(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
2025年1月16日(16.01.2025)

WIPO | PCT

(10) 国際公開番号
WO 2025/013272 A1

(51) 国際特許分類:
G06F 21/55 (2013.01)

(21) 国際出願番号： PCT/JP2023/025835

(22) 国際出願日： 2023年7月13日(13.07.2023)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(71) 出願人:日立Ａｓｔｅｍｏ株式会社(**HITACHI ASTEMO, LTD.**) [JP/JP]; 〒3128503 茨城県ひたちなか市高場２５２０番地 Ibaraki (JP).

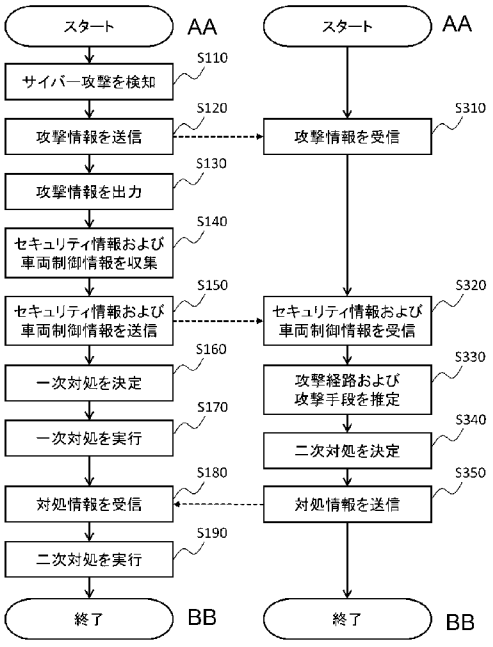
(72) 発明者:前田 功治(**MAEDA Koji**); 〒3128503 茨城県ひたちなか市高場２５２０番地 日立Ａｓｔｅｍｏ株式会社内 Ibaraki (JP). 前濱 宏樹(**MAEHAMA Hiroki**); 〒3128503 茨城県ひたちなか市高場２５２０番地 日立Ａｓｔｅｍｏ株式会社内 Ibaraki (JP). 村上 隆(**MURAKAMI Takashi**); 〒3128503 茨城県ひたちなか市高場２５２０番地 日立Ａｓｔｅｍｏ株式会社内 Ibaraki (JP).

(74) 代理人: 弁理士法人開知(**KAICHI IP**); 〒1030022 東京都中央区日本橋室町四丁目３番１６号 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, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR,

(54) **Title:** VEHICLE CONTROL SYSTEM

(54) 発明の名称： 車両制御システム



S110... Detect cyber attack
S120... Transmit attack information
S130... Output attack information
S140... Collect security information and vehicle control information
S150... Transmit security information and vehicle control information
S160... Determine primary countermeasure
S170... Execute primary countermeasure
S180... Receive countermeasure information
S190... Execute secondary countermeasure
S310... Receive attack information
S320... Receive security information and vehicle control information
S330... Estimate attack path and attack means
S340... Determine secondary countermeasure
S350... Transmit countermeasure information
AA ... Start
BB ... End

(57) **Abstract:** A vehicle control system includes a plurality of control devices and is mounted on a vehicle. At least one control device among the plurality of control devices comprises an arithmetic device. The arithmetic device: detects a cyber attack on the plurality of control devices; implements, against the cyber attack, a primary countermeasure to prevent the cyber attack or another cyber attack subsequent to the cyber attack, or to mitigate the influence thereof; transmits attack information related to the cyber attack to a center device provided outside the vehicle; receives countermeasure information corresponding to the attack information from the center device after implementing the primary countermeasure; and implements a secondary countermeasure different from the primary countermeasure on the basis of the countermeasure

WO 2025/013272 A1

[続葉有]

HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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))

information.

(57) 要約:車両制御システムは、複数の制御装置を備え、車両に搭載される。複数の制御装置のうち少なくとも１つの制御装置は演算装置を備える。演算装置は、複数の制御装置に対するサイバー攻撃を検知し、サイバー攻撃に対して、サイバー攻撃またはサイバー攻撃に引き続く他のサイバー攻撃を防止するもしくはその影響を緩和する第１対処を実施し、サイバー攻撃に関する攻撃情報を車両の外部に設けられたセンタ装置に送信し、第１対処の実施後に、センタ装置から攻撃情報に対応する対処情報を受信し、対処情報に基づき第１対処とは異なる第２対処を実施する。

明　細　書

発明の名称 ： 車両制御システム

技術分野

[0001]　本発明は、車両制御システムに関する。

背景技術

[0002]　サイバー攻撃に対する防御手段を備えた車両制御装置が知られている。例えば特許文献１には、車載装置が車両において収集したログを車両外部のセンタ装置に送信し、暫定装置の要否をセンタ装置において判断し、暫定措置が必要と判断した場合、暫定措置実行指示を車載装置に送信する不正侵入防止装置が記載されている。

先行技術文献

特許文献

[0003] 特許文献1：特開２０２２－１７８７３号公報

発明の概要

発明が解決しようとする課題

[0004]　特許文献１に記載の技術には、車両の外部に設けられたセンタ装置からの指示を待ってからサイバー攻撃に対する対処を実施するため、サイバー攻撃を受けてから対処を実施するまでのタイムラグが長くなるという問題がある。

[0005]　本発明は、サイバー攻撃を受けてから対処を実施するまでの時間を短縮することが可能な車両制御システムを提供することを目的とする。

課題を解決するための手段

[0006]　本発明の一態様による車両制御システムは、複数の制御装置を備えた、車両に搭載される車両制御システムであって、前記複数の制御装置のうち少なくとも１つの制御装置は演算装置を備え、前記演算装置は、前記複数の制御装置に対するサイバー攻撃を検知し、前記サイバー攻撃に対して、前記サイバー攻撃または前記サイバー攻撃に引き続く他のサイバー攻撃を防止するも

しくはその影響を緩和する第１対処を実施し、前記サイバー攻撃に関する攻撃情報を前記車両の外部に設けられたセンタ装置に送信し、前記第１対処の実施後に、前記センタ装置から前記攻撃情報に対応する対処情報を受信し、前記対処情報に基づき前記第１対処とは異なる第２対処を実施する。

発明の効果

[0007] 本発明によれば、サイバー攻撃を受けてから対処を実施するまでの時間を短縮することができる。

図面の簡単な説明

[0008] [図1]図１は、第１実施形態に係る車両制御システムのハードウェア構成を模式的に示すブロック図である。

[図2]図２は、第１実施形態に係る車両制御システムの機能構成を模式的に示すブロック図である。

[図3]図３は、車両制御システムが実行する処理のフローチャートである。

[図4]図４は、車両制御装置で実施される二次対処の説明図である。

[図5]図５は、第２実施形態に係る車両制御システムが実行する処理のフローチャートである。

[図6]図６は、第３実施形態に係る車両制御システムの機能構成を模式的に示すブロック図である。

[図7]図７は、第４実施形態に係る車両制御システムの機能構成を模式的に示すブロック図である。

[図8]図８は、ソフトウェアの配置を変更する対処の説明図である。

[図9]図９は、各ＥＣＵのＩＤを変更する対処の説明図である。

[図10]図１０は、縮退ソフトウェアを実行する対処の説明図である。

発明を実施するための形態

[0009] ＜第１実施形態＞

図１～図４を参照して、本発明の第１実施形態に係る車両制御システム１について説明する。

[0010] 図１は、第１実施形態に係る車両制御システム１のハードウェア構成を模

式的に示すブロック図である。車両制御システム１は、車両２に搭載される車両制御装置３と、車両２の外部に設けられるセンタ装置４とを含む。なお、車両制御システム１は、複数の車両２および車両制御装置３を有していてもよい。図１では１組の車両２および車両制御装置３のみを例示している。

