024208

(22) 国際出願日: 2019年6月19日(19.06.2019)

(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 2018-128914 2018年7月6日(06.07.2018) JP

(71) 出願人: 日立オートモティブシステムズ株式会社(HITACHI AUTOMOTIVE SYSTEMS,

LTD.) [JP/JP]; 〒3128503 茨城県ひたちなか市高場 2 5 2 0 番地 Ibaraki (JP).

(72) 発明者: 伊藤 慎悟(ITO Shingo); 〒3128503 茨城県ひたちなか市高場 2 5 2 0 番地 日立オートモティブシステムズ株式会社内 Ibaraki (JP). 芹沢 一(SERIZAWA Kazuyoshi); 〒3128503 茨城県ひたちなか市高場 2 5 2 0 番地 日立オートモティブシステムズ株式会社内 Ibaraki (JP).

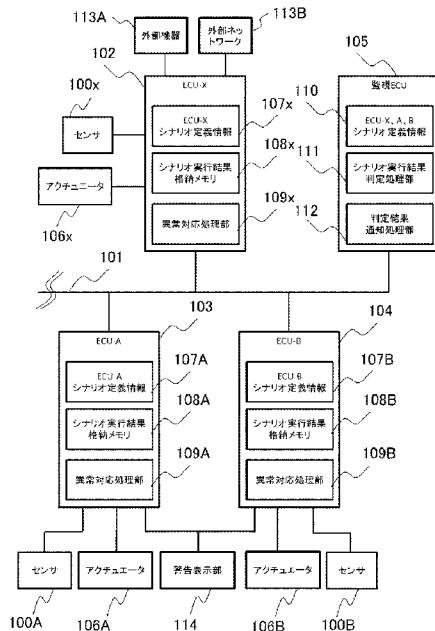
(74) 代理人: 戸田 裕二(TODA Yuji); 〒1008220 東京都千代田区丸の内一丁目 6 番 1 号 株式会社日立製作所内 Tokyo (JP).

(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,

(54) Title: ON-BOARD SECURITY SYSTEM AND ATTACK DEALING METHOD

(54) 発明の名称: 車載セキュリティシステムおよび攻撃対処方法

[図1]



100A, 100B, 100x Sensor
105 Monitoring ECU
106A, 106B, 106x Actuator
107A, 107B, 107x, 110 Scenario definition information
108A, 108B, 108x Scenario-execution-result storage memory
109A, 109B, 109x Abnormality-handling processing unit
111 Scenario-execution-result check processing unit
112 Check-result notification processing unit
113A External appliance
113B External network
114 Alert display unit

(57) Abstract: According to the present invention, even when processing for an input in the event of an attack has been executed, a response indicating that processing different from that processing has been executed is returned. A monitoring ECU 105 collects, from an ECU-X 102, information indicating the operation status of the ECU-X 102, which is an attacking target ECU, and determines that a takeover of the ECU-X 102 has occurred when there is a departure beyond a certain level in the operation status from a legitimate operation condition defined for the ECU-X 102. When a departure of the

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, JO, JP, KE, KG, KH,
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), ユーラシア (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:

- 一 国際調査報告 (条約第21条(3))

ECU-X 102 from a prescribed operation has been detected, an ECU-A 103 and an ECU-B 104 execute safety processing for inputs from the ECU-X 102 to return such responses to the inputs from the ECU-X 102 that indicate that processing has been executed as instructed by the inputs from the ECU-X 102.

(57) 要約: 攻撃時の入力に対する処理を実行した場合においても、その処理と異なる処理が実行されたという応答を返す。監視 ECU 105 は、攻撃対象 ECU である ECU-X 102 から、ECU-X 102 の動作状態を示す情報を収集し、ECU-X 102 について定められた正規の動作条件からの動作状態の一定以上の逸脱がある場合、ECU-X 102 の乗っ取りが発生したと判断し、ECU-A 103 および ECU-B 104 は、ECU-X 102 が所定の動作から逸脱したことを検知すると、ECU-X 102 からの入力に対する安全処理を実行し、ECU-X 102 からの入力に対して ECU-X 102 からの入力の指示通りに処理を実行したことを示す応答を ECU-X 102 に返す。

明 細 書

発明の名称：車載セキュリティシステムおよび攻撃対処方法

技術分野

[0001] 本発明は、車載システムの乗っ取りや、外部機器のなりすまし等のセキュリティ脅威に対処することが可能な車載セキュリティシステムおよび攻撃対処方法に関する。

背景技術

[0002] 近年、自動車は、カーナビゲーションシステムや携帯電話からのネットワーク接続によるネットワーク機能（サービス）が搭載されるなど、車載システムのネットワーク化（有線・無線）が急速に進んでいる。この車載システムのネットワーク化により、自動車に対する外部からのハッキングや車載システムの乗っ取りによる不正操作、外部機器のなりすましによるソフトウェアの改竄などのセキュリティ脅威が増大している。そのため、車載システムにおけるサイバーセキュリティ（以降、セキュリティと言う）対策が急務となっている。特に、車載システムの乗っ取りによる不正操作の脅威に対し、安全上もセキュリティ対策が必須となる。

[0003] そのような中、車載システムの電子制御装置（E l e c t r o n i c C o n t r o l U n i t : 以下、ECUと称す）には、メインのECU機能とは別にセキュリティハードウェアであるHSM（H a r d w a r e S e c u r i t y M o d u l e）の搭載が進んでいる。HSMは、暗号化や認証などのセキュリティ機能をハードウェアで実現し、同様の機能をソフトウェアで実現するよりもECUの処理負荷を少なくすることができる。また、セキュリティ機能を通常のシステムとは別に独立したハードウェアで実現するため、ソフトウェアの改竄などに対するセキュリティ脅威にも強く、車載システムに対しよりセキュアな機能（環境）を提供することができる。

[0004] しかし、HSMを用いて強固なセキュリティ機能を実装したとしても、セキュリティを突破される可能性がある。特に、車載システムの乗っ取りなど

のセキュリティ脅威では、車載システム自身が乗っ取られていることに気づかない状況も考えられる。このように強固なセキュリティ機能を実装したとしても、セキュリティを突破されたことを想定し、いかにして、セキュリティ脅威を検出し迅速に安全を確保するかが重要である。

[0005] 特許文献1では、車載ネットワーク間に設けられた監視ECUにより不正データの検知および不正データのルーティングの抑止処理を実行する技術が提案されている。例えば、各車載ネットワーク間の通信を監視するECUが設けられ、ネットワーク間の通信を監視し、不正データを検知する。そして、不正データを検知した場合、抑止処理として警告情報をネットワーク上のECUに送信するとともに、不正なデータのルーティングを禁止するメッセージを送信する技術が提案されている。

[0006] また、特許文献2では、検証センタと呼ばれる監視装置が、車載ネットワークを監視し、検証メッセージとして電子署名を用いてメッセージの改ざんや、ECUのなりすましを検出する技術が提案されている。

先行技術文献

特許文献

[0007] 特許文献1：特開2013-131907号公報

特許文献2：特開2014-138380号公報

発明の概要

発明が解決しようとする課題

[0008] しかしながら、ECUへのハッキングやソフトウェアを不正に改竄するなどして車載システムを乗っ取る場合、異常な状態に陥ることや、異常な制御値および異常なメッセージIDを入出力することなく、不正操作を行うため、検出が困難である。なお、メッセージIDとは、メッセージの種別を識別するためのIDである。

[0009] また、上記特許文献1に開示された技術では、データが不正な状態でなければ異常を検知できず、例えばECUが乗っ取られた場合、正常なデータを

使用されていればECUが乗っ取られていたとしても不正な状態と検知することができず、異常に対して適切な対応処理ができなかった。さらに、抑止処理として警告情報を送信したとしても、不正な状態のECUを介する可能性があるため、警告に対する処理が正しく実行できないこともあった。

[0010] また、上記特許文献2に開示された技術では、不正データや外部のなりすましの検出はできるが、ECUの乗っ取りなど、データ自体に不正がない場合の異常を検出することができず、異常に対して適切な対応処理ができなかった。さらに、なりすましたECUを介してネットワークが使用されるので、異常に対する処理が正しく実行できない可能性もあった。

[0011] また、上記特許文献1、2に開示された技術では、不正データや外部のなりすましを検知し、脅威に対して適切な対応処理を実行した時に、その対応処理を適切に実行したことが攻撃者に知られることがあるため、その対応処理に対して攻撃者からの更なる攻撃や別の手段による新たな攻撃を招く可能性もあった。

[0012] 本発明は、上記事情に鑑みなされたものであり、その目的は、攻撃時の入力に対する処理を実行した場合においても、その処理と異なる処理が実行されたという応答を返すことが可能な車載セキュリティシステムおよび攻撃対処方法を提供することにある。

課題を解決するための手段

[0013] 上記目的を達成するため、第1の観点に係る車載セキュリティシステムは、第1電子制御装置と、前記第1電子制御装置と通信可能な第2電子制御装置とを備え、前記第2電子制御装置は、前記第1電子制御装置からの入力に対する第1処理を実行し、前記入力に対して前記第1処理と異なる第2処理を実行したことを示す応答を前記第1電子制御装置に返す。

発明の効果

[0014] 本発明によれば、攻撃時の入力に対する処理を実行した場合においても、その処理と異なる処理が実行されたという応答を返すことができる。

図面の簡単な説明

[0015] [図1]図1は、第1実施形態に係る車載セキュリティシステムの構成を示すブロック図である。

[図2]図2は、図1のシナリオ定義情報の構成例を示す図である。

[図3]図3は、第1実施形態に係る車載セキュリティシステムの動作例を示すブロック図である。

[図4]図4は、第1実施形態に係る車載セキュリティシステムの異常判定処理を示すフローチャートである。

[図5]図5は、第1実施形態に係る車載セキュリティシステムのシナリオ実行結果判定処理を示すフローチャートである。

[図6]図6は、第1実施形態に係る車載セキュリティシステムの異常対応処理の内容を示すブロック図である。

[図7]図7は、第1実施形態に係る車載セキュリティシステムの異常対応処理を示すフローチャートである。

[図8]図8は、図7の機能レベル高処理を示すフローチャートである。

[図9]図9は、図7の機能レベル中処理および機能レベル低処理を示すフローチャートである。

[図10]図10は、第2実施形態に係る車載セキュリティシステムの構成を示すブロック図である。

[図11]図11は、第3実施形態に係る車載セキュリティシステムの異常対応処理を示すフローチャートである。

[図12]図12は、第3実施形態に係る車載セキュリティシステムの構成を示すブロック図である。

[図13]図13は、第4実施形態に係る車載セキュリティシステムに用いられるECUのハードウェア構成を示すブロック図である。

発明を実施するための形態

[0016] 実施形態について、図面を参照して説明する。なお、以下に説明する実施形態は特許請求の範囲に係る発明を限定するものではなく、また、実施形態の中で説明されている諸要素及びその組み合わせの全てが発明の解決手段に

必須であるとは限らない。

[0017] 図1は、第1実施形態に係る車載セキュリティシステムの構成を示すブロック図である。

図1において、この車載セキュリティシステムには、ECU-X102、ECU-A103、ECU-B104および監視ECU105が設けられている。ECU-X102、ECU-A103、ECU-B104および監視ECU105は、車両に搭載することができる。この時、ECU-X102、ECU-A103、ECU-B104および監視ECU105は、車載ネットワーク101を介して互いに接続することができる。車載ネットワーク101の例としては、CAN (Control Area Network)、FlexRay、LIN (Local Interconnect Network)、Ethernet (登録商標) 等である。

[0018] また、ECU-X102は、外部機器113Aおよび外部ネットワーク113Bに接続されている。外部機器113Aとの接続には、OBD (On-Board Diagnostics) またはEthernetを用いることができる。外部ネットワーク113Bは、インターネットなどのWAN (Wide Area Network) であってもよいし、WiFiなどのLAN (Local Area Network) であってもよいし、WANとLANが混在していてもよい。図1では、ECU-X102は、外部機器113Aおよび外部ネットワーク113Bに接続されている例を示したが、外部機器113Aおよび外部ネットワーク113Bのいずれか一方にのみ接続されていてもよい。

[0019] ここで、外部機器113Aおよび外部ネットワーク113Bに接続されているECU-X102は、外部ネットワーク113Bを介した乗っ取りまたは外部機器113Aのなりすましによる攻撃対象ECUとして扱うことができる。

[0020] ECU-X102、ECU-A103およびECU-B104は、車両の車載機器を電子制御する。車載機器は、例えば、動力装置、操舵装置、制動

装置または変速装置である。車両の動力装置として、エンジンまたは電動機を用いることができる。車載機器は、ヘッドライト、パワーウィンドウ、ドアロック、電動シート、インストルメントパネルなどであってもよい。

[0021] ECU-X102は、センサ100xおよびアクチュエータ106xに接続されている。ECU-A103は、センサ100Aおよびアクチュエータ106Aに接続されている。ECU-B104は、センサ100Bおよびアクチュエータ106Bに接続されている。アクチュエータ106x、106A、106Bは、例えば、アクセル、ブレーキ、ステアリングを操作するためのアクチュエータである。また、ECU-A103およびECU-B104は、警告表示部114に接続されている。警告表示部114は、外部ネットワーク113Bを介した乗っ取りまたは外部機器113Aのなりすましによる異常発生時に警告表示を行う。この時、ECU-A103およびECU-B104は、外部機器113Aおよび外部ネットワーク113Bに接続されたECU-X102を含まない通信ネットワークを介して警告表示部114と通信する。

[0022] 監視ECU105は、ECU-X102、ECU-A103およびECU-B104に異常がないかを監視する。監視ECU105のセキュリティレベルは、ECU-X102、ECU-A103およびECU-B104のセキュリティレベルより高くすることができる。この時、監視ECU105は、HSMのようなセキュリティ機能を持っていてもよいし、外部ネットワークと直接接続されないようにしてもよい。

[0023] 監視ECU105は、車載ネットワーク101を介し、攻撃対象ECUであるECU-X102から、ECU-X102の動作状態を示す情報を収集する。そして、監視ECU105は、ECU-X102から収集したECU-X102の動作状態を示す情報に基づいて、ECU-X102の動作状態を監視する。この時、監視ECU105は、ECU-X102について定められた正規の動作条件からの動作状態の一定以上の逸脱がある場合、ECU-X102の乗っ取りが発生したと判断することができる。