[0011] 車両制御装置３は、無線通信網５に接続するためのアンテナ３０を備える。センタ装置４は、無線通信網５に接続するためのアンテナ４０を備える。車両制御装置３およびセンタ装置４は、無線通信網５を介して相互にデータ通信が可能に構成される。無線通信網５は、例えば複数の基地局を含む携帯電話網や、複数の通信衛星を含む衛星通信網などである。

[0012] 車両制御装置３は、車両２の各部を制御する制御装置である。車両制御装置３は、複数のＥＣＵを備える。図１では、車両制御装置３が備える複数のＥＣＵとして、第１ＥＣＵ３２ａ、第２ＥＣＵ３２ｂ、第３ＥＣＵ３２ｃ、および第４ＥＣＵ３２ｄを例示している。以下の説明では、これらのＥＣＵをＥＣＵ３２と総称する。

[0013] 第１ＥＣＵ３２ａは、アンテナ３０および第２ＥＣＵ３２ｂに接続される。第２ＥＣＵ３２ｂ、第３ＥＣＵ３２ｃ、および第４ＥＣＵ３２ｄは相互に接続される。なお、ここで説明した複数のＥＣＵ３２の接続形態は一例である。ＥＣＵ３２間の接続形態は、ＥＣＵ３２の数や用途などによって適宜決定される。

[0014] 第１ＥＣＵ３２ａは、ＣＰＵ（Central Processing Unit）、ＭＰＵ（Micro Processing Unit）、ＤＳＰ（Digital Signal Processor）等の演算装置５１、ＲＯＭ（Read Only Memory）、フラッシュメモリ、ハードディスクドライブ等の不揮発性メモリ５２、所謂ＲＡＭ（Random Access Memory）と呼ばれる揮発性メモリ５３、入出力インタフェース５４、及び、その他の周辺回路を備えたコンピュータで構成される。これらのハードウェアは、協働してソフトウェアを動作させ、複数の機能を実現する。なお、第１ＥＣＵ３２ａは、１つのコンピュータで構成してもよいし、複数のコンピュータで構成してもよい。また、演算装置５１としては、ＡＳＩＣ（application specific

integrated circuit）、ＦＰＧＡ（Field Programmable Gate Array）などを用いることができる。

[0015] 不揮発性メモリ５２には、各種演算が実行可能なプログラムが格納されている。すなわち、不揮発性メモリ５２は、本実施形態の機能を実現するプログラムを読み取り可能な記憶媒体（記憶装置）である。揮発性メモリ５３は、演算装置５１による演算結果及び入出力インタフェース５４から入力された信号を一時的に記憶する記憶媒体（記憶装置）である。演算装置５１は、不揮発性メモリ５２に記憶されたプログラムを揮発性メモリ５３に展開して演算実行する装置であって、プログラムに従って入出力インタフェース５４、不揮発性メモリ５２及び揮発性メモリ５３から取り入れたデータに対して所定の演算処理を行う。

[0016] 入出力インタフェース５４の入力部は、各種装置（アンテナ３０、第２ＥＣＵ３２ｂ等）から入力された信号を演算装置５１で演算可能なデータに変換する。また、入出力インタフェース５４の出力部は、演算装置５１での演算結果に応じた出力用の信号を生成し、その信号を各種装置（アンテナ３０、第２ＥＣＵ３２ｂ等）に出力する。

[0017] なお、第２ＥＣＵ３２ｂ、第３ＥＣＵ３２ｃ、および第４ＥＣＵ３２ｄのハードウェア構成は、第１ＥＣＵ３２ａと同一であるので図示および説明を省略する。つまり、複数のＥＣＵ３２は、いずれも第１ＥＣＵ３２ａと同様に、演算装置５１、不揮発性メモリ５２、揮発性メモリ５３、および入出力インタフェース５４を備えている。

[0018] 車両２は、不図示のセンサやアクチュエータ等を有している。これらのセンサやアクチュエータ等は、複数のＥＣＵ３２のうち少なくともいずれか１つに接続される。

[0019] センタ装置４は、ＣＰＵ、ＭＰＵ、ＤＳＰ等の演算装置４１、ＲＯＭ、フラッシュメモリ、ハードディスクドライブ等の不揮発性メモリ４２、所謂ＲＡＭと呼ばれる揮発性メモリ４３、入出力インタフェース４４、及び、その他の周辺回路を備えたコンピュータで構成される。これらのハードウェアは

、協働してソフトウェアを動作させ、複数の機能を実現する。なお、センタ装置４は、１つのコンピュータで構成してもよいし、複数のコンピュータで構成してもよい。また、演算装置４１としては、ＡＳＩＣ、ＦＰＧＡなどを用いることができる。

[0020] 不揮発性メモリ４２には、各種演算が実行可能なプログラムが格納されている。すなわち、不揮発性メモリ４２は、本実施形態の機能を実現するプログラムを読み取り可能な記憶媒体（記憶装置）である。揮発性メモリ４３は、演算装置４１による演算結果及び入出力インタフェース４４から入力された信号を一時的に記憶する記憶媒体（記憶装置）である。演算装置４１は、不揮発性メモリ４２に記憶されたプログラムを揮発性メモリ４３に展開して演算実行する装置であって、プログラムに従って入出力インタフェース４４、不揮発性メモリ４２及び揮発性メモリ４３から取り入れたデータに対して所定の演算処理を行う。

[0021] 入出力インタフェース４４の入力部は、各種装置（アンテナ４０等）から入力された信号を演算装置４１で演算可能なデータに変換する。また、入出力インタフェース４４の出力部は、演算装置４１での演算結果に応じた出力用の信号を生成し、その信号を各種装置（アンテナ４０等）に出力する。入出力インタフェース４４の入力部には、無線通信網５に接続される車両制御装置３や不図示の装置から、それぞれの車両２の現在位置を表す位置情報や、車両２を安全に停止させることができる場所が記録された地図情報も入力される。

[0022] なお、車両制御装置３がセンタ装置４等の外部装置と通信する手段は、無線通信網５を介した無線通信に限らない。例えば有線通信であってもよい。

[0023] 図２は、第１実施形態に係る車両制御システム１の機能構成を模式的に示すブロック図である。第１ＥＣＵ３２ａは、無線通信網５に接続された各種装置と、車両制御装置３が備える他のＥＣＵ３２とのデータ通信を中継する。第２ＥＣＵ３２ｂは、通信部６１およびセキュリティエージェント６２を備える。第２ＥＣＵ３２ｂ上では、所定のアプリケーション６３が動作する