[0024] さらに、監視ECU105は、車載ネットワーク101を介し、ECU-A103およびECU-B104から、ECU-A103およびECU-B104の動作状態を示す情報を収集する。そして、監視ECU105は、ECU-A103およびECU-B104から収集したECU-A103およびECU-B104の動作状態を示す情報に基づいて、ECU-A103およびECU-B104の動作状態を監視する。この時、監視ECU105は、例えば、ECU-A103について定められた正規の動作条件からの動作状態の一定以上の逸脱がある場合、ECU-A103の動作状態の一定以上の逸脱がECU-A103とECU-X102との通信に起因しているかどうかを判断する。そして、ECU-A103とECU-X102との通信に起因してECU-A103の動作状態の一定以上の逸脱がある場合、ECU-X102の乗っ取りが発生したと判断することができる。

[0025] ECU-A103およびECU-B104は、ECU-X102が所定の動作から逸脱したことを検知すると、ECU-X102からの入力に対する第1処理を実行する。また、ECU-A103およびECU-B104は、ECU-X102からの入力に対して第1処理と異なる第2処理を実行したことを示す応答をECU-X102に返す。この時、ECU-A103およびECU-B104は、ECU-X102が所定の動作から逸脱したことを示す検知結果を監視ECU105から取得することができる。ECU-A103およびECU-B104が自ら、ECU-X102の所定の動作からの逸脱を検知するようにしてもよい。この時、監視ECU105はなくてもよい。

[0026] 第1処理は、ECU-X102からの入力に対する安全処理とすることができる。この安全処理は、ECU-X102への攻撃時の指示に対してフェールセーフ側の処理とすることができる。第2処理は、ECU-X102からの入力の指示通りに実行した処理とすることができる。

[0027] ここで、ECU-X102に攻撃があった時に、ECU-A103およびECU-B104は、ECU-X102からの入力に対する安全処理を実行

する一方で、ECU-X102には、ECU-X102からの入力の指示通りに実行したことを示す応答を返す。これにより、ECU-X102に攻撃があった場合においても、ECU-A103およびECU-B104は、その攻撃に対して自らの安全性を確保しつつ、攻撃者の指示通りに攻撃が実行されているように攻撃者に見せかけることができる。この結果、攻撃に対して安全処理が行われたことを攻撃者に知られるのを防止することができ、その安全処理に対して攻撃者からの更なる攻撃や別の手段による新たな攻撃を招くのを防止することができる。

[0028] なお、ECU-A103およびECU-B104は、ECU-X102からの入力の指示通りに実行したことを示す応答をECU-X102に返す時に、攻撃者を探索する探索プログラムをその応答に付加するようにしてもよい。この探索プログラムは、ECU-X102に取り込まれると、攻撃者を逆探知することにより、攻撃者を特定することができる。そして、探索プログラムは、攻撃者を特定する情報をECU-A103およびECU-B104に通知することができる。

[0029] 以下、ECU-X102、ECU-A103、ECU-B104および監視ECU105の構成例について具体的に説明する。

図1において、ECU-X102は、ECU-Xシナリオ定義情報107xを保持し、ECU-A103は、ECU-Aシナリオ定義情報107Aを保持し、ECU-B104は、ECU-Bシナリオ定義情報107Bを保持する。ECU-Xシナリオ定義情報107xには、ECU-X102が実行する正規の一連の動作を示す機能シーケンス情報が設定される。ECU-Aシナリオ定義情報107Aには、ECU-A103が実行する正規の一連の動作を示す機能シーケンス情報が設定される。ECU-Bシナリオ定義情報107Bには、ECU-B104が実行する正規の一連の動作を示す機能シーケンス情報が設定される。

[0030] 機能シーケンス情報は、ECU-X102、ECU-A103およびECU-B104のそれぞれの機能を実行するための正規の処理順番、実行条件

および実行タイミングを実行手順として含む。例えば、ECU-X102がアクチュエータ106xに対して“機能A”を正常に実行させる場合、ECU-X102は、処理1⇒処理4⇒処理5⇒機能Aという一連の動作を実行するものとする。ECU-Xシナリオ定義情報107xには、機能シーケンス情報として、“処理1⇒処理4⇒処理5⇒機能Aを実行”という情報が設定される。

[0031] また、機能シーケンス情報は、ECU-X102、ECU-A103およびECU-B104が機能を実行するために必要な制御値の情報や通信の情報を含むことができる。制御値の情報は、制御値の項目、制御値の変化量または範囲、制御値の上下限值および制御値の更新タイミングである。通信の情報は、通信項目、メッセージID、メッセージのデータ長、更新タイミングおよび更新頻度である。

[0032] また、ECU-X102、ECU-A103およびECU-B104には、シナリオ実行結果格納メモリ108x、108A、108Bがそれぞれ設けられている。各シナリオ実行結果格納メモリ108x、108A、108Bには、ECU-X102、ECU-A103およびECU-B104のそれぞれ自身のECU-Xシナリオ定義情報107x、ECU-Aシナリオ定義情報107AおよびECU-Bシナリオ定義情報107Bで定義された機能シーケンスの実行結果に関する情報を格納する。さらに、各シナリオ実行結果格納メモリ108x、108A、108Bには、互いに関係するECU-X102、ECU-A103およびECU-B104のそれぞれのECU-Xシナリオ定義情報107x、ECU-Aシナリオ定義情報107AおよびECU-Bシナリオ定義情報107Bで定義された機能シーケンスの実行結果に関する情報を格納する。

[0033] 例えば、シナリオ実行結果格納メモリ108xには、ECU-X102のシナリオの実行結果やタイミング、制御値の中間生成値の情報だけでなく、ECU-X102が機能を実行するために行った他のECU-A103およびECU-B104との送受信の通信データ、ECU-X102の処理に関

係する他のECU-A103およびECU-B104がどのシナリオ定義情報を実行し、その際にECU-A103およびECU-B104が行った送受信の通信データなどを格納することができる。

[0034] 各シナリオ実行結果格納メモリ108x、108A、108Bは、ECU-X102、ECU-A103、ECU-B104および監視ECU105が共通でアクセスできるように外部の共有メモリを用いるようにしてもよい。この共有メモリは、例えば、EEPROM (Electrically Erasable Programmable Read-Only Memory) 等の不揮発メモリを使用することができる。外部の共有メモリを使用できない場合は、CANやFlexRay通信等の車載ネットワーク通信を用いて、監視ECU105に全ての情報を集めるなど、ECU-X102、ECU-A103、ECU-B104および監視ECU105のうちのどれか一つのECUがまとめて情報を持つような構成としてもよい。

[0035] さらに、ECU-X102、ECU-A103およびECU-B104には、異常対応処理部109x、109A、109Bがそれぞれ設けられている。各異常対応処理部109x、109A、109Bは、周辺のECUが所定の動作から逸脱したことを検知すると、その周辺のECUからの入力に対する安全処理を自身のECU上で実行する。また、各異常対応処理部109x、109A、109Bは、周辺のECUからの入力に対して、その周辺のECUからの入力の指示通りに処理を実行したことを示す応答をその周辺のECUに返す。この時、各異常対応処理部109x、109A、109Bは、周辺のECUが所定の動作から逸脱したことを示す検知結果を監視ECU105から取得することができる。

[0036] 例えば、各異常対応処理部109x、109A、109Bは、周辺のECUの実行手順に異常があった場合は、自身のECUに対しては、正規の実行手順で機能を再実行し継続して動作させることができる。一方、各異常対応処理部109x、109A、109Bは、周辺のECUに対しては、異常な実行手順で機能が実行されたことを示す応答を返し、自身のECU上で警告

表示することができる。

[0037] また、各異常対応処理部109x、109A、109Bは、周辺のECUの制御値に異常があれば、自身のECUに対しては制御値を初期値に戻して動作させることができる。一方、各異常対応処理部109x、109A、109Bは、周辺のECUに対しては、異常な制御値で機能が実行されたことを示す応答を返し、自身のECU上で警告表示することができる。

[0038] さらに、各異常対応処理部109x、109A、109Bは、通信項目に異常があれば、自身のECUに対しては該当の通信を遮断することができる。一方、各異常対応処理部109x、109A、109Bは、周辺のECUに対しては、通信項目に異常がある状態で機能が実行されたことを示す応答を返し、自身のECU上で警告表示することができる。

[0039] 監視ECU105は、ECU-X、A、Bシナリオ定義情報110を保持する。ECU-X、A、Bシナリオ定義情報110は、ECU-Xシナリオ定義情報107x、ECU-Aシナリオ定義情報107AおよびECU-Bシナリオ定義情報107Bを含むことができる。

[0040] また、監視ECU105には、シナリオ実行結果判定処理部111が設けられている。シナリオ実行結果判定処理部111は、ECU-X102、ECU-A103およびECU-B104から、ECU-X102、ECU-A103およびECU-B104の動作状態を示す情報を収集する。そして、ECU-X102、ECU-A103およびECU-B104のECU-X、A、Bシナリオ定義情報110と、ECU-X102、ECU-A103およびECU-B104の動作状態を示す情報とを比較することにより、ECU-X102、ECU-A103およびECU-B104について、外部からの乗っ取りや、外部機器のなりすましによる不正操作等がないかを判定する。

[0041] 監視ECU105が、ECU-X102、ECU-A103およびECU-B104から情報を取得する方法としては、例えば、EEPROM等の外部メモリがあれば、その外部メモリから取得することができる。外部メモリ

がない場合は、監視ECU105とECU-X102、ECU-A103およびECU-B104との間のCANやFlexRay通信などの車載ネットワーク通信を用いることができる。

[0042] その際、監視のための車載ネットワーク通信では、情報を送信するための専用のメッセージを用いるなど、通常的車載ネットワーク通信とは別に用意することができる。また、監視のための情報を取得するタイミングは、車載システムに合わせた任意のタイミングに設定することができる。例えば、特定の値が変化したタイミングや、異常と判断された場合に安全に異常処理を実行できるタイミングで情報を取得することができる。

[0043] さらに、監視ECU105には、判定結果通知処理部112が設けられている。判定結果通知処理部112は、ECU-X、A、Bシナリオ定義情報110で定義された機能シーケンス通りにECU-X102、ECU-A103およびECU-B104の処理が実行されたかどうかを示す判定結果をECU-X102、ECU-A103およびECU-B104に通知する。

[0044] この時、監視ECU105は、例えば、判定結果を通知するメッセージをECU-X102、ECU-A103およびECU-B104に送信するようにしてもよい。あるいは、監視ECU105は、ECU-X102、ECU-A103およびECU-B104からアクセス可能な共通メモリに判定結果を格納するようにしてもよい。

[0045] 図2は、図1のシナリオ定義情報の構成例を示す図である。

図2において、ECU-Xシナリオ定義情報107x、ECU-Aシナリオ定義情報107AおよびECU-Bシナリオ定義情報107Bは、ECU-X102、ECU-A103、ECU-B104の乗っ取りまたは外部機器のなりすましによる不正操作を監視ECU105が検知するために使用することができる。

[0046] ECU-Xシナリオ定義情報107x、ECU-Aシナリオ定義情報107AおよびECU-Bシナリオ定義情報107Bのそれぞれは大きく分けて、機能の実行手順115、ECUで扱う重要な制御値の情報116およびE

C Uとの通信項目の情報 1 1 7 という 3 つの情報で構成することができる。

[0047] 機能の実行手順 1 1 5 は、特定の機能を実行するための処理の順番を示す情報、機能を実行する条件および機能を実行するタイミングを示す情報を含むことができる。特定の機能を実行するための処理の順番を示す情報は、例えば、実行完了フラグである。機能を実行する条件は、例えば、機能が実行できるステータスの情報である。機能を実行するタイミングは、例えば実行周期である。

[0048] 監視 E C U 1 0 5 は、正規の手順で特定の機能が実行されているか確認するために機能の実行手順 1 1 5 を用いることができる。例えば、機能 A を実行するための手順が“処理 1 ⇒処理 3 ⇒処理 5”の場合、機能の実行手順 1 1 5 は、“処理 1 ⇒処理 3 ⇒処理 5”の順番を示す実行完了フラグを変数で定義することができる。特定の機能を実行するための条件があれば、その実行条件として、例えば、“ステータスがアイドル状態の時”などの情報を定義することができる。特定の機能を周期的に実行するのであれば、実行周期情報として、例えば、“1 0 0 μ s e c 毎に機能を実行する”などの情報を定義することができる。

[0049] 機能の実行手順 1 1 5 を定義することにより、E C U や外部から実行した機能が正しい条件下で実行されているか、監視 E C U 1 0 5 や監視対象以外の他の E C U から確認および監視することができる。

[0050] E C U で扱う重要な制御値の情報 1 1 6 は、E C U - X 1 0 2、E C U - A 1 0 3 および E C U - B 1 0 4 が特定の機能を実行する際に取り得る、E C U - X 1 0 2、E C U - A 1 0 3 および E C U - B 1 0 4 が扱う制御値の項目、制御項目の制御値の変化に対する適正值、変化量（範囲）や上下限值および制御値が更新されるタイミング情報を含むことができる。

[0051] 例えば、制御値は、E C U - X 1 0 2、E C U - A 1 0 3 および E C U - B 1 0 4 がそれぞれ制御するアクチュエータ 1 0 6 x、1 0 6 A、1 0 6 B やセンサ 1 0 0 x、1 0 0 A、1 0 0 B を制御するための値である。制御値は、不正な操作で改竄された場合、車載システムの安全上問題になるような

重要な制御項目の値である。例えば、モータ制御に使用する電流値やバッテリー制御に使用する電圧値などの実際に出力される値や、他のECUに送信される値である。

[0052] ECUで扱う重要な制御値の情報116は、当該ECUが正しく動いているか外部から確認および監視が可能な情報で構成することができる。また、ECUで扱う重要な制御値の情報116は、通常、外部から改竄されない限り変更されない値、具体的には、ソフトウェアのバージョン情報なども含むことができる。また、制御値が更新されるタイミング情報は、制御値の更新周期情報、例えば100 μ s e c毎などの情報で構成することができる。

[0053] 各ECUとの通信項目の情報117は、各ECUと行う通信項目の情報で、例えば、メッセージIDや通信データ長、それらの情報の更新タイミングや更新間隔を含むことができる。各ECUとの通信項目の情報117は、例えば、メッセージID毎の通信周期情報などの外部から監視が可能な情報で構成することができる。

[0054] 上述した3つの情報でECU-X、A、Bシナリオ定義情報110を構成することにより、ECU-X102、ECU-A103およびECU-B104の機能が正しく動作しているか判定するために、監視ECU105が何を監視すればよいかを判断することが可能となる。監視ECU105は、ECU-X、A、Bシナリオ定義情報110で定義された情報を確認および監視することにより、ECU-X102、ECU-A103およびECU-B104に対して乗っ取りや外部機器のなりすましによる不正操作がされていないかを判定することができる。

[0055] 図3は、第1実施形態に係る車載セキュリティシステムの動作例を示すブロック図である。なお、図3では、ECU-X102が攻撃対象ECUであるものとする。そして、ECU-X102が所定の動作から逸脱したことを監視ECU105が検知し、ECU-A103およびECU-B104は、監視ECU105の検知結果に基づいてECU-X102からの入力に対する処理を実行する場合を例にとる。

- [0056] 図3において、ECU-X102が攻撃対象ECUに設定されると、ECU-A103およびECU-B104のそれぞれは、ECU-A、Xシナリオ定義情報117AおよびECU-B、Xシナリオ定義情報117Bとして、自身のECU-Aシナリオ定義情報107AおよびECU-Bシナリオ定義情報107Bを保持するだけでなく、ECU-X102のECU-Xシナリオ定義情報107xも保持する。
- [0057] ECU-A103およびECU-B104は、ECU-X102が攻撃対象ECUに設定された時に、ECU-X102のECU-Xシナリオ定義情報107xを監視ECU105から取得するようにしてもよいし、ECU-Xシナリオ定義情報107xを予め保持するようにししてもよい。
- [0058] ECU-X102は、外部機器113Aまたは外部ネットワーク113Bから攻撃を受ける(P1)。ECU-A103、ECU-B104および監視ECU105は、ECU-X102の動作状態を示す情報をECU-X102から取得し記録する(P2~P4)。この時、ECU-A103、ECU-B104および監視ECU105は、ECU-X102のECU-Xシナリオ定義情報107xを参照することにより、攻撃対象ECUに設定されたECU-X102のどの情報を取得すればよいか判別することができる。
- [0059] 次に、監視ECU105は、ECU-A103の動作状態を示す情報をECU-A103から収集し(P5)、ECU-B104の動作状態を示す情報をECU-B104から収集する(P6)。そして、監視ECU105は、ECU-X102のECU-Xシナリオ定義情報107xと、ECU-X102の動作状態を示す情報とを比較することにより、ECU-X102について、外部からの乗っ取りや、外部機器のなりすましによる不正操作等がないかを判定する。また、監視ECU105は、ECU-A103のECU-Aシナリオ定義情報107Aと、ECU-A103の動作状態を示す情報とを比較することにより、ECU-X102との通信に起因するECU-A103の不正操作等がないかを判定する。さらに、監視ECU105は、ECU-B104のECU-Bシナリオ定義情報107Bと、ECU-B10

4の動作状態を示す情報とを比較することにより、ECU-X102との通信に起因するECU-B104の不正操作等がないかを判定する。

[0060] そして、監視ECU105は、ECU-X102の不正操作等があるか、またはECU-X102との通信に起因するECU-A103の不正操作等があるか、またはECU-X102との通信に起因するECU-B104の不正操作等があると判定した場合、ECU-X102に異常があると判定し、その判定結果をECU-A103およびECU-B104に通知する（P7、P8）。

[0061] ECU-A103およびECU-B104は、ECU-X102の異常の判定結果を監視ECU105から受け取ると、ECU-X102から入力されたメッセージや制御値などに対する安全処理を自身のECU上で実行する。また、ECU-A103およびECU-B104は、ECU-X102から入力されたメッセージや制御値などに対して、ECU-X102から入力されたメッセージや制御値の通りに処理を実行したことを示す応答をECU-X102に返す（P9、P10）。さらに、ECU-A103およびECU-B104は、ECU-X102から入力されたメッセージや制御値などに対して、警告表示部114上で警告表示する（P11、P12）。

[0062] これにより、ECU-X102に攻撃があった場合においても、ECU-A103およびECU-B104は、ECU-X102の攻撃に対してECU-A103およびECU-B104の安全性を確保しつつ、攻撃者の指示通りに攻撃が実行されているように攻撃者に見せかけることができる。

[0063] また、ECU-X102、ECU-A103およびECU-B104のECU-X、A、Bシナリオ定義情報110と、ECU-X102、ECU-A103およびECU-B104の動作状態を示す情報とを比較することにより、異常な状態に陥ることや、異常な制御値または異常なメッセージIDを入出力することなく、ECU-X102の不正操作が行われた場合においても、その不正操作を検知することができる。このため、HSMを持たないECU-X102、ECU-A103、ECU-B104および監視ECU

105を使用する車載システムであっても、車載システムの乗っ取りや、外部機器のなりすまし等のセキュリティ脅威に対処することができる。

[0064] また、攻撃対象として設定されたECU-X102について、外部からの乗っ取りや、外部機器のなりすましによる不正操作等がないかを監視するために、ECU-A103、ECU-B104および監視ECU105は、ECU-X102のECU-Xシナリオ定義情報107xを保持すればよい。このため、ECU-X102、ECU-A103およびECU-B104の処理能力が低い等の理由でソフトウェアの機能追加が難しい場合においても、車載システムの乗っ取りや、外部機器のなりすまし等のセキュリティ脅威に対するセキュリティを保障することができる。

[0065] ここで、監視ECU105は、攻撃対象として設定されたECU-X102のECU-Xシナリオ定義情報107xだけでなく、ECU-Aシナリオ定義情報107AおよびECU-Bシナリオ定義情報107Bも保持している。これにより、監視ECU105は、攻撃対象として設定されたECU-X102の情報だけでなく、ECU-A103およびECU-B104の情報を加味することができ、攻撃対象として設定されたECU-X102が乗っ取られていないか、外部機器から不正操作されていないかをより高い精度で判定することができる。

[0066] 例えば、攻撃者がECU-X102を経由してECU-A103を不正操作するものとする。この時、監視ECU105は、ECU-A103の動作状態を示す情報をECU-A103から取得し、ECU-A103のECU-Aシナリオ定義情報107Aと、ECU-A103の動作状態を示す情報とを比較することにより、ECU-X102との通信に起因するECU-A103の不正操作等がないかを判定することができる。

[0067] 図4は、第1実施形態に係る車載セキュリティシステムの異常判定処理を示すフローチャートである。

図4のステップS101において、監視ECU105は、攻撃対象として設定されたECU-X102の異常判定処理を開始すると、ステップS10

2において、ECU-X102からECU-X102の動作状態を示す情報を取得する。

[0068] 次に、ステップS103において、監視ECU105は、ECU-A103からECU-A103の動作状態を示す情報を取得する。次に、ステップS104において、監視ECU105は、ECU-B104からECU-B104の動作状態を示す情報を取得する。

[0069] 次に、ステップS105において、監視ECU105は、ステップS102～S104で取得したECU-X102、ECU-A103およびECU-B104の動作状態を示す情報と、ECU-X、A、Bシナリオ定義情報110を比較する。そして、監視ECU105は、ステップS102～S104で取得したECU-X102、ECU-A103およびECU-B104の動作状態のいずれかを示す情報が、ECU-X、A、Bシナリオ定義情報110の内容から一定以上逸脱している場合、ECU-X102に異常がある判定する。

[0070] 次に、ステップS106において、監視ECU105は、ステップS105で得られた判定結果をECU-A103およびECU-B104に通知する。その後、ステップS107において、ECU-X102の異常判定処理を終了する。

[0071] なお、監視ECU105によるECU-X102の異常判定は、任意のタイミングで実行が可能だが、乗っ取りや外部機器からのなりすましによる不正操作に対して、安全に対処できるタイミングで実行することが望ましい。例えば、基準となる特定の値が変化したタイミング、機能を実施する制御周期、または機能安全のFTTI (Fault Tolerant Time Interval) などのタイミングで実行することができる。基本的には、車載システムの処理負荷に影響が少なく、かつセキュリティが保障できるタイミングで実行することが望ましい。

[0072] 図5は、第1実施形態に係る車載セキュリティシステムのシナリオ実行結果判定処理を示すフローチャートである。なお、図5の処理は、図4のステ

ップS 1 0 5の処理で実行することができる。

図5のステップS 2 0 1において、シナリオ実行結果判定処理部1 1 1は、シナリオ実行結果判定処理を開始すると、ステップS 2 0 2において、実行手順の確認を行う。ここで、シナリオ実行結果判定処理部1 1 1は、E C U-X 1 0 2、E C U-A 1 0 3およびE C U-B 1 0 4から取得したE C U-X 1 0 2、E C U-A 1 0 3およびE C U-B 1 0 4の動作時の実行手順情報と、E C U-X、A、Bシナリオ定義情報1 1 0で定義された機能の実行手順1 1 5を比較する。

[0073] そして、シナリオ実行結果判定処理部1 1 1は、E C U-Xシナリオ定義情報1 0 7 xの機能の実行手順1 1 5に登録された実行手順通りにE C U-X 1 0 2の機能が実行されているかを確認することにより、E C U-X 1 0 2に異常がないかを判定する。また、シナリオ実行結果判定処理部1 1 1は、E C U-X 1 0 2からE C U-A 1 0 3に送信された送信データに基づいてE C U-Aシナリオ定義情報1 0 7 Aの機能の実行手順1 1 5に登録された実行手順通りにE C U-A 1 0 3の機能が実行されているかを確認することにより、E C U-X 1 0 2に異常がないかを判定する。さらに、シナリオ実行結果判定処理部1 1 1は、E C U-X 1 0 2からE C U-B 1 0 4に送信された送信データに基づいてE C U-Bシナリオ定義情報1 0 7 Bの機能の実行手順1 1 5に登録された実行手順通りにE C U-B 1 0 4の機能が実行されているかを確認することにより、E C U-X 1 0 2に異常がないかを判定する。

[0074] シナリオ実行結果判定処理部1 1 1は、E C U-X 1 0 2、E C U-A 1 0 3、E C U-B 1 0 4のいずれかの機能の実行が、E C U-X、A、Bシナリオ定義情報1 1 0の機能の実行手順1 1 5に登録された実行手順から一定以上逸脱している場合、E C U-X 1 0 2に異常があると判定することができる。

[0075] E C U-X、A、Bシナリオ定義情報1 1 0の機能の実行手順1 1 5に登録された実行手順通りにE C U-X 1 0 2、E C U-A 1 0 3、E C U-B

104のそれぞれの機能が実行されているかどうかを判断するために、例えば、機能の実行手順115で定義された実行可否を示す実行完了フラグが全て揃っているか、機能の実行手順115で定義された機能を実行する際のステータスは正しいか、機能の実行手順115で定義された指定の周期で実行しているかを判定することができる。

[0076] 次に、ステップS203において、シナリオ実行結果判定処理部111は、制御値の変化の確認を行う。ここで、シナリオ実行結果判定処理部111は、ECU-X102、ECU-A103およびECU-B104から取得したECU-X102、ECU-A103およびECU-B104の動作時の制御値情報と、ECU-X、A、Bシナリオ定義情報110で定義されたECUで扱う重要な制御値の情報116を比較し、ECU-X102に異常がないかを判定する。これらの比較対象の具体例は、制御値の項目、制御項目の制御値の変化に対する適正值、変化量（範囲）や上下限值、制御値が更新されるタイミング情報である。

[0077] シナリオ実行結果判定処理部111は、ECU-X102から取得した制御値情報が、ECU-Xシナリオ定義情報107xに登録されたECUで扱う重要な制御値の情報116から一定以上逸脱している場合、ECU-X102に異常がある判定することができる。また、シナリオ実行結果判定処理部111は、ECU-A103から取得した制御値情報が、ECU-Aシナリオ定義情報107Aに登録されたECUで扱う重要な制御値の情報116から一定以上逸脱している場合、その逸脱がECU-X102からECU-A103に送信された送信データに起因する場合、ECU-X102に異常がある判定することができる。さらに、シナリオ実行結果判定処理部111は、ECU-B104から取得した制御値情報が、ECU-Bシナリオ定義情報107Bに登録されたECUで扱う重要な制御値の情報116から一定以上逸脱している場合、その逸脱がECU-X102からECU-A104に送信された送信データに起因する場合、ECU-X102に異常がある判定することができる。

- [0078] 制御値情報の比較では、例えば、E C U－Xシナリオ定義情報1 0 7 xのE C Uで扱う重要な制御値の情報1 1 6で指定している値と、E C U－X 1 0 2の実際の制御値がそれぞれ一致しているか、E C U－X 1 0の制御値が一定時間上限値に張り付いていないか、E C U－X 1 0 2の制御値の変化量が適切かを判定することができる。
- [0079] 具体的には、E C U－X 1 0 2の制御値が通常1 0ずつ増加する場合、その制御値がその通り増加しているか、2周期に1回更新される制御値の場合、その制御値が指定の周期で更新されているかを判定することができる。
- [0080] 次に、ステップS 2 0 4において、シナリオ実行結果判定処理部1 1 1は、通信項目の変化の確認を行う。ここで、シナリオ実行結果判定処理部1 1 1は、E C U－X 1 0 2、E C U－A 1 0 3およびE C U－B 1 0 4から取得したE C U－X 1 0 2の通信項目の内容と、E C U－X、A、Bシナリオ定義情報1 1 0で定義された各E C Uとの通信項目の情報1 1 7を比較し、E C U－X 1 0 2に異常がないかを判定する。
- [0081] シナリオ実行結果判定処理部1 1 1は、E C U－X 1 0 2、E C U－A 1 0 3およびE C U－B 1 0 4から取得したE C U－X 1 0 2の通信項目の内容が、E C U－X、A、Bシナリオ定義情報1 1 0に登録された各E C Uとの通信項目の情報1 1 7から一定以上逸脱している場合、E C U－X 1 0 2に異常がある判定することができる。
- [0082] 通信項目の情報の比較では、例えば、特定のメッセージIDの通信回数が増えていないか、同じデータが続いていないか、データ長は適切か、指定の周期で通信を実施しているかなどを判定する。
- [0083] 次に、ステップS 2 0 5において、シナリオ実行結果判定処理部1 1 1は、ステップS 2 0 2～ステップS 2 0 4で確認した結果に異常がないか判定する。もし、異常がある場合は、ステップS 2 0 6において、異常判定結果を格納する。ステップS 2 0 2～ステップS 2 0 4の確認で異常がない場合は、ステップS 2 0 7でシナリオ実行結果判定処理を終了する。
- [0084] E C U－A 1 0 3およびE C U－B 1 0 4が、図4のステップS 1 0 5で