。通信部６１は、第１ＥＣＵ３２ａを介して無線通信網５に接続された各種装置とデータ通信を行う機能をアプリケーション６３およびセキュリティエージェント６２に提供する。アプリケーション６３は、例えば不図示のアクチュエータを制御する、不図示のセンサによる計測値を無線通信網５を介して外部に送信する、不図示の表示装置にメッセージを表示する、無線通信網５を介して外部から受信したデータを表示および保存する、等の種々の処理を行う、いわゆるアプリケーションプログラムである。

[0024] セキュリティエージェント６２は、検知部６４、収集部６５、および対処部６６を備える。検知部６４は、車両制御装置３に対するサイバー攻撃を検知する。車両制御装置３に対するサイバー攻撃とは、例えばいずれかのＥＣＵ３２上で動作するアプリケーション６３に対するサイバー攻撃や、いずれかのＥＣＵ３２の通信部６１へのサイバー攻撃などである。検知部６４が検知するサイバー攻撃は、例えばなりすまし等による認証の不正な通過や、大量のデータを送り込むことによるサービス拒否（Denial of Service）攻撃などである。

[0025] なお、サイバー攻撃は無線通信網５を介した外部通信によるものに限定されない。例えば検知部６４を、不図示のセンサやアクチュエータに対して直接サイバー攻撃を受けたり、装置間の伝送路に取り付けられた不正な装置により直接サイバー攻撃を受けた場合であっても、それらのサイバー攻撃を検知できるよう構成してよい。

[0026] 検知部６４は、検知したサイバー攻撃に関する攻撃情報を収集部６５および対処部６６に出力する。検知部６４は、攻撃情報をセンタ装置４に送信する。攻撃情報は、サイバー攻撃を受けたことを表す情報である。攻撃情報には、例えば攻撃対象となったＥＣＵ３２を特定するＩＤ、サイバー攻撃の種別（なりすまし、サービス拒否など）、サイバー攻撃の種別に応じた特徴（なりすましならなりすまし対象の認証情報、サービス拒否攻撃ならデータの送出頻度）など、サイバー攻撃そのものに関する情報が含まれる。攻撃情報には更に、そのサイバー攻撃によって損なわれる（もしくは損なわれうる）

機能に関する情報、すなわちサイバー攻撃による被害状況に関する情報が含まれていてもよい。

[0027] 収集部６５は、検知部６４が出力した攻撃情報に基づき、セキュリティ情報および車両制御情報を収集する。セキュリティ情報は、通信部６１の通信ログ情報、アプリケーション６３の動作ログ情報など、サイバー攻撃を分析するための情報である。車両制御情報は、車両２の位置情報や車両２を安全に停車可能な場所を示す地図情報など、車両２の制御に関する情報である。収集部６５は、収集したセキュリティ情報および車両制御情報を対処部６６に出力する。収集部６５は、収集したセキュリティ情報および車両制御情報をセンタ装置４に送信する。対処部６６は、検知部６４が出力した攻撃情報と、収集部６５が出力したセキュリティ情報および車両制御情報とに基づき、検知されたサイバー攻撃への対処を決定し実行する。例えば、サイバー攻撃の経路や攻撃手段の組み合わせそれぞれに対して、対応する対処方法を予め不揮発性メモリ５２にテーブル等の形態で格納しておき、このテーブルを検索することで適切な対処方法を特定する。自車両内で収集された情報に基づき対処部６６が実行するサイバー攻撃への対処を、一次対処と称する。一次対処は、センタ装置４の指示等によらず、車両制御装置３が独自の判断で実行する。センタ装置４が介在しないので、一次対処はサイバー攻撃が検知され次第速やかに実行される。

[0028] 一次対処としては、例えば車両２のドライバーにサイバー攻撃を通知し車両２が自動運転モードであった場合は手動運転に切り替えるように促す、車両２のハザードやＬＥＤ表示、車両間通信等でサイバー攻撃を受けていることを周囲の車両に伝え安全を確保する、などの処理が考えられる。また、安全性を検討した上で、サイバー攻撃を受けたネットワークを遮断したり、サイバー攻撃を受けたシステムやＥＣＵ３２を再起動するといった対処を実行してもよい。

[0029] センタ装置４は、通信部７１および分析部７２を備える。通信部７１は、車両制御装置３から送信された攻撃情報、セキュリティ情報、および車両制

御情報を受信する。分析部７２は、通信部７１により受信された攻撃情報、セキュリティ情報、および車両制御情報を分析し、サイバー攻撃への対処を決定する。例えば、アプリケーション６３の通信ログや通信部６１の通信ログから通信量を算出し、通常時の通信量と比較する。通信量が通常時よりも増大していれば、サービス拒否攻撃の可能性が考えられるので、サービス拒否攻撃への対処を決定する。また、セキュリティ機能の動作ログを参照することで、これまでにどのような対策が実施されたかを特定し、それらとは異なる対処を決定することができる。他にも、複数の車両２から同様のサイバー攻撃が検知されていれば、大規模攻撃がなされていると判断し、複数の車両２でより強力な対処（通常とは異なる対処）を実行することにしてもよい。

[0030] 通信部７１は、分析部７２により決定された対処の内容を表す対処情報を、受信した攻撃情報、セキュリティ情報、および車両制御情報への応答として、それらの情報を送信してきた車両制御装置３に向けて送信する。換言すると、通信部７１は、分析部７２により決定された対処を実行するよう車両制御装置３に指示する。車両制御装置３の対処部６６は、通信部６１を介してセンタ装置４から送信された対処情報を受信すると、その対処情報により表される対処を実行する。センタ装置４の指示に基づき対処部６６が実行するサイバー攻撃への対処を、二次対処と称する。センタ装置４からの指示を待つ必要があるため、二次対処は一次対処に比べて実行タイミングが遅くなる。

[0031] 二次対処としては、例えばサイバー攻撃を受けている車両２の近くを走行する他の車両に対して無線通信を行い、サイバー攻撃を受けた車両２が近くを走行している旨をナビゲーションシステムで通知したり、あるいは電光掲示板のようなインフラを介して通知することが考えられる。また、サイバー攻撃を受けた車両２のログを解析し、新たなセキュリティ対策ルールやソフトを作成し、車両制御装置３に配信してもよい（いわゆるＯＴＡ更新）。さらに、外部からサイバー攻撃を受けた車両２の遠隔操縦を行って、車両２を

安全に停止させる措置をとってもよい。また、周辺を走行する車両が、サイバー攻撃を受けた車両２からの情報（動作ログ等）を受信し、その情報に基づき車両制御装置３が有していないパターンの対処や新たな情報収集をサイバー攻撃を受けた車両制御装置３に指示してもよい。また、二次対処の内容はシステム管理者が手動で決定してもよい。

[0032] なお、第３ＥＣＵ３２ｃおよび第４ＥＣＵ３２ｄの機能構成は、第２ＥＣＵ３２ｂと同一であるので図示および説明を省略する。すなわち、第２ＥＣＵ３２ｂ、第３ＥＣＵ３２ｃ、および第４ＥＣＵ３２ｄは、それぞれが上述したセキュリティエージェント６２を有している。車両２のどこかにサイバー攻撃が行われたとき、サイバー攻撃が行われた箇所（サイバー攻撃の標的になった地点）に最も近いセキュリティエージェント６２がそのサイバー攻撃を検知し、必要な対処を行う。例えばあるＥＣＵ３２上で動作しているアプリケーション６３に対してサイバー攻撃が行われた場合は、そのＥＣＵ３２が有するセキュリティエージェント６２がサイバー攻撃を検知する。また、サイバー攻撃が行われた箇所に対して、ほとんど同じ近さで複数のＥＣＵ３２が存在する場合には、それら複数のＥＣＵ３２のうちのいずれかが有するセキュリティエージェント６２がサイバー攻撃を検知すればよい。なお、サイバー攻撃が行われた箇所とセキュリティエージェント６２との近さは、物理的な距離で決定してもよいし、通信距離で決定してもよいし、その他任意の基準で決定してもよい。

[0033] 図３は、車両制御システム１が実行する処理のフローチャートである。まず、車両制御装置３側の処理について説明する。

[0034] ステップＳ１１０において検知部６４が、車両制御装置３に対するサイバー攻撃を検知する。ステップＳ１２０において検知部６４は、ステップＳ１１０で検知したサイバー攻撃に関する攻撃情報をセンタ装置４に送信する。ステップＳ１３０において検知部６４は、ステップＳ１１０で検知したサイバー攻撃に関する攻撃情報を収集部６５および対処部６６に出力する。ステップＳ１４０において収集部６５が、セキュリティ情報および車両制御情報

を収集する。ステップＳ１５０において収集部６５が、セキュリティ情報および車両制御情報をセンタ装置４に送信する。

[0035] ステップＳ１６０において対処部６６が、ステップＳ１３０で検知部６４から入力された攻撃情報と、ステップＳ１４０で収集部６５により収集されたセキュリティ情報および車両制御情報とに基づき、検知されたサイバー攻撃への一次対処を決定する。ステップＳ１７０において対処部６６が、ステップＳ１６０で決定したサイバー攻撃への一次対処を実行する。ステップＳ１８０において対処部６６が、ステップＳ１５０で収集部６５により送信されたセキュリティ情報および車両制御情報に対応する対処情報を、センタ装置４から受信する。ステップＳ１９０において対処部６６が、ステップＳ１８０で受信した対処情報に基づく二次対処を実行する。

[0036] 次に、センタ装置４側の処理について説明する。ステップＳ３１０において分析部７２が、ステップＳ１２０で車両制御装置３の検知部６４から送信された攻撃情報を受信する。ステップＳ３２０において分析部７２が、ステップＳ１５０で車両制御装置３の収集部６５から送信されたセキュリティ情報および車両制御情報を受信する。

[0037] ステップＳ３３０において分析部７２が、ステップＳ３１０で受信した攻撃情報とステップＳ３２０で受信したセキュリティ情報および車両制御情報とに基づき、サイバー攻撃の攻撃経路や攻撃手段を推定する。ステップＳ３４０において分析部７２が、ステップＳ３３０で推定した攻撃経路や攻撃手段に基づき、状況に応じたサイバー攻撃への対処（二次対処）を決定する。ステップＳ３５０において分析部７２が、ステップＳ３４０で決定した二次対処を表す対処情報を車両制御装置３に送信する。

[0038] 図４は、車両制御装置３で実施される二次対処の説明図である。攻撃者８が特定の車両２ａに対してサイバー攻撃を行うと、サイバー攻撃を受けた車両２ａでは前述したように、センタ装置４からの指示を待たずに一次対処が実行される。その後、センタ装置４ではより多くの情報を基に二次対処の内容を決定し、サイバー攻撃を受けた車両２ａに対して決定した二次対処を実

行するよう指示する（対処情報を送信する）。このとき、まだサイバー攻撃を受けていない他の車両２ｂに対して、サイバー攻撃を受けた車両２ａに二次対処として指示したものと同様の対処を実行するよう指示（対処情報を送信）してもよい。例えば、二次対処として新たなセキュリティ対策ルールやソフトを作成し、サイバー攻撃を受けた車両２ａに配信するとともに、まだ攻撃を受けていない車両２ｂに対しても同様にそれらを配信してよい。このようにすることで、サイバー攻撃に対する予防措置を施すことができ、社会全体のサイバー攻撃に対する耐性が向上する。なお、サイバー攻撃を受けていない車両２ｂでは一次対処は実行されていないが、サイバー攻撃を受けた車両２ａで実行される二次対処と同様の対処を実行した場合、その対処を二次対処と定義する。

[0039] 第１実施形態によれば、次の作用効果を奏する。

[0040] （１）演算装置５１は、複数のＥＣＵ３２（制御装置）に対するサイバー攻撃を検知し、そのサイバー攻撃またはそれに引き続く他のサイバー攻撃を防止するもしくはその影響を緩和する一次対処（第１対処）を実施する。その後、サイバー攻撃に関する攻撃情報を車両２の外部に設けられたセンタ装置４に送信し、一次対処（第１対処）の実施後に、センタ装置４から攻撃情報に対応する対処情報を受信し、対処情報に基づき一次対処（第１対処）とは異なる二次対処（第２対処）を実施する。このようにしたので、サイバー攻撃を受けてから対処を実施するまでの時間を短縮することができる。

[0041] （２）複数のＥＣＵ３２（制御装置）はそれぞれ演算装置５１を備え、複数のＥＣＵ３２（制御装置）のうち、サイバー攻撃を受けた地点に最も近いＥＣＵ３２（制御装置）の演算装置５１が一次対処（第１対処）および二次対処（第２対処）を実施する。このようにしたので、サイバー攻撃に対して迅速な対処が可能となり、サイバー攻撃による被害が他のＥＣＵ３２に及ばないようにできる。

[0042] （３）車両制御システム１は、複数の車両２にそれぞれ搭載されたＥＣＵ３２に対してサイバー攻撃が行われた場合、１つのＥＣＵ３２に対してサイ

バー攻撃が行われた場合とは異なる二次対処（第２対処）を実施してもよい。センタ装置４には、複数の車両２からこれまでに送信された攻撃情報、セキュリティ情報、および車両制御情報が蓄積されているので、車両制御装置３単体よりも優れた分析を行うことができる。

[0043] （４）二次対処（第２対処）は、センタ装置４に車両２を遠隔操縦させ車両２を安全に停止させる処理とすることができる。これにより、車両２の安全性を適切に確保できる。