得られた判定結果を監視ECU105から受信すると、図1の異常対応処理部109A、109Bは、図6の異常対応処理109を実行する。

[0085] 図6は、第1実施形態に係る車載セキュリティシステムの異常対応処理の内容を示すブロック図である。

図6において、異常対応処理109は、ECUステータス判定処理120、機能レベル定義情報121、機能レベル毎対応処理122、警告表示処理123およびダミー応答処理124を備える。

[0086] ECUステータス判定処理120は、監視ECU105から通知されたECU-X102の異常判定結果を確認する。例えば、ECUステータス判定処理120は、車載ネットワーク101上のECU-X102が正常か異常かを示すフラグを確認する。そして、異常対応処理部109A、109Bは、正常であれば正規の処理を実施し、異常であれば異常に応じた処理を実行する。

[0087] 機能レベル定義情報121は、ECU-A103およびECU-B104が持つ機能を、機能の実行周期などの処理間隔を基にカテゴリ分けする。もし、ECU-A103およびECU-B104に異常が生じた場合、ECU-A103およびECU-B104が全ての機能に対し異常対応処理を実行すると、ECU-A103およびECU-B104の処理負荷が増加し、重要な機能に対して理想の異常対応処理ができない可能性がある。

[0088] そこで、各機能の実行周期などの処理間隔による機能レベルを機能レベル定義情報121で定義することにより、ECU-A103およびECU-B104は、異常対応処理までの時間を有効に使用することが可能となる。例えば、モータ回転数制御や高電圧制御など処理周期が短い機能を機能レベル高とする。バッテリーの充電など処理周期が機能レベル高の機能より長い機能を機能レベル中とする。ワイパーやウィンドの動作など処理周期が機能レベル中の機能より長い機能を機能レベル低とする。機能レベル定義情報121は、これらの機能情報をデータベースとして定義する。

[0089] また、ECU-A103およびECU-B104 ECUの機能上、異常が

発生すると安全上の影響が大きいなどの機能は、実行周期が長くても、実行周期の機能レベルよりも高い機能レベルに定義することも可能である。機能レベルの定義に使用する基準として、機能の実行周期または機能の重要度以外にも、別の基準を使用するようにしてもよい。

[0090] 機能レベル毎対応処理 1 2 2 は、機能レベル定義情報 1 2 1 で定義した機能レベルに合わせた処理を実行する。例えば、機能レベル高の処理の場合、異常に対応するための時間の余裕が少ないため、初期値や前回値などを使用し、処理時間優先で実行する。機能レベル中および機能レベル低の処理の場合、E C U - X 1 0 2 から送信されたデータをチェックし、そのデータに問題がなければ通常処理を実施するなど、処理負荷を増加させないような異常処理を実行する。機能レベル中と機能レベル低の処理の差として、E C U - X 1 0 2 から送信されたデータをチェックする際の判定に用いる閾値に差を設けることで機能レベルに対する異常対応処理に差を設けることができる。判定に用いる閾値の例として、例えば、機能レベル中の処理の場合、本来の値の範囲は 1 ~ 1 0 だが、3 ~ 7 の中間値の範囲とするなど、上限でも下限でもなく確実に動作できる範囲の値のみ通常処理を実行できるように定義する。

[0091] 警告表示処理 1 2 3 は、外部機器 1 1 3 A および外部ネットワーク 1 1 3 B と接続しない外部機器のなりすましや外部からの乗っ取りのリスクの低い E C U - A 1 0 3 および E C U - B 1 0 4 で警告表示を実行する。実際に制御を実行する E C U - A 1 0 3 および E C U - B 1 0 4 が警告表示処理 1 2 3 を直接実行することにより、外部機器のなりすましや外部からの乗っ取りにより異常状態になった E C U - X 1 0 2 を介することなく、警告表示することができる。また、警告表示処理 1 2 3 は、E C U - A 1 0 3 および E C U - B 1 0 4 からの出力のみとし、外部からの入力をなくすことにより、外部機器のなりすましや外部からの乗っ取りのリスクを抑えることができる。

[0092] ダミー応答処理 1 2 4 は、外部機器のなりすましや外部からの乗っ取りなど異常状態にある E C U - X 1 0 2 から送信されたデータに対して、あたか

も送信されたデータを使用してECU-A103およびECU-B104が機能や処理を実行したようにECU-X102に応答（ダミー応答と言う）を返す。例えば、本来、ECU-A103がデータ値10で実行する機能に対して、ECU-X102からECU-A103にデータ値15が送信されたものとする。この時、ECU-A103内部では実際にはデータ値10で機能を実行するが、ECU-X102からのデータ値15の送信に対するECU-X102への応答では、データ値15で実行したように見せかける応答をECU-X102に返す。

[0093] これにより、ECU-X102への攻撃に対し、車載システムが攻撃者の支配下にあると錯覚させつつ、実際には攻撃者の支配下から逃れることができる。このため、攻撃に失敗した時の攻撃者からの更なる攻撃や別の手段による新たな攻撃を防ぎ、その間に車載システムを安全な状態にするための処理を実行する時間を稼ぐことが可能となる。

[0094] 図7は、第1実施形態に係る車載セキュリティシステムの異常対応処理を示すフローチャートである。

図7のステップS301において、ECU-A103およびECU-B104は、異常対応処理を開始すると、ステップS302において、ECU-X102から送信されたメッセージデータを取得する。この時、ECU-A103およびECU-B104は、ECU-X102からの入力に対し、ECU-A103およびECU-B104の機能の実行に必要なデータを取得する。ECU-A103およびECU-B104は、例えば、メッセージバッファにあるデータを取得するようにしてもよいし、データ授受のインタフェース機能を使用して取得するようにしてもよいし、グローバルメモリに格納されたデータを取得するようにしてもよい。

[0095] 次に、ステップS303において、ECU-A103およびECU-B104は、図4のステップS106で監視ECU105から通知された判定結果に基づいて、ステップS302で取得したメッセージデータの送信元のECU-X102のステータスを判定する。例えば、ECU-A103および

ECU-B104は、監視ECU105から送信されたECU-X102の状態を示すメッセージや、ECU-X102のステータスが格納された共通メモリなどからECU-X102の状態を取得し、その状態を基にECU-X102が正常か異常かを判定する。

[0096] ステップS303の判定結果が正常状態の場合、ステップS304に進み、通常処理を実行する。一方、ステップS303の判定結果が異常状態つまりECU-X102に対して外部機器のなりすましや外部からの乗っ取りがある場合、ステップS305に進み、ECU-A103およびECU-B104が実行する機能の機能レベルを判定する。

[0097] 次に、ECU-A103およびECU-B104は、ステップS305で判定した機能レベルに合わせた処理を実行する。すなわち、判定結果が機能レベル高の時、ステップS306において機能レベル高の処理を実行する。判定結果が機能レベル中の時、ステップS307において機能レベル中の処理を実行する。判定結果が機能レベル低の時、ステップS308において機能レベル低の処理を実行する。

[0098] 例えば、今回実行する制御がモータ回転数制御である場合、モータ回転数制御がどの機能レベルに属するかを判定する。そして、モータ回転数制御が機能レベル高として定義されている場合、機能レベル高の処理を実行する。

[0099] 次に、ステップS309において、ECU-A103およびECU-B104は、必要に応じてユーザに対し警告表示を実行する。この時、例えば、ユーザに異常内容を通知し、ユーザが対策を選択できるようにしてもよい。あるいは、発生した異常毎に警告ランプの点灯やディスプレイによるメッセージ表示などを行い、ユーザに対応を促すようにしてもよい。

[0100] 次に、ステップS310において、ECU-A103およびECU-B104は、攻撃者が指定したデータを使用して機能を実行したように見せかけるダミー応答用データを作成する。例えば、本来、データ値10で実行する機能に対して、データ値15がECU-X102から送信された場合、ECU-A103およびECU-B104内部ではデータ値10で機能を実行し

たにもかかわらず、応答メッセージとしては、データ値 15 で実行したことを示すダミー応答用データを作成する。

[0101] 次に、ステップ S 3 1 1 において、ECU-A 1 0 3 および ECU-B 1 0 4 は、ECU-X 1 0 2 の通常状態または異常状態に応じて作成された応答を ECU-X 1 0 2 に返し、ステップ S 3 1 2 で異常対応処理を終了する。ECU-X 1 0 2 に応答を返す場合、例えば、車載ネットワーク 1 0 1 のプロトコルまたはインタフェース機能を用いることができる。

[0102] 図 8 は、図 7 の機能レベル高処理を示すフローチャートである。

図 8 のステップ S 4 0 1 において、ECU-A 1 0 3 および ECU-B 1 0 4 は、機能レベル高の処理を開始すると、ステップ S 4 0 2 において、安全処理を実行する。安全処理では、外部からの乗っ取りまたは外部機器のなりすましによる不正操作により送信されたデータ値が無効になるような対策処理を実行することができる。例えば、正規の手順で機能を再実行したり、制御値や取得したデータ値を初期値に変更し動作を継続させたり、動作上問題のない値（中間値等）に設定し動作させたりすることができる。S 4 0 2 の安全処理を実行すると、ステップ S 4 0 3 において、機能レベル高の処理を終了する。

[0103] 機能レベル高の機能は、処理の実行周期が短く重要な機能が多いため、処理をシンプルにして処理時間を短くし、安全かつ確実に処理を実行することができるデータ値を使用するような処理が望ましい。

[0104] 図 9 は、図 7 の機能レベル中処理および機能レベル低処理を示すフローチャートである。

図 9 のステップ S 5 0 1 において、ECU-A 1 0 3 および ECU-B 1 0 4 は、機能レベル中および機能レベル低の処理を開始すると、ステップ S 5 0 2 において、ECU-A 1 0 3 および ECU-B 1 0 4 が使用するデータの確認を行う。ECU-A 1 0 3 および ECU-B 1 0 4 が使用するデータの値が適正範囲かつ異常なしの場合、ステップ S 5 0 3 において通常処理を実行する。一方、ECU-A 1 0 3 および ECU-B 1 0 4 が使用するデ

ータの値が適正範囲外または異常ありの場合は、ステップS504において安全処理を実行する。ステップS503の通常処理またはステップS504の安全処理を実行すると、ステップS505において機能レベル中または機能レベル低の処理を終了する。

[0105] 機能レベル中および機能レベル低の処理は、基本的に処理フローは同じであるが、ステップS502の使用データの確認で使用する判定値の閾値が異なる。例えば、機能レベル中の処理の場合、データ値の±5まで許容するが、機能レベル低の処理の場合はデータ値の±10まで許容することができる。もしくは、通常の異常判定と同じ閾値などとし、判定値に差を設けるようにしてもよい。機能レベルに応じて判定基準に差を設けることで、安全処理までの時間を確保し、処理周期が短く優先度の高い機能の安全処理を優先的に実行することができる。

[0106] 上述した第1実施形態では、監視ECU105は、ECU-X102の状態を判定するために、ECU-X102、ECU-A103およびECU-B104から情報を取得する方法について説明したが、ECU-X102のみから情報を取得するようにしてもよいし、ECU-A103のみから情報を取得するようにしてもよいし、ECU-B104のみから情報を取得するようにしてもよいし、ECU-A103およびECU-B104から情報を取得するようにしてもよい。あるいは、ECU-X102、ECU-A103およびECU-B104からだけではなく、それ以上の数のECUから情報を取得し、ECU-X102の異常を判定するようにしてもよい。ECUから取得する情報が多ければ多いほど、外部からの乗っ取りや外部機器のなりすましによる不正操作の判定精度を向上させることができる。

[0107] また、上述した第1実施形態では、監視ECU105が、ECU-X102の異常を判定し、その判定結果をECU-A103およびECU-B104に通知する方法について説明したが、監視ECU105が持つ機能をECU-A103またはECU-B104に組み込み、ECU-A103またはECU-B104がECU-X102の異常を判定するようにしてもよい。こ

の時、監視ECU105を省略することができる。監視ECU105を省略した場合、複数のECUの情報を用いることでECU-X102の異常を判定するようにしてもよい。複数のECUの情報を用いる場合、1個でも異常判定したECUがあれば、ECU-X102に異常があると判定するようにしてもよいし、全てのECUが異常判定した時にECU-X102に異常があると判定するようにしてもよいし、複数のECUの多数決によってECU-X102の異常を判定するようにしてもよい。

[0108] 以上説明したように、上述した第1実施形態によれば、車載ネットワークを介して複数のECUが接続された車載システム上において、正常な制御値で制御され、動作異常と判定されないような車載システムの外部からの乗っ取りや外部機器のなりすましによる不正操作等のセキュリティ脅威に対して、外部からの乗っ取りや外部機器のなりすましによる不正操作を検知し、その不正操作に対する処理を攻撃者に知られないようにすることが可能となり、攻撃者からの攻撃に対して、車載システムを安全に動作させるための時間を確保することが可能となる。

[0109] 以下、通常的車載ネットワークとは別に、外部と接続されないバックアップ用の車載ネットワークを持つ第2実施形態について説明する。なお、異常の検知の方法や対処方法については、第1実施形態と同様の仕組みを持つことができる。

[0110] 図10は、第2実施形態に係る車載セキュリティシステムの構成を示すブロック図である。

図10の構成では、図3のECU-A103、ECU-B104および監視ECU105の代わりに、ECU-A203、ECU-B204および監視ECU205を備える。また、図10の構成では、図3の車載ネットワーク101と別に、外部機器113Aおよび外部ネットワーク113Bと接続されないバックアップ用の車載ネットワーク125（以降、バックアップネットワークと称す）を備える。

[0111] バックアップネットワーク125は、外部機器113Aおよび外部ネット

ワーク 1 1 3 B と接続されない ECU-A 2 0 3、ECU-B 2 0 4 および監視 ECU 2 0 5 のみを含み、外部機器 1 1 3 A および外部ネットワーク 1 1 3 B と接続される ECU-X 1 0 2 を含まない。このため、バックアップネットワーク 1 2 5 は、外部機器のなりすましや外部からの乗っ取りの発生リスクが少ないセキュアな車載ネットワークである。

[0112] ECU-A 2 0 3、ECU-B 2 0 4 および監視 ECU 2 0 5 は、ECU-X 1 0 2 に異常がない場合は、車載ネットワーク 1 0 1 を用いて通信を実行することができる。ECU-A 2 0 3、ECU-B 2 0 4 および監視 ECU 2 0 5 は、ECU-X 1 0 2 に異常がある場合は、ECU-X 1 0 2 との間では車載ネットワーク 1 0 1 を用いて通信を実行し、ECU-A 2 0 3、ECU-B 2 0 4 および監視 ECU 2 0 5 間ではバックアップネットワーク 1 2 5 を用いて通信を実行することができる。ECU-A 2 0 3、ECU-B 2 0 4 および監視 ECU 2 0 5 のその他の構成については、ECU-A 1 0 3、ECU-B 1 0 4 および監視 ECU 1 0 5 と同様である。

[0113] 例えば、ECU-X 1 0 2 が外部機器のなりすましや外部からの乗っ取りをされた場合、ECU-A 2 0 3、ECU-B 2 0 4 および監視 ECU 2 0 5 は、異常状態にある ECU-X 1 0 2 が接続されている車載ネットワーク 1 0 1 に対しては、ダミー応答を常を送信し、バックアップネットワーク 1 2 5 にのみ正常なデータを送信することができる。このように、外部からの脅威がない独立したバックアップネットワーク 1 2 5 を備えることで、通信データ中に不正データと正常データが混在するのを防止することができ、セキュアな通信を行うことができる。また、不正データによる脅威に晒されるリスクを減らすことができ、処理負荷を軽減することも可能となる。

[0114] 図 1 1 は、第 3 実施形態に係る車載セキュリティシステムの異常対応処理を示すフローチャートである。

図 1 1 のステップ S 6 0 1 において、ECU-A 2 0 3 および ECU-B 2 0 4 は、異常対応処理を開始すると、ステップ S 6 0 2 において、ECU-X 1 0 2 から送信されたメッセージデータを取得する。この時、ECU-

A 2 0 3 および E C U - B 2 0 4 は、E C U - X 1 0 2 からの入力に対し、E C U - A 2 0 3 および E C U - B 2 0 4 の機能の実行に必要なデータを取得する。

[0115] 次に、ステップ S 6 0 3 において、E C U - A 1 0 3 および E C U - B 1 0 4 は、監視 E C U 2 0 5 から通知された判定結果に基づいて、ステップ S 6 0 2 で取得したメッセージデータの送信元の E C U - X 1 0 2 のステータスを判定する。

[0116] ステップ S 6 0 3 の判定結果が正常状態の場合、ステップ S 6 0 4 に進み、通常処理を実行する。一方、ステップ S 6 0 3 の判定結果が異常状態である場合、ステップ S 6 0 5 に進み、E C U - A 2 0 3 および E C U - B 2 0 4 が実行する機能の機能レベルを判定する。

[0117] 次に、E C U - A 2 0 3 および E C U - B 2 0 4 は、ステップ S 6 0 5 で判定した機能レベルに合わせた処理を実行する。すなわち、判定結果が機能レベル高の時、ステップ S 6 0 6 において機能レベル高の処理を実行する。判定結果が機能レベル中の時、ステップ S 6 0 7 において機能レベル中の処理を実行する。判定結果が機能レベル低の時、ステップ S 6 0 8 において機能レベル低の処理を実行する。

[0118] 次に、ステップ S 6 0 9 において、E C U - A 2 0 3 および E C U - B 2 0 4 は、必要に応じてユーザに対し警告表示を実行する。この時、例えば、ユーザに異常内容を通知し、ユーザが対策を選択できるようにしてもよい。あるいは、発生した異常毎に警告ランプの点灯やディスプレイによるメッセージ表示などを行い、ユーザに対応を促すようにしてもよい。

[0119] 次に、ステップ S 6 1 0 において、E C U - A 2 0 3 および E C U - B 2 0 4 は、バックアップネットワーク 1 2 5 を介し、ステップ S 6 0 5 で判定した機能レベル毎対応処理に必要な値を送信または受信する通信処理を実行する。

[0120] 次に、ステップ S 6 1 1 において、E C U - A 2 0 3 および E C U - B 2 0 4 は、攻撃者が指定したデータを使用して機能を実行したように見せかけ

るダミー応答用データを作成する。

[0121] 次に、ステップS 6 1 2において、E C U－A 2 0 3およびE C U－B 2 0 4は、E C U－X 1 0 2の通常状態または異常状態に応じて作成された応答をE C U－X 1 0 2に返し、ステップS 6 1 3で異常対応処理を終了する。E C U－X 1 0 2に応答を返す場合、例えば、車載ネットワーク1 0 1のプロトコルまたはインタフェース機能を用いることができる。

[0122] 以上説明したように、上述した第2実施形態によれば、車載ネットワークを介して複数のE C Uが接続された車載システム上において、正常な制御値で制御され、動作異常と判定されないような車載システムの外部からの乗っ取りや外部機器のなりすましによる不正操作等のセキュリティ脅威に対して、外部からの乗っ取りや外部機器のなりすましによる不正操作を検知し、その不正操作に対する処理を攻撃者に知られないようにして、車載システムを安全に動作させるための時間を確保することが可能となるだけでなく、不正操作されたE C Uが接続されない独立したネットワークを使用することにより、不正データと正常データを混在させないセキュアな通信を実現することができる。

[0123] 図1 2は、第3実施形態に係る車載セキュリティシステムの構成を示すブロック図である。

図1 2の構成では、図3のE C U－A 1 0 3、E C U－B 1 0 4および監視E C U 1 0 5の代わりに、E C U－A 3 0 3、E C U－B 3 0 4および監視E C U 3 0 5を備える。また、図1 2の構成では、図3の車載ネットワーク1 0 1の代わりに、車載ネットワーク1 2 6、1 2 7、3 0 1、3 2 5およびゲートウェイ1 2 8、1 2 9を備える。

[0124] 車載ネットワーク1 2 6、1 2 7、3 0 1、3 2 5はそれぞれ独立して設けられている。E C U－X 1 0 2と監視E C U 3 0 5とは、車載ネットワーク3 0 1、3 2 5をそれぞれ介して2重に接続されている。E C U－A 3 0 3とE C U－B 3 0 4とは、車載ネットワーク1 2 6、1 2 7をそれぞれ介して2重に接続されている。車載ネットワーク3 0 1、1 2 6は、ゲートウ

エイ 128 を介して接続されている。車載ネットワーク 325、127 は、ゲートウェイ 129 を介して接続されている。

[0125] 監視 ECU 305 は、ゲートウェイ 128、129 を切替制御する。ECU-A 303 および ECU-B 304 は、ECU-X 102 に異常がない場合は、車載ネットワーク 126 を介して通信を実行し、ECU-X 102 に異常がある場合は、車載ネットワーク 126 を介して ECU-X 102 および監視 ECU 305 と通信を実行し、車載ネットワーク 127 を介して ECU-A 303 と ECU-B 304 との間で通信を実行することができる。ECU-A 303、ECU-B 304 および監視 ECU 305 のその他の構成については、ECU-A 103、ECU-B 104 および監視 ECU 105 と同様である。

[0126] ECU-X 102 に異常がない場合、ECU-X 102、ECU-A 303、ECU-B 304 および監視 ECU 305 は、車載ネットワーク 301、126 を介して通信を行う。ECU-X 102 が乗っ取られていることを監視 ECU 305 が検出すると、監視 ECU 305 は、ECU-A 303、ECU-B 304 に対して車載ネットワーク 127、325 間の接続を切断する旨を通知する。また、監視 ECU 305 は、ゲートウェイ 129 に対し、車載ネットワーク 127、325 間の接続を切断するように指示する。監視 ECU 305 から通知を受けた ECU-A 303、ECU-B 304 は、通常の応答を車載ネットワーク 127 に返し、ECU-X 102 へのダミー応答を車載ネットワーク 126 に返す。

[0127] これにより、ECU-A 303、ECU-B 304 は、ダミー応答が流れる範囲を車載ネットワーク 126、301 に限定しつつ、ECU-X 102 と切断された車載ネットワーク 127 を介して正常動作を継続することができる。システムの安定性を向上させることができる。

[0128] 図 13 は、第 4 実施形態に係る車載セキュリティシステムに用いられる ECU のハードウェア構成を示すブロック図である。

図 13 において、ECU 10 には、プロセッサ 11、通信制御デバイス 1

2、通信インタフェース13、主記憶デバイス14、外部記憶デバイス15および入出力インタフェース17が設けられている。プロセッサ11、通信制御デバイス12、通信インタフェース13、主記憶デバイス14、外部記憶デバイス15および入出力インタフェース17は、内部バス16を介して相互に接続されている。主記憶デバイス14および外部記憶デバイス15は、プロセッサ11からアクセス可能である。

[0129] また、ECU10の外部には、センサ20、表示部30およびアクチュエータ40が設けられている。センサ20、表示部30およびアクチュエータ40は、入出力インタフェース17を介して内部バス16に接続されている。センサ20は、例えば、空気吸入量を検出するエアフローメータ、吸気管圧力を検出する圧力センサ、スロットル開度を検出するスロットルセンサ、エンジン回転数を検出する回転数センサである。表示部30は、ネットワーク19を介して接続されている他のECUの乗っ取りなどが行われた時に警告メッセージなどを表示したり、ユーザが選択できる対策などを表示したりする。アクチュエータ40は、自車両のエンジン、変速機、ブレーキおよびステアリングなどを操作することで、自車両の加減速、制動および操舵などを実行する。

[0130] プロセッサ11は、ECU10全体の動作制御を司るハードウェアである。主記憶デバイス14は、例えば、SRAMまたはDRAMなどの半導体メモリから構成することができる。主記憶デバイス14には、プロセッサ11が実行中のプログラムを格納したり、プロセッサ11がプログラムを実行するためのワークエリアを設けることができる。

[0131] 外部記憶デバイス15は、大容量の記憶容量を有する記憶デバイスであり、例えば、ハードディスク装置、SSD (Solid State Drive) またはフラッシュメモリである。外部記憶デバイス15は、各種プログラムの実行ファイルやプログラムの実行時に用いられるデータを保持することができる。

[0132] ECU10が、図1のECU-A103またはECU-B104である場

合、外部記憶デバイス 15 には、攻撃対処プログラム 15 A、シナリオ定義情報 15 B および機能レベル定義情報 15 C を格納することができる。攻撃対処プログラム 15 A は、ECU 10 にインストール可能なソフトウェアであってもよいし、ECU 10 にファームウェアとして組み込まれていてもよい。

[0133] 通信制御デバイス 12 は、外部との通信を制御する機能を有するハードウェアである。通信制御デバイス 12 は、通信インタフェース 13 を介してネットワーク 19 に接続される。ネットワーク 19 は、CAN、FlexRay、LIN、Ethernet などの車載ネットワークを用いることができる。

[0134] プロセッサ 11 が攻撃対処プログラム 15 A および機能レベル定義情報 15 C を主記憶デバイス 14 に読み出し、機能レベル定義情報 15 C を参照しつつ攻撃対処プログラム 15 A を実行することにより、図 7 の異常対応処理を実現することができる。

符号の説明

[0135] 100x、100A、100B…センサ、101…車載ネットワーク、102…ECU-X、103…ECU-A、104…ECU-B、105…監視ECU、106x、106A、106B…アクチュエータ、107x、107A、107B、110…シナリオ定義情報、108x、108A、108B…シナリオ実行結果格納メモリ、109x、109A、109B…異常対応処理部、111…シナリオ実行結果判定処理部、112…判定結果通知処理部、113A…外部機器、113B…外部ネットワーク、114…警告表示部

請求の範囲

- [請求項1] 第1電子制御装置と、
前記第1電子制御装置と通信可能な第2電子制御装置とを備え、
前記第2電子制御装置は、
前記第1電子制御装置からの入力に対する第1処理を実行し、
前記入力に対して前記第1処理と異なる第2処理を実行したことを
示す応答を前記第1電子制御装置に返す車載セキュリティシステム。
- [請求項2] 前記第2電子制御装置は、
前記第1電子制御装置が所定の動作から逸脱したことを検知し、
前記検知結果に基づいて前記第1電子制御装置からの入力に対する
前記第1処理を実行し、
前記入力に対して前記第1処理と異なる第2処理を実行したことを
示す応答を前記第1電子制御装置に返す請求項1に記載の車載セキュ
リティシステム。
- [請求項3] 前記第1処理は、前記第1電子制御装置からの入力に対する安全処
理であり、
前記第2処理は、前記第1電子制御装置からの入力の指示通りに実
行した処理である請求項1に記載の車載セキュリティシステム。
- [請求項4] 前記第2電子制御装置は、前記第1電子制御装置からの入力に対し
、予め定義された処理の機能レベルに応じて前記第1処理を実行する
請求項1に記載の車載セキュリティシステム。
- [請求項5] 前記機能レベルは、前記第1処理の処理周期または処理内容に応じ
て定義されている請求項4に記載の車載セキュリティシステム。
- [請求項6] 前記第2電子制御装置は、前記第1処理に使用されるデータに基づ
いて、前記安全処理を実行するか通常処理を実行するかを決定する請
求項3に記載の車載セキュリティシステム。
- [請求項7] 前記第2電子制御装置は、前記第1電子制御装置を含まない通信ネ
ットワークを介して前記検知結果に応じた警告を行う請求項2に記載

の車載セキュリティシステム。

- [請求項8] 前記第1電子制御装置および前記第2電子制御装置と通信可能な第3電子制御装置を備え、
前記第3電子制御装置は、
前記第1電子制御装置が所定の動作から逸脱したことを検知し、
前記検知結果を前記第2電子制御装置に通知し、
前記第2電子制御装置は、
前記第3電子制御装置から通知された検知結果に基づいて前記第1電子制御装置からの入力に対する前記第1処理を実行し、
前記入力に対して前記第1処理と異なる第2処理を実行したことを示す応答を前記第1電子制御装置に返す請求項1に記載の車載セキュリティシステム。

- [請求項9] 前記第1電子制御装置、前記第2電子制御装置および前記第3電子制御装置を含む第1車載ネットワークと、
前記第2電子制御装置および前記第3電子制御装置を含み、前記第1電子制御装置を含まない第2車載ネットワークとを備える請求項8に記載の車載セキュリティシステム。