[0044] （５）車両制御システム１は、複数の車両２のうち少なくとも１つの車両２に搭載されたＥＣＵ３２に対してサイバー攻撃が行われた場合、サイバー攻撃が行われていない他のＥＣＵ３２においても二次対処（第２対処）を実施することが好ましい。これにより、サイバー攻撃に対する予防措置を施すことができ、社会全体のサイバー攻撃に対する耐性が向上する。

[0045] ＜第２実施形態＞

図５を参照して、本発明の第２実施形態に係る車両制御システム１について説明する。なお、第１実施形態で説明した構成と同一もしくは相当する構成には同一の参照記号を付し、相違点を主に説明する。

[0046] 図５は、図３と同様の図であり、第２実施形態に係る車両制御システム１が実行する処理のフローチャートである。図５のフローチャートでは、図３のフローチャートのステップＳ１９０の次に、ステップＳ２００～Ｓ２１０の処理が追加されている。また、ステップＳ３５０の次に、ステップＳ３６０～Ｓ３７０の処理が追加されている。

[0047] ステップＳ１９０で二次対処を実行した後、ステップＳ２００において検知部６４が、サイバー攻撃に関する攻撃情報を再度生成してセンタ装置４に送信する。ステップＳ２１０において検知部６４が、攻撃情報からサイバー攻撃が継続しているか否か、すなわちサイバー攻撃による異常が車両制御装置３において未だに検知されているか否かを判定する。サイバー攻撃が継続していた場合、すなわちこれまでに実行した対処によってサイバー攻撃の影響を緩和しきれていない（サイバー攻撃を阻止しきれていない）場合、処理

はステップＳ１３０に進み、現在の状況に応じて適切に選択された一次対処および二次対処が繰り返し実行される。他方、ステップＳ２００において、これまでに実行した対処によってサイバー攻撃の影響が十分に緩和または阻止されている場合、図５に示した処理は終了する。

[0048] センタ装置４側の処理についても同様である。すなわち、ステップＳ３５０で二次対処の指示を示す対処情報を車両制御装置３に送信した後、ステップＳ３６０において分析部７２が、ステップＳ２００で車両制御装置３の検知部６４から送信された攻撃情報を受信する。ステップＳ３７０において分析部７２が、攻撃情報からサイバー攻撃が継続しているか否か、すなわちサイバー攻撃による異常が車両制御装置３において未だに検知されているか否かを判定する。サイバー攻撃が継続していた場合、すなわちこれまでに実行した対処によってサイバー攻撃の影響を緩和しきれていない（サイバー攻撃を阻止しきれていない）場合、処理はステップＳ３２０に進み、再度セキュリティ情報および車両制御情報を受信し、現在の状況に応じて適切に選択された二次対処を車両制御装置３に繰り返し実行させる。他方、ステップＳ３７０において、これまでに実行した対処によってサイバー攻撃の影響が十分に緩和または阻止されている場合、図５に示した処理は終了する。

[0049] 以上のように、第２実施形態に係る車両制御システム１は、サイバー攻撃の影響がなくなるまで、最新の状況に応じた一次対処および二次対処を繰り返し決定し実行することにより、サイバー攻撃を確実に阻止しようとする。特許文献１で示された方法では、一度の対処で問題を解決出来なかった場合や、対処の途中でサイバー攻撃の内容が変化した場合に、それ以上の対処が出来ないため、車両を安全な状態にできない可能性があった。第２実施形態に係る車両制御システム１によって、一次対処、二次対処によって問題が解決されない場合やサイバー攻撃の内容が変化した場合においても、情報収集の方法や対処方法を次々に変化させることができる。車両２側で受けたサイバー攻撃の内容やその進行状態に合わせて対処方法を変えていくことで、サイバー攻撃の被害を最小化しながら他の車両２も含めてより多くの情報を収

集することが可能になる。センタ装置４側では、時間的な余裕が生まれ、またより多くの情報が集まることから、より適切な対処方法を選択することが可能になる。

[0050] 第２実施形態によれば、次の作用効果を奏する。

[0051] （１）演算装置５１は、検知したサイバー攻撃またはそのサイバー攻撃に引き続く他のサイバー攻撃の防止、もしくはその影響の緩和に成功するまで、新たな攻撃情報の送信、一次対処（第１対処）の実施、および二次対処（第２対処）の実施を繰り返し行う。このようにしたので、より確実にサイバー攻撃の影響を免れることができる。

[0052] ＜第３実施形態＞

図６を参照して、本発明の第３実施形態に係る車両制御システム１００について説明する。なお、第１実施形態で説明した構成と同一もしくは相当する構成には同一の参照記号を付し、相違点を主に説明する。

[0053] 図６は、図１と同様の図であり、第３実施形態に係る車両制御システム１００の機能構成を模式的に示すブロック図である。図６のブロック図では、図１の各部に加えて、車両制御装置３に第５ＥＣＵ３２ｅが追加されている。第５ＥＣＵ３２ｅにはアンテナ３０ａが接続される。第５ＥＣＵ３２ｅは第３ＥＣＵ３２ｃと接続されている。無線通信網５を介して第１ＥＣＵ３２ａにサイバー攻撃が加えられ、第１ＥＣＵ３２ａを介したデータ通信ができなくなった場合、一次対処は可能であるものの、センタ装置４と連携したサイバー攻撃への二次対処を行うことが困難となる。そのため、本実施形態ではセンタ装置４との通信手段を冗長化している。

[0054] 第３実施形態に係る車両制御システム１００は、サイバー攻撃により外部とのデータ通信を担当する第１ＥＣＵ３２ａを介したデータ通信ができなくなったとしても、第５ＥＣＵ３２ｅを介してセンタ装置４とのデータ通信を行うことができるので、二次対処の指示を確実に受信することができる。そのため、サイバー攻撃に対してより堅牢な車両制御システムを提供することができる。なお、第５ＥＣＵ３２ｅによるセンタ装置４とのデータ通信方式

は、第１ＥＣＵ３２ａによるものと異なっていてもよい。例えば、第５ＥＣＵ３２ｅとセンタ装置４とが有線により接続されていてもよい。

[0055] 第３実施形態によれば、次の作用効果を奏する。

[0056] （１）ＥＣＵ３２（制御装置）は、センタ装置４との通信路を複数有する。このようにしたので、サイバー攻撃に対してより堅牢な車両制御システム１００を提供することができる。

[0057] ＜第４実施形態＞

図７～図１０を参照して、本発明の第４実施形態に係る車両制御システム２００について説明する。なお、第１実施形態で説明した構成と同一もしくは相当する構成には同一の参照記号を付し、相違点を主に説明する。

[0058] 図７は、図２と同様の図であり、第４実施形態に係る車両制御システム２００の機能構成を模式的に示すブロック図である。図７のブロック図では、図１の各部に加えて、車両制御装置３に統括ＥＣＵ３２ｆが追加されている。統括ＥＣＵ３２ｆは他のＥＣＵ３２と接続されている。統括ＥＣＵ３２ｆは、複数のＥＣＵ３２の状態を把握し、複数のＥＣＵ３２に対して設定変更を行う。統括ＥＣＵ３２ｆは、複数のＥＣＵ３２に対してソフトウェアの配置やネットワークの状態を変更する機能を有する。統括ＥＣＵ３２ｆは、各ＥＣＵ３２の通信ログや各ＥＣＵ３２が提供する機能の状態ログを各ＥＣＵ３２から収集し、最適な機能配置および通信設定を演算する。