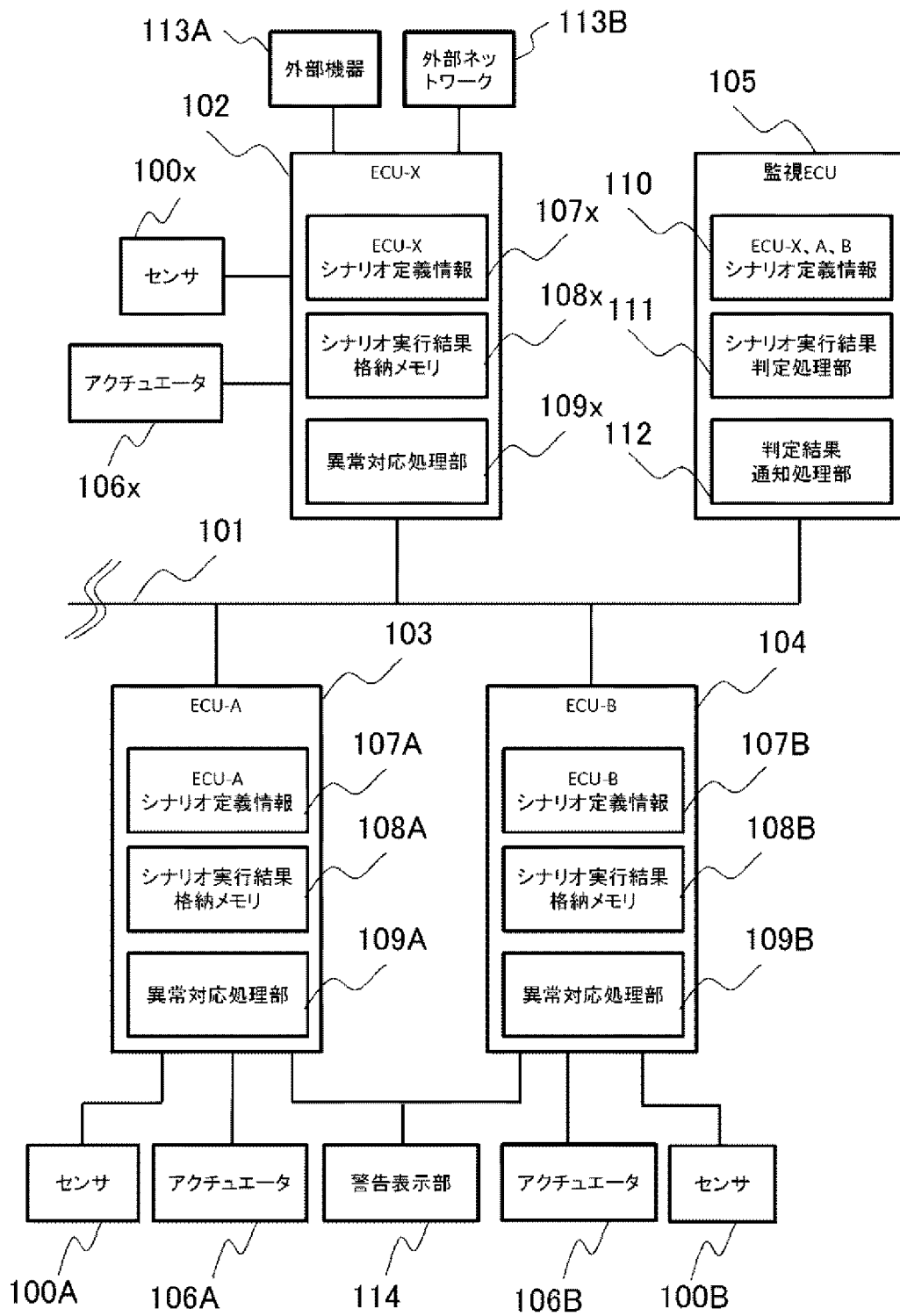
- [請求項10] 前記第1電子制御装置および前記第3電子制御装置を含む第1車載ネットワークと、
前記第1電子制御装置および前記第3電子制御装置を含む第2車載ネットワークと、
前記第2電子制御装置を含む第3車載ネットワークと、
前記第2電子制御装置を含む第4車載ネットワークと、
前記第1車載ネットワークと前記第3車載ネットワークとを接続可能な第1ゲートウェイと、
前記第2車載ネットワークと前記第4車載ネットワークとを接続可能な第2ゲートウェイとを備える請求項8に記載の車載セキュリティシステム。

- [請求項11] プロセッサを備える攻撃対処方法であって、
 前記プロセッサは、
 攻撃時の入力に対する第1処理を実行し、
 前記入力に対して前記第1処理と異なる第2処理を実行したことを
 示す応答を返す攻撃対処方法。
- [請求項12] 前記第1処理は、前記攻撃時の指示に対してフェールセーフ側の処
 理であり、
 前記第2処理は、前記攻撃時の指示通りの処理である請求項11に
 記載の攻撃対処方法。
- [請求項13] 攻撃対象となる機能に要求される機能レベルに応じて前記第1処理
 を実行する請求項11に記載の攻撃対処方法。
- [請求項14] 攻撃対象となる第1プロセッサと、
 前記第1プロセッサとネットワークを介して接続された第2プロセ
 ッサとを備え、
 前記第2プロセッサは、
 前記第1プロセッサからの入力に対する前記第1処理を実行し、
 前記入力に対して前記第1処理と異なる第2処理を実行したことを
 示す応答を前記第1プロセッサに返す請求項11に記載の攻撃対処方
 法。
- [請求項15] 前記第1プロセッサとネットワークを介して接続された第3プロセ
 ッサとを備え、
 前記第3プロセッサは、
 前記第1プロセッサが所定の動作から逸脱したことを検知し、
 前記検知結果を前記第2プロセッサに通知し、
 前記第2プロセッサは、
 前記第3プロセッサから通知された検知結果に基づいて前記第1プロ
 セッサからの入力に対する前記第1処理を実行し、
 前記入力に対して前記第1処理と異なる第2処理を実行したことを

示す応答を前記第 1 プロセッサに返す請求項 1 4 に記載の攻撃対処方法。

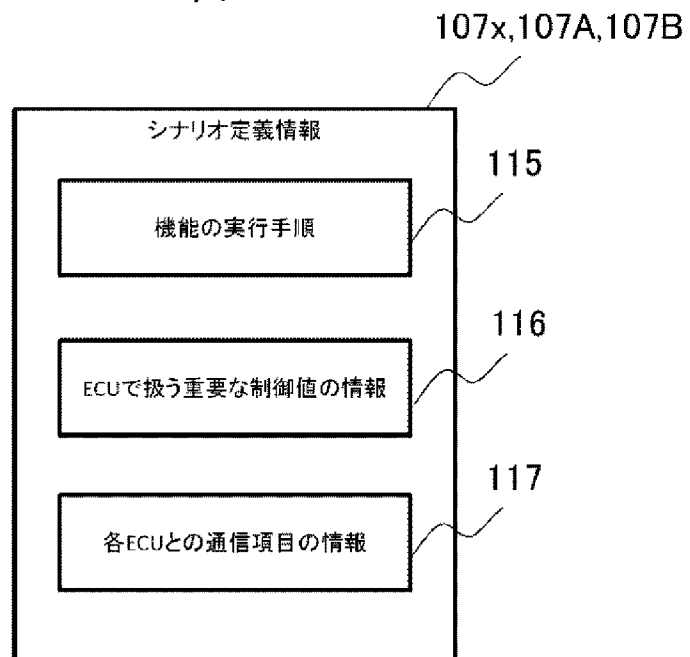
[図1]

図1



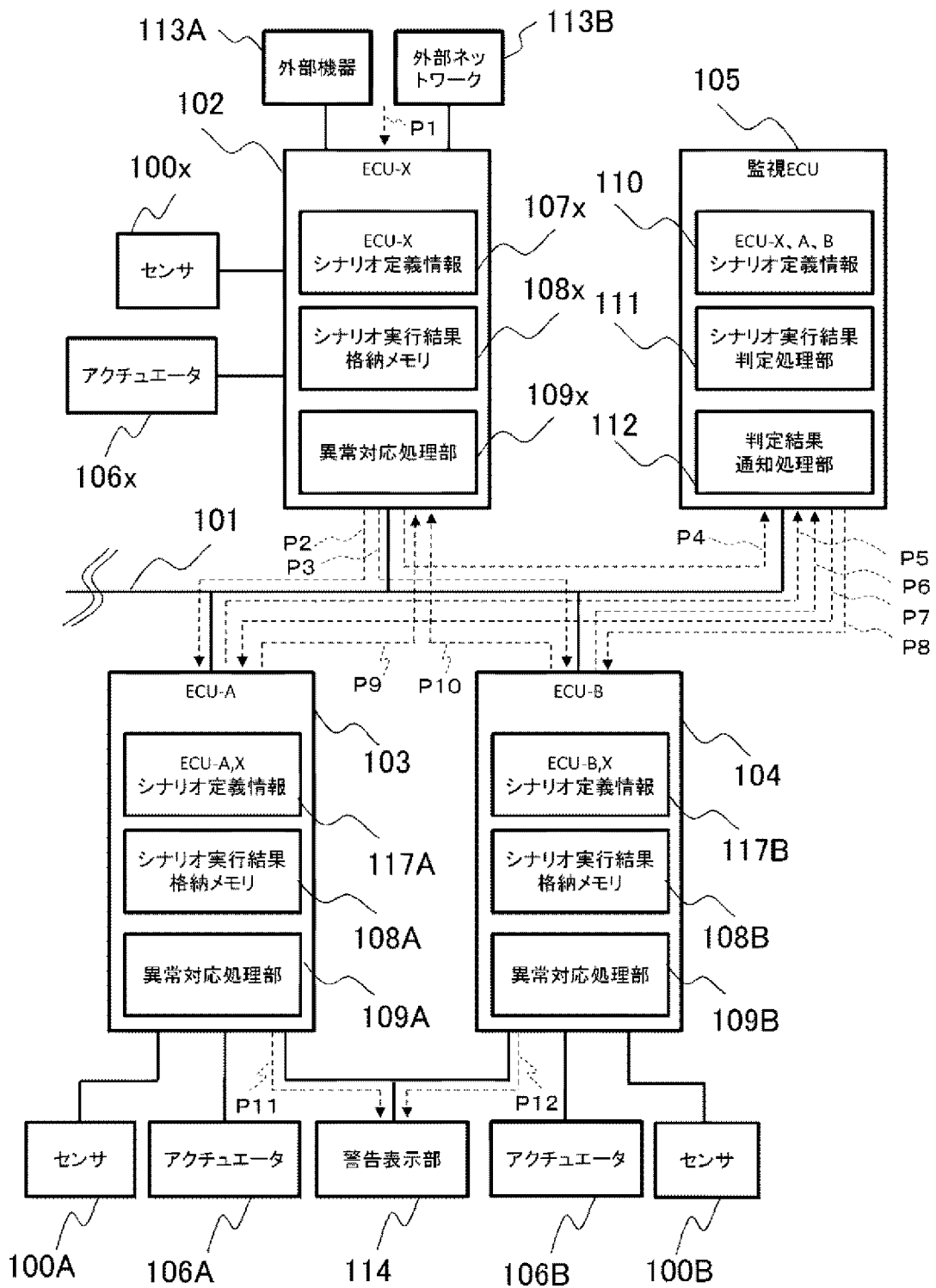
[図2]

図2



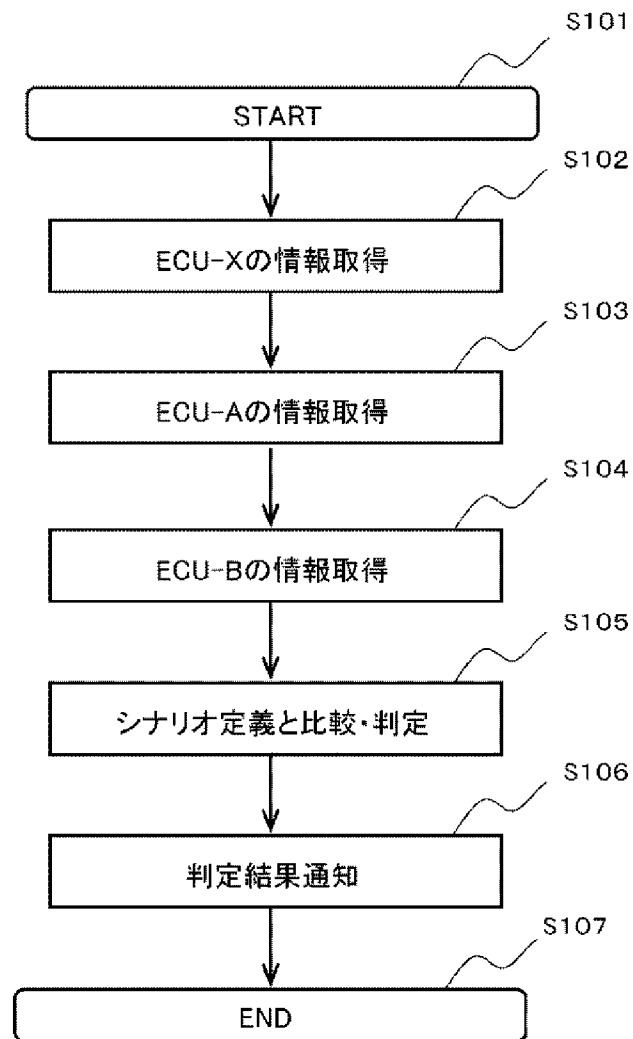
[図3]

図3



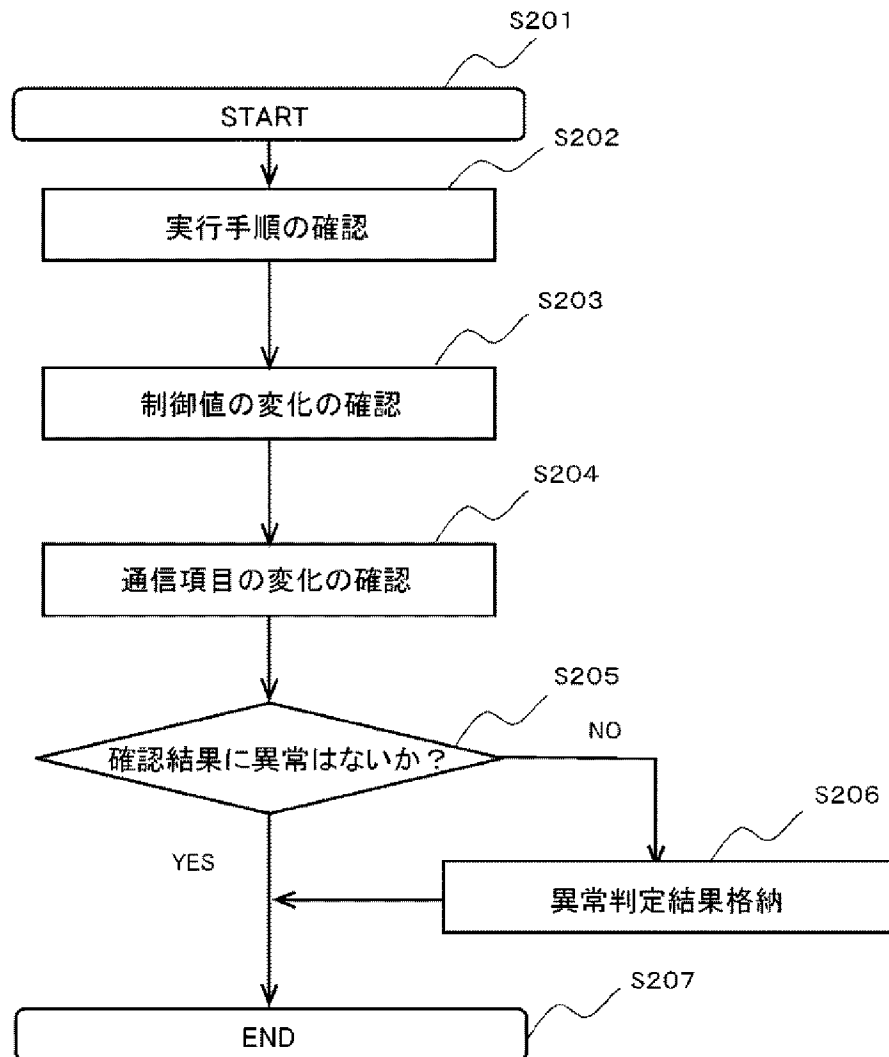
[図4]

図4



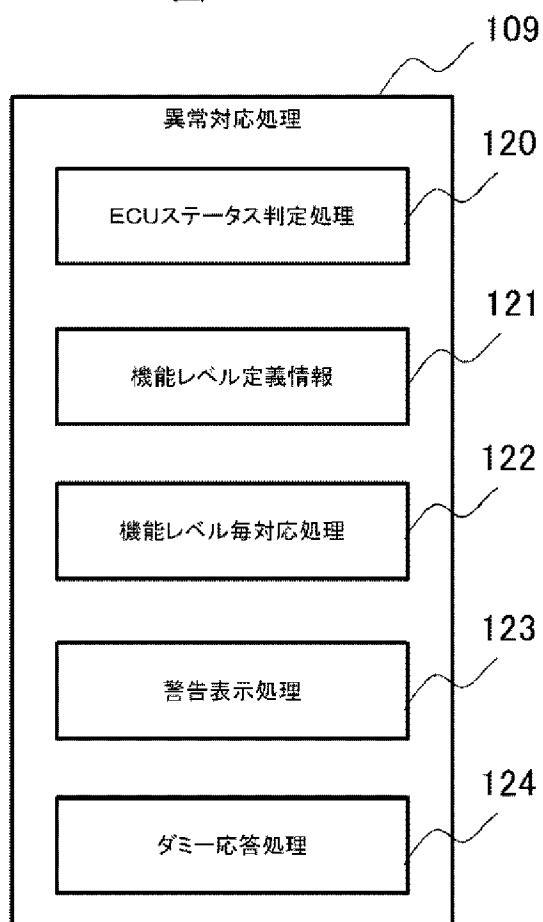
[図5]

図5



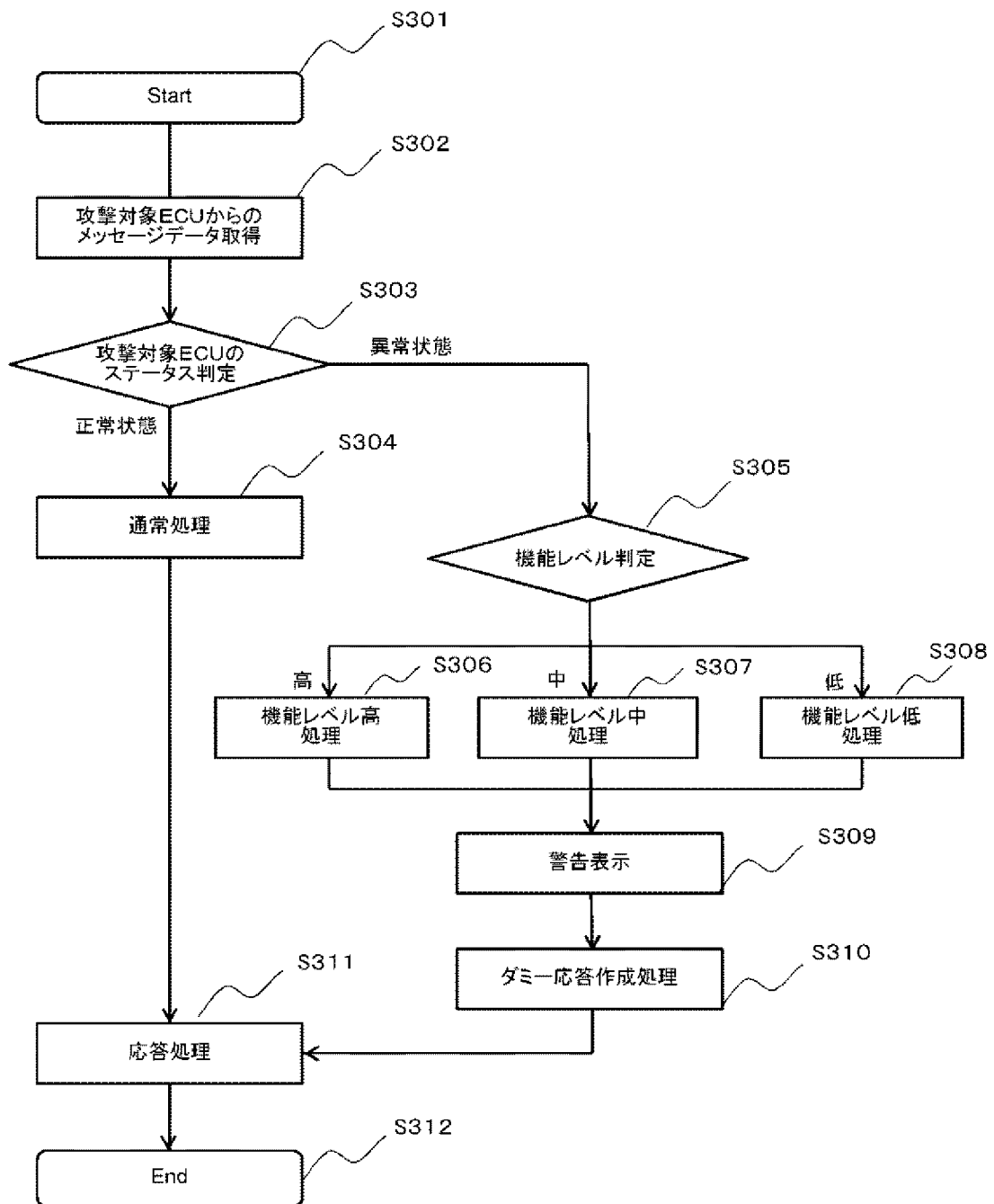
[図6]

図6

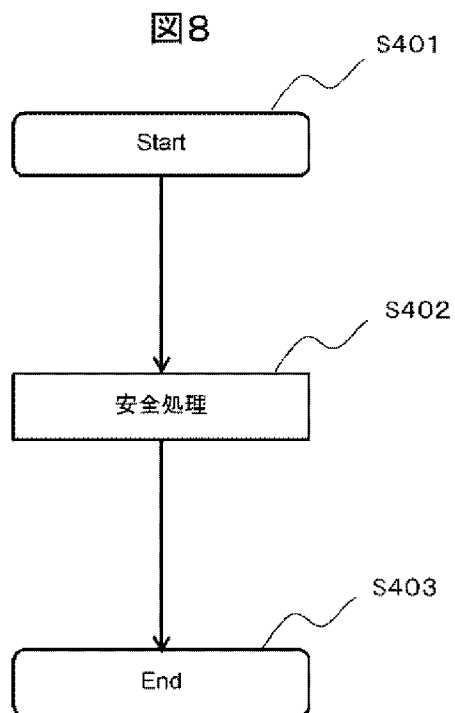


[図7]

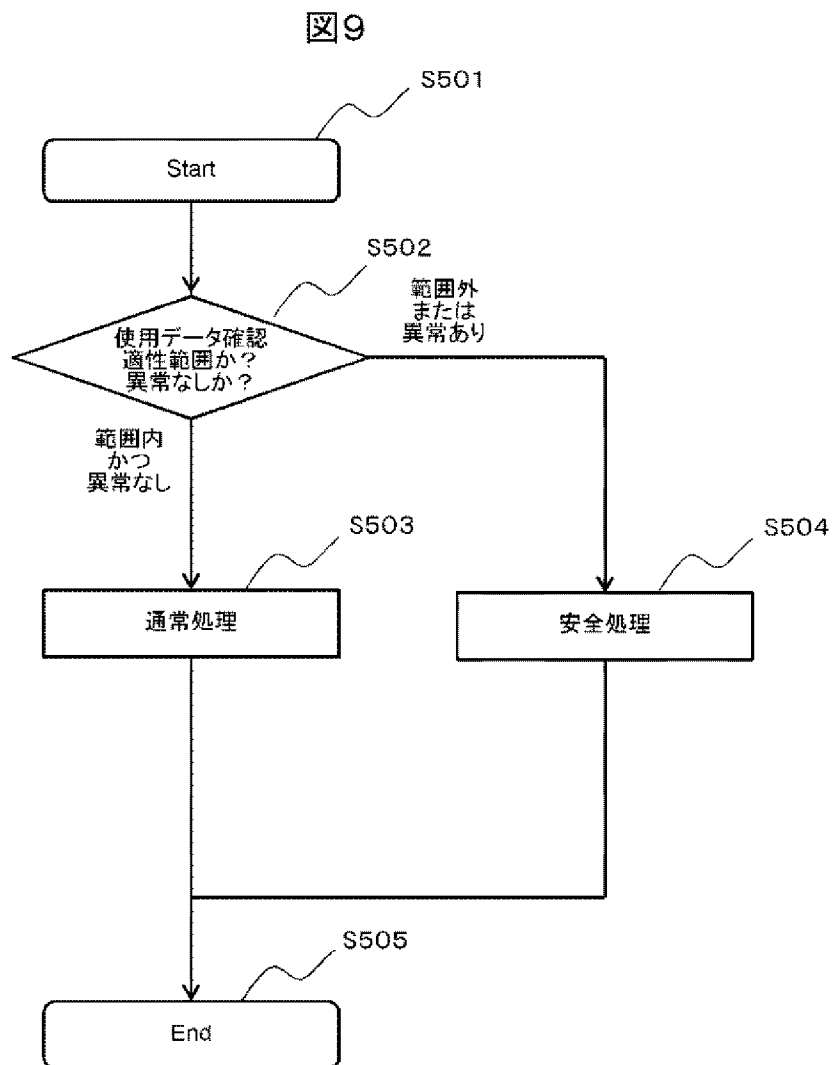
図7



[図8]

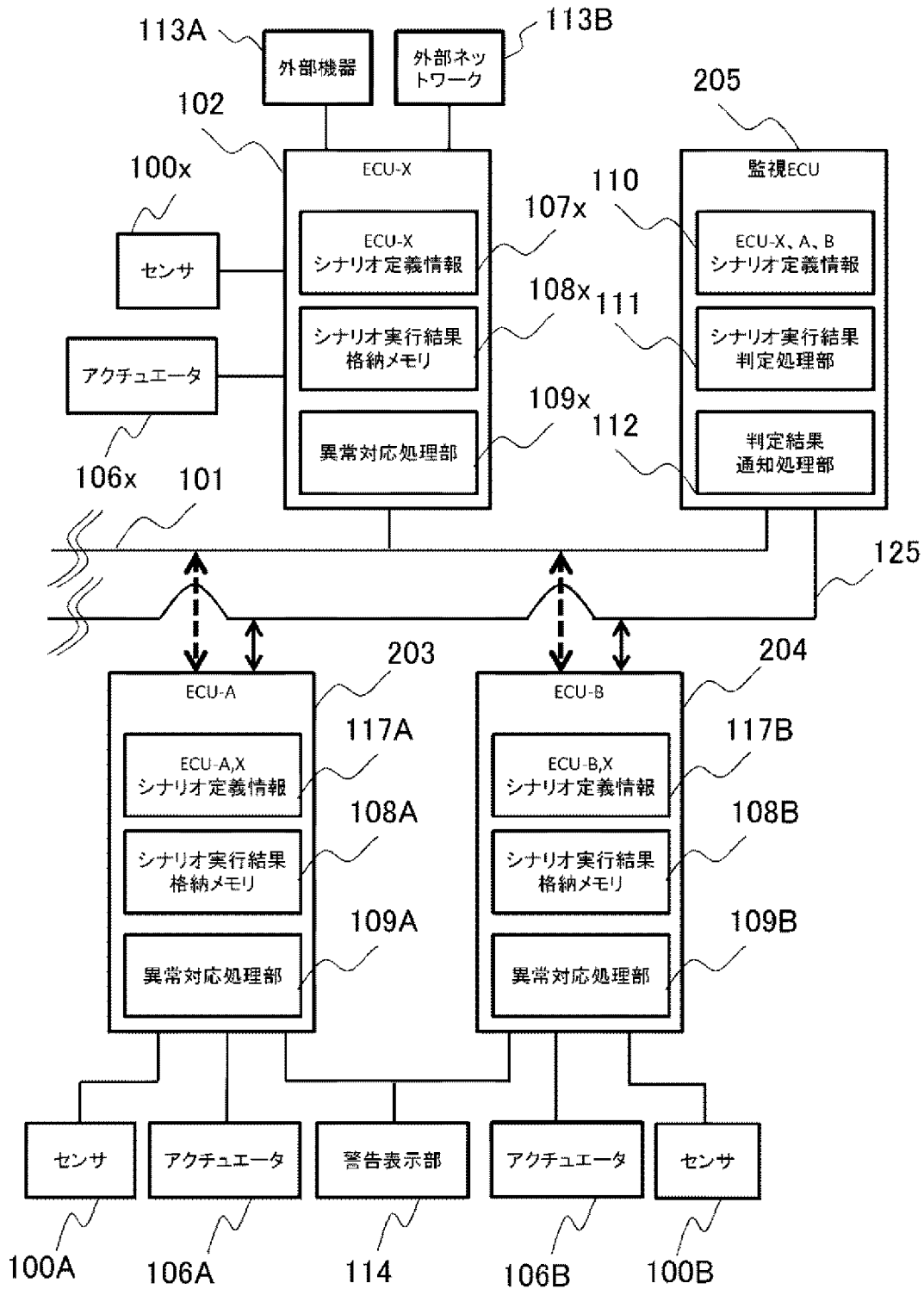


[図9]