[0059] 統括ＥＣＵ３２ｆに車両２全体のセキュリティや各ＥＣＵ３２の状態に関する情報を集約しているため、安全確保に向けた対処を行いつつ、サイバー攻撃に関する情報収集を継続するといった対応が可能となる。例えば、第２ＥＣＵ３２ｂがサイバー攻撃を受けた場合に、第２ＥＣＵ３２ｂ上で動作しているアプリケーション６３を他のＥＣＵ３２へ移動させ、車両２を安全に停止するといった安全行動をとりつつ、第２ＥＣＵ３２ｂに対するサイバー攻撃は継続させてサイバー攻撃に関する情報収集を継続してもよい。

[0060] 図８は、ソフトウェアの配置を変更する対処の説明図である。いま、第２ＥＣＵ３２ｂでは車両２を安全に停止するために必要なアプリケーション６

３ａが動作し、第３ＥＣＵ３２ｃでは比較的重要でないアプリケーション６３ｂが動作しているものとする。例えば第２ＥＣＵ３２ｂがサイバー攻撃を受けた場合、統括ＥＣＵ３２ｆは、第３ＥＣＵ３２ｃで動作していた比較的重要でないアプリケーション６３ｂを停止させ、第２ＥＣＵ３２ｂで動作していたアプリケーション６３ａを第３ＥＣＵ３２ｃ上で動作開始させる。アプリケーション６３ｂを停止させるのは、アプリケーション６３ａの動作に必要な計算資源を確保するためである。なお、第３ＥＣＵ３２ｃにアプリケーション６３ａを読み込ませるには、第２ＥＣＵ３２ｂから第３ＥＣＵ３２ｃにアプリケーション６３ａを送信させてもよいし、あらかじめ第３ＥＣＵ３２ｃの不揮発性メモリ５２にアプリケーション６３ａを格納しておいてもよい。

[0061] 移動対象のアプリケーション６３ａが特定の通信先（例えば他のＥＣＵ３２、センサ、アクチュエータ等）と通信を行うことで動作していた場合、第２ＥＣＵ３２ｂから第３ＥＣＵ３２ｃにアプリケーション６３ａを移動させると、アプリケーション６３ａがその特定の通信先と通信を行うことができなくなる場合がある。そのような場合は、統括ＥＣＵ３２ｆに通信部６１の設定を変更させ、アプリケーション６３ａの移動先である第３ＥＣＵ３２ｃとその特定の通信先とが通信できるようにすればよい。

[0062] このように、ソフトウェアの配置および通信設定を変更することにより、特定のＥＣＵ３２がサイバー攻撃を受けても、必要な演算を他のＥＣＵ３２に代わりに実行させることができ、車両２の安全を確保することができる。

[0063] なお、複数のＥＣＵ３２間でソフトウェアの配置を変更したり通信設定を変更したりする場合、ＥＣＵ３２同士が個別にそのような変更を行うと、車両制御装置３全体の状態を把握することが困難になる。また、個々のＥＣＵ３２が現在の状態を把握していなければならず非効率である。そこで統括ＥＣＵ３２ｆは、各ＥＣＵ３２のセキュリティエージェント６２からの情報を集約することで、どのＥＣＵ３２の負荷に余裕があるか、各ＥＣＵ３２間の通信量にどの程度の余裕があるかを把握する。サイバー攻撃を受けた場合、

統括ＥＣＵ３２ｆは、それらの把握していた情報を用いて、複数のＥＣＵ３２に跨る最適な対処方法を各ＥＣＵ３２に設定する。

[0064] なお、統括ＥＣＵ３２ｆは単独のＥＣＵであってもよいし、他のＥＣＵが統括ＥＣＵ３２ｆの役割を兼ねていてもよい。また、統括ＥＣＵ３２ｆは１つだけ存在していてもよいし、故障やサイバー攻撃に備えて複数存在していてもよい。

[0065] 図９は、各ＥＣＵのＩＤを変更する対処の説明図である。第２ＥＣＵ３２ｂ、第３ＥＣＵ３２ｃ、第４ＥＣＵ３２ｄのいずれかのセキュリティエージェント６２がサイバー攻撃を検知すると、そのセキュリティエージェント６２は統括ＥＣＵ３２ｆにサイバー攻撃を通知する。統括ＥＣＵ３２ｆは、他の各ＥＣＵ３２に付されているＩＤを変更すると共に、そのＩＤの変更を各ＥＣＵ３２に通知する。ＥＣＵ３２に付されているＩＤは、例えばＩＰアドレスやＭＡＣアドレスなど、各ＥＣＵ３２で一意な識別子である。ＥＣＵ３２は、通信相手を特定するためにこのＩＤを用いる。例えば図９において、第２ＥＣＵ３２ｂにはＩＤ＝Ａが付されており、第３ＥＣＵ３２ｃにはＩＤ＝Ｂが付されているものとする。サイバー攻撃の通知を受けた統括ＥＣＵ３２ｆは、第２ＥＣＵ３２ｂのＩＤをＡからＡ’に、第３ＥＣＵ３２ｃのＩＤをＢからＢ’に、それぞれ変更する。

[0066] このように、各ＥＣＵのＩＤを変更することで、攻撃者は攻撃先のＩＤを見失い、連続的な攻撃が困難になる。一方、車両制御装置３内では、各ＥＣＵ３２のＩＤが変わったものの、統括ＥＣＵ３２ｆがＩＤの変更を把握しており、変更内容を各ＥＣＵ３２に通知することで変更前と同様の通信を行うことができる。サイバー攻撃の前後で同じ処理を継続できるため、車両２の安全な走行および停車が可能となる。

[0067] なお、統括ＥＣＵ３２ｆのＩＤも併せて変更してもよい。また、ＥＣＵ３２同士の接続にイーサネットスイッチが用いられている場合、通信アクセスを制御するためのリストとしてＡＣＬ（Access Control List）が存在するので、制御したいＥＣＵ３２に対応するＡＣＬのエントリをすべて書き換えて

もよい。また、ＡＣＬとは別に通信先のアドレスが格納されたメモリを有している場合は、そのメモリの値を書き換えてもよい。

[0068] 図１０は、縮退ソフトウェアを実行する対処の説明図である。例えば第２ＥＣＵ３２ｂがサイバー攻撃を受けた場合、第２ＥＣＵ３２ｂ上で動作していた、車両２を安全に停止させるために必要なアプリケーション６３ａが動作不能になる可能性がある。図９では、アプリケーション６３ａを他のＥＣＵ３２に移動させて動作させる例を説明したが、他のＥＣＵ３２にアプリケーション６３ａを動作させるための十分な計算資源がない可能性もある。このような場合、アプリケーション６３ａよりも性能は劣るが、アプリケーション６３ａよりも低負荷で車両２を安全に停止させることができる縮退アプリケーション６３ｘを、アプリケーション６３ａの代わりに実行させてもよい。

[0069] 縮退アプリケーション６３ｘを実行させる手順は、図９の場合と同様である。すなわち、まず第３ＥＣＵ３２ｃ上で動作していた比較的重要でないアプリケーション６３ｂを停止させることで、第３ＥＣＵ３２ｃに必要な計算資源を確保する。その後、縮退アプリケーション６３ｘを第３ＥＣＵ３２ｃ上で動作開始させる。このとき、第２ＥＣＵ３２ｂ上で動作しているアプリケーション６３ａは、停止させてもよいし、そのまま動作させ続けてもよい。また、第３ＥＣＵ３２ｃの計算資源に余裕がある場合、縮退アプリケーション６３ｘがサイバー攻撃の前から（最初から）動作していてもよい。また、アプリケーション６３ａが特定の通信先（例えば他のＥＣＵ３２、センサ、アクチュエータ等）と通信を行うことで動作していた場合、統括ＥＣＵ３２ｆに通信部６１の設定を変更させ、縮退アプリケーション６３ｘが動作する第３ＥＣＵ３２ｃとその特定の通信先とが通信できるようにすればよい。

[0070] このように、縮退アプリケーション６３ｘを動作させることで、第２ＥＣＵ３２ｂがサイバー攻撃を受けた場合であっても、車両２を安全に停車させることが可能になる。縮退アプリケーション６３ｘはサイバー攻撃を受けたＥＣＵとは別のＥＣＵで実行されるため、車両２の安全性が向上する。なお

、縮退アプリケーション６３ｘが動作する第３ＥＣＵ３２ｃは、第２ＥＣＵ３２ｂのバックアップとして機能するため、第２ＥＣＵ３２ｂと第３ＥＣＵ３２ｃとでそれぞれ別の電源を用意しておいてもよい。このようにすることで、車両制御システム２００の冗長性が向上し、サイバー攻撃を受けた場合の安全性がより向上する。

[0071] 第４実施形態によれば、次の作用効果を奏する。

[0072] （１）二次対処（第２対処）は、複数のＥＣＵ３２（制御装置）の各々を特定するための一意な識別子を変更する処理、サイバー攻撃を受けたＥＣＵ３２（制御装置）のアプリケーション６３（少なくとも一部の機能）を他のＥＣＵ３２（制御装置）に移動させる処理、およびサイバー攻撃を受けたＥＣＵ３２（制御装置）のアプリケーション６３（少なくとも一部の機能）と同等の縮退アプリケーション６３ｘ（機能）を他のＥＣＵ３２（制御装置）に実現させる処理のいずれかである。このようにしたので、サイバー攻撃を受けた場合の安全性がより向上する。

[0073] （２）複数のＥＣＵ３２（制御装置）のうち統括ＥＣＵ３２ｆ（制御装置）は、識別子またはアプリケーション６３（一部の機能）を統合制御し、演算装置５１による二次対処（第２対処）の実施を管理する。このようにしたので、車両制御装置３全体の状態を効率的に把握することができる。

[0074] 次のような変形例も本発明の範囲内であり、変形例に示す構成と上述の実施形態で説明した構成を組み合わせたり、上述の異なる実施形態で説明した構成同士を組み合わせたり、以下の異なる変形例で説明する構成同士を組み合わせることも可能である。

[0075] ＜変形例１＞

第１実施形態では、サイバー攻撃を受けた地点から一番近いＥＣＵ３２のセキュリティエージェント６２がサイバー攻撃への対処を実行した。しかしながら、対処の形態はこれに限定されない。例えば、計算資源に余裕のあるＥＣＵ３２（すなわち、計算資源の多いＥＣＵ３２）のセキュリティエージェント６２がサイバー攻撃への対処を実行してもよい。このようにすること

で、サイバー攻撃を受けて一時的に処理負荷が増大し、計算資源に余裕がなくなってしまった場合であっても、確実にサイバー攻撃への対処を実行することが可能となる。

[0076] ＜変形例２＞

第１実施形態では、サイバー攻撃を受けた地点から一番近いＥＣＵ３２のセキュリティエージェント６２がサイバー攻撃への対処を実行した。しかしながら、対処の形態はこれに限定されない。例えば、自動運転や車両制御に関わるような重要な機能が実装されたＥＣＵ３２のセキュリティエージェント６２がサイバー攻撃への対処を実行してもよい。このようにすることで、サイバー攻撃を受けて他の機能が失陥したとしても、車両２を安全に停止させるための機能が優先的に守られ、サイバー攻撃による被害を最小化することが可能となる。

[0077] ＜変形例３＞

第１実施形態では、サイバー攻撃を受けた地点から一番近いＥＣＵ３２のセキュリティエージェント６２がサイバー攻撃への対処を実行したが、サイバー攻撃を検知したＥＣＵ３２のセキュリティエージェント６２がサイバー攻撃への対処を実行してもよい。最初にサイバー攻撃を検知したセキュリティエージェント６２は、他のＥＣＵ３２のセキュリティエージェント６２に対してもサイバー攻撃に関する情報を共有する。サイバー攻撃を受けたことを通知された他のＥＣＵ３２は、個別に、もしくは複数のＥＣＵ３２で連携してサイバー攻撃への対処を実行する。第１実施形態では、サイバー攻撃を受けた地点から一番近いＥＣＵ３２がサイバー攻撃により制御不能となった場合にサイバー攻撃への対処ができなくなるが、本変形例のようにすることで、対処可能なＥＣＵ３２がそれぞれサイバー攻撃への対処を実行するので、問題を解決できる可能性が高まる。また、複数のＥＣＵ３２でサイバー攻撃への対処を実行することで、サイバー攻撃に対してより多くのパターンで対処が可能となる。

[0078] ＜変形例４＞

セキュリティエージェント６２における検知部６４や対処部６６、センタ装置４における分析部７２などに、機械学習によるロジックを適用してもよい。このようにすることで、サイバー攻撃の検知やサイバー攻撃への対処の精度が向上し、より最適な対処を実行可能となる。また、車両２側だけでも学習による性能向上が見込めるため、通信コストやソフトウェア更新コストの低減が期待できる。

[0079] 以上、本発明の実施形態について説明したが、上記実施形態は本発明の適用例の一部を示したに過ぎず、本発明の技術的範囲を上記実施形態の具体的構成に限定する趣旨ではない。

符号の説明

[0080] １、１００、２００…車両制御システム、２…車両、３…車両制御装置、４…センタ装置、５…無線通信網、３０、３０ａ、４０…アンテナ、３２…ＥＣＵ、４１、５１…演算装置、４２、５２…不揮発性メモリ、４３、５３…揮発性メモリ、４４、５４…入出力インタフェース、６１、７１…通信部、６２…セキュリティエージェント、６３…アプリケーション、６４…検知部、６５…収集部、６６…対処部、７２…分析部