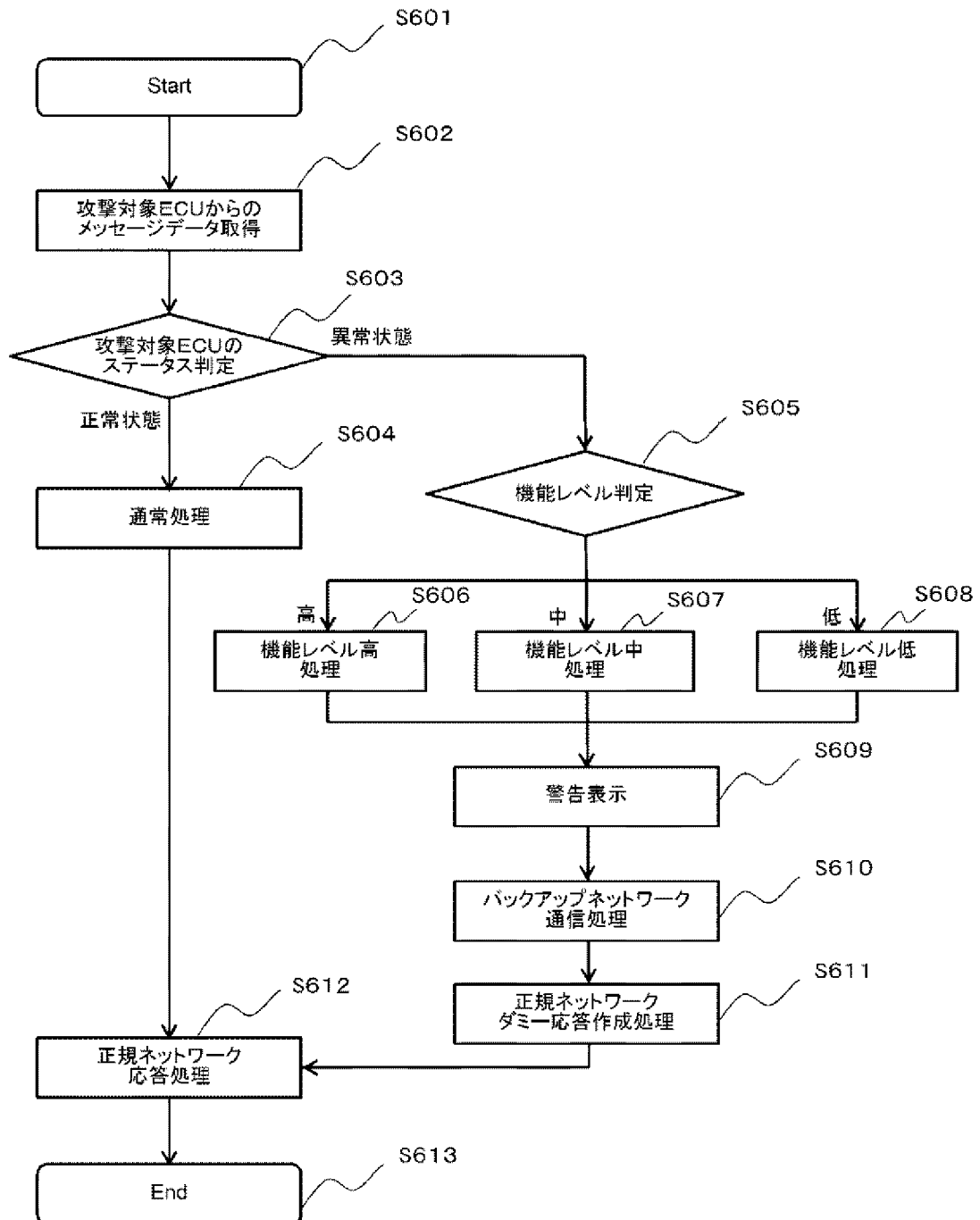
[図10]

図 10

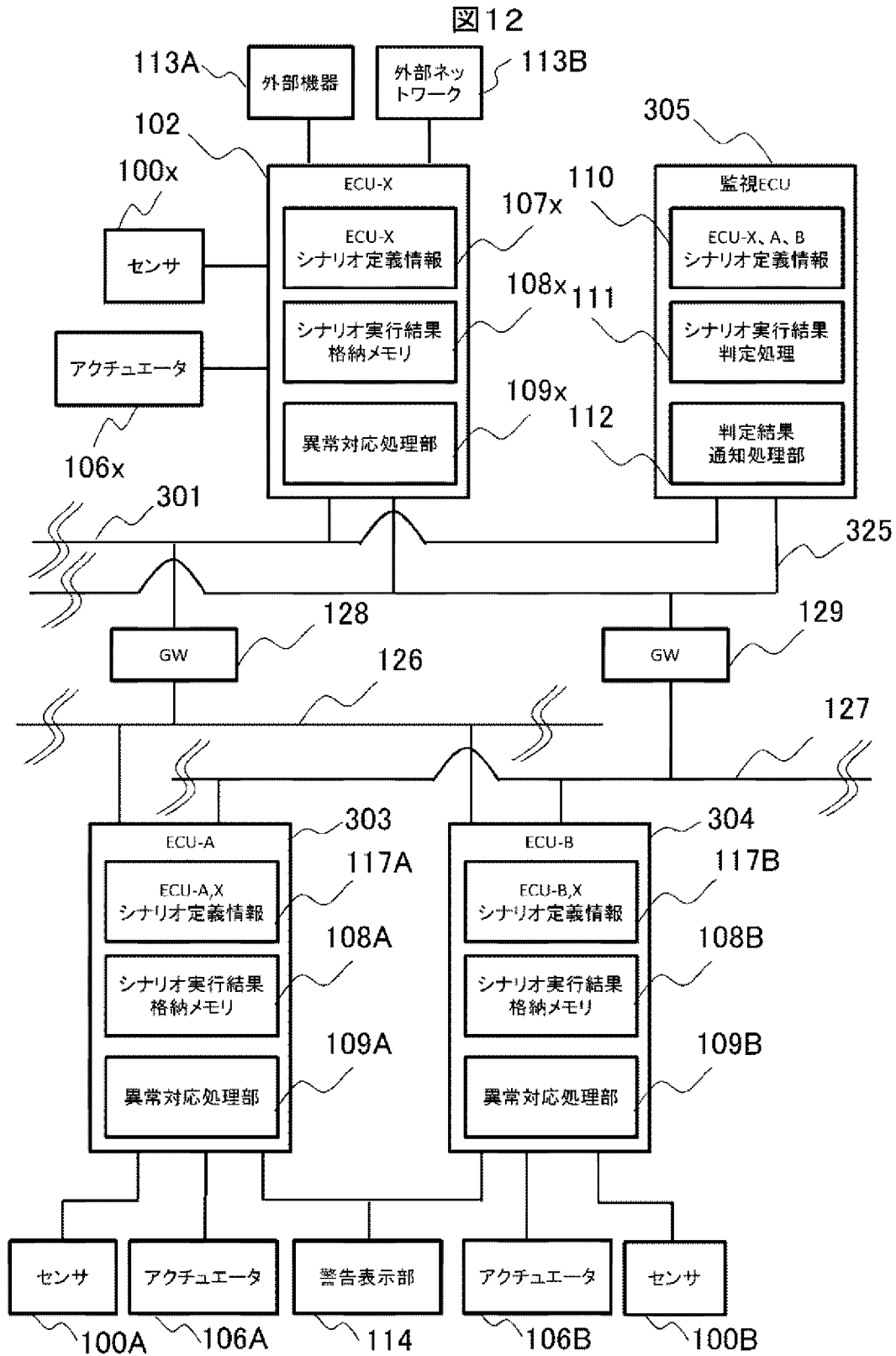


[図11]

図11

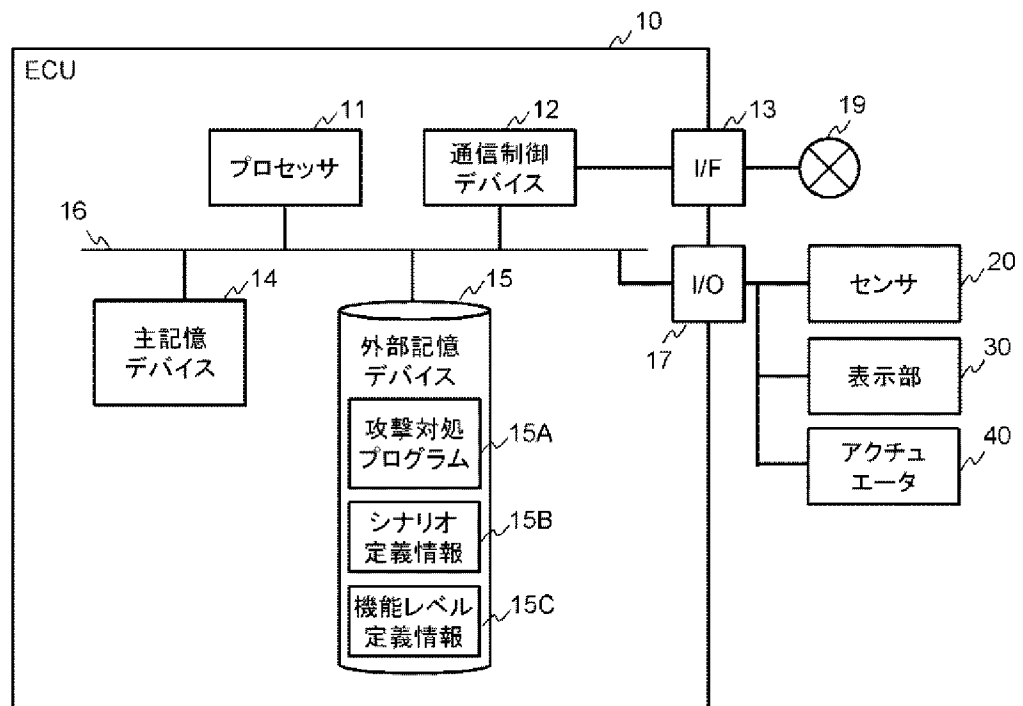


[図12]



[図13]

図13



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/024208

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. G06F21/55 (2013.01) i, B60R16/02 (2006.01) i, G06F11/07 (2006.01) i, H04L12/28 (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)

Int.Cl. G06F21/55, B60R16/02, G06F11/07, H04L12/28

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

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

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.
X Y A	JP 2002-111 726 A (KDDI CORPORATION) 12 April 2002, paragraphs [0012]-[0044], fig. 1-9 & US 2002/0046351 A1, paragraphs [0024]-[0042], fig. 1-9	11-13 1-6 7-10, 14-15
Y	JP 2014-183395 A (HITACHI AUTOMOTIVE SYSTEMS, LTD.) 29 September 2014, paragraphs [0020]-[0040], fig. 1-3 (Family: none)	1-6
Y	中野 学, 自動車の情報セキュリティ 初版, 第 1 版, 日経 BP 社 望月洋介, 27 December 2013, pp. 144-147, pp. 152-160, (NAKANO, Gaku, "Automotive Information Security, first edition", First edition, NIKKEI BUSINESS PUBLICATIONS, INC., MOCHIZUKI, Yosuke)	5



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

"I" 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
01 October 2019 (01.10.2019)

Date of mailing of the international search report
15 October 2019 (15.10.2019)

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

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/024208

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-342279 A (FUJITSU LTD.) 29 November 2002, & US 2002/0133606 A1	1-15
A	針生 剛男, NTT グループのセキュリティビジネスを支えるマルウェア対策用セキュリティインテリジェンス, NTT 技術ジャーナル第 27 巻第 10 号, 01 October 2015, vol. 27, pp. 18-22, (HARIU, Takeo, "Security Intelligence for Malware Countermeasures to Support NTT Group's Security Business", NTT GIJUTU Journal vol. 27, no. 10)	1-15
A	WO 2016/189841 A1 (NEC CORP.) 01 December 2016 & US 2018/0159897 A1	1-15

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. G06F21/55(2013.01)i, B60R16/02(2006.01)i, G06F11/07(2006.01)i, H04L12/28(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. G06F21/55, B60R16/02, G06F11/07, H04L12/28

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	1971-2019年
日本国実用新案登録公報	1996-2019年
日本国登録実用新案公報	1994-2019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
X Y A	JP 2002-111726 A（ケイディーディーアイ株式会社）2002.04.12, [0012]-[0044], 図1-9 & US 2002/0046351 A1, [0024]-[0042], Figs.1-9	11-13 1-6 7-10, 14-15
Y	JP 2014-183395 A（日立オートモティブシステムズ株式会社）2014.09.29, [0020]-[0040], 図1-3（ファミリーなし）	1-6
Y	中野 学, 自動車の情報セキュリティ 初版, 第1版, 日経BP社 望月 洋介, 2013.12.27, pp.144-147, pp.152-160	5

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

01.10.2019

国際調査報告の発送日

15.10.2019

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）

岸野 徹

5 S

3983

電話番号 03-3581-1101 内線 3546

C (続き) . 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
A	JP 2002-342279 A (富士通株式会社) 2002. 11. 29, & US 2002/0133606 A1	1-15
A	針生 剛男, N T Tグループのセキュリティビジネスを支えるマルウェア対策用セキュリティインテリジェンス, N T T技術ジャーナル 第27巻 第10号, 2015. 10. 01, 第27巻, pp. 18-22	1-15
A	WO 2016/189841 A1 (日本電気株式会社) 2016. 12. 01, & US 2018/0159897 A1	1-15