請求の範囲

[請求項1] 複数の制御装置を備えた、車両に搭載される車両制御システムであって、

前記複数の制御装置のうち少なくとも１つの制御装置は演算装置を備え、

前記演算装置は、

前記複数の制御装置に対するサイバー攻撃を検知し、

前記サイバー攻撃に対して、前記サイバー攻撃または前記サイバー攻撃に引き続く他のサイバー攻撃を防止するもしくはその影響を緩和する第１対処を実施し、

前記サイバー攻撃に関する攻撃情報を前記車両の外部に設けられたセンタ装置に送信し、

前記第１対処の実施後に、前記センタ装置から前記攻撃情報に対応する対処情報を受信し、

前記対処情報に基づき前記第１対処とは異なる第２対処を実施する、

車両制御システム。

[請求項2] 請求項１に記載の車両制御システムにおいて、

前記演算装置は、前記サイバー攻撃または前記サイバー攻撃に引き続く他のサイバー攻撃の防止、もしくはその影響の緩和に成功するまで、新たな前記攻撃情報の送信、前記第１対処の実施、および前記第２対処の実施を繰り返し行う車両制御システム。

[請求項3] 請求項１に記載の車両制御システムにおいて、

前記複数の制御装置はそれぞれ前記演算装置を備え、

前記複数の制御装置のうち、前記サイバー攻撃を受けた地点に最も近い前記制御装置の前記演算装置が前記第１対処および前記第２対処を実施する車両制御システム。

[請求項4] 請求項１に記載の車両制御システムにおいて、

前記第２対処は、前記複数の制御装置の各々を特定するための一意な識別子を変更する処理、前記サイバー攻撃を受けた前記制御装置の少なくとも一部の機能を他の前記制御装置に移動させる処理、および前記サイバー攻撃を受けた前記制御装置の少なくとも一部の機能と同等の機能を他の前記制御装置に実現させる処理のいずれかである車両制御システム。

[請求項5] 請求項４に記載の車両制御システムにおいて、

前記複数の制御装置のうち少なくとも１つの制御装置は、前記識別子または前記一部の機能を統合制御し、前記演算装置による前記第２対処の実施を管理する車両制御システム。

[請求項6] 請求項１に記載の車両制御システムにおいて、

複数の前記車両のうち少なくとも１つの車両に搭載された前記制御装置に対して前記サイバー攻撃が行われた場合、前記サイバー攻撃が行われていない他の前記制御装置においても前記第２対処を実施する車両制御システム。

[請求項7] 請求項１に記載の車両制御システムにおいて、

複数の前記車両にそれぞれ搭載された前記制御装置に対して前記サイバー攻撃が行われた場合、１つの前記制御装置に対して前記サイバー攻撃が行われた場合とは異なる前記第２対処を実施する車両制御システム。

[請求項8] 請求項１に記載の車両制御システムにおいて、

前記演算装置を有する前記制御装置は、前記複数の制御装置のうち、計算資源の多い前記制御装置、または他の制御装置よりも重要な機能を有する前記制御装置である車両制御システム。

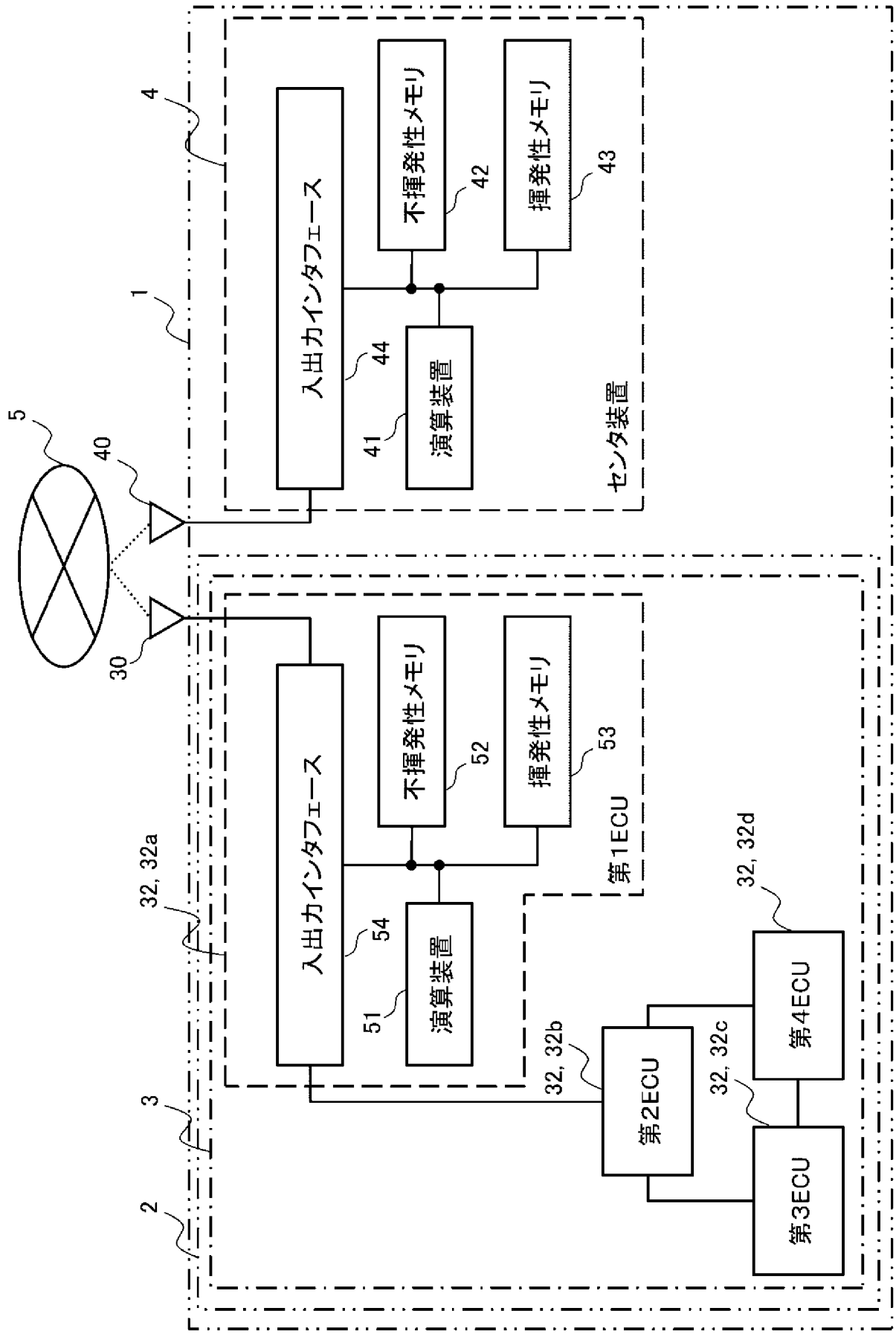
[請求項9] 請求項１に記載の車両制御システムにおいて、

前記１つの制御装置は、前記センタ装置との通信路を複数有する車両制御システム。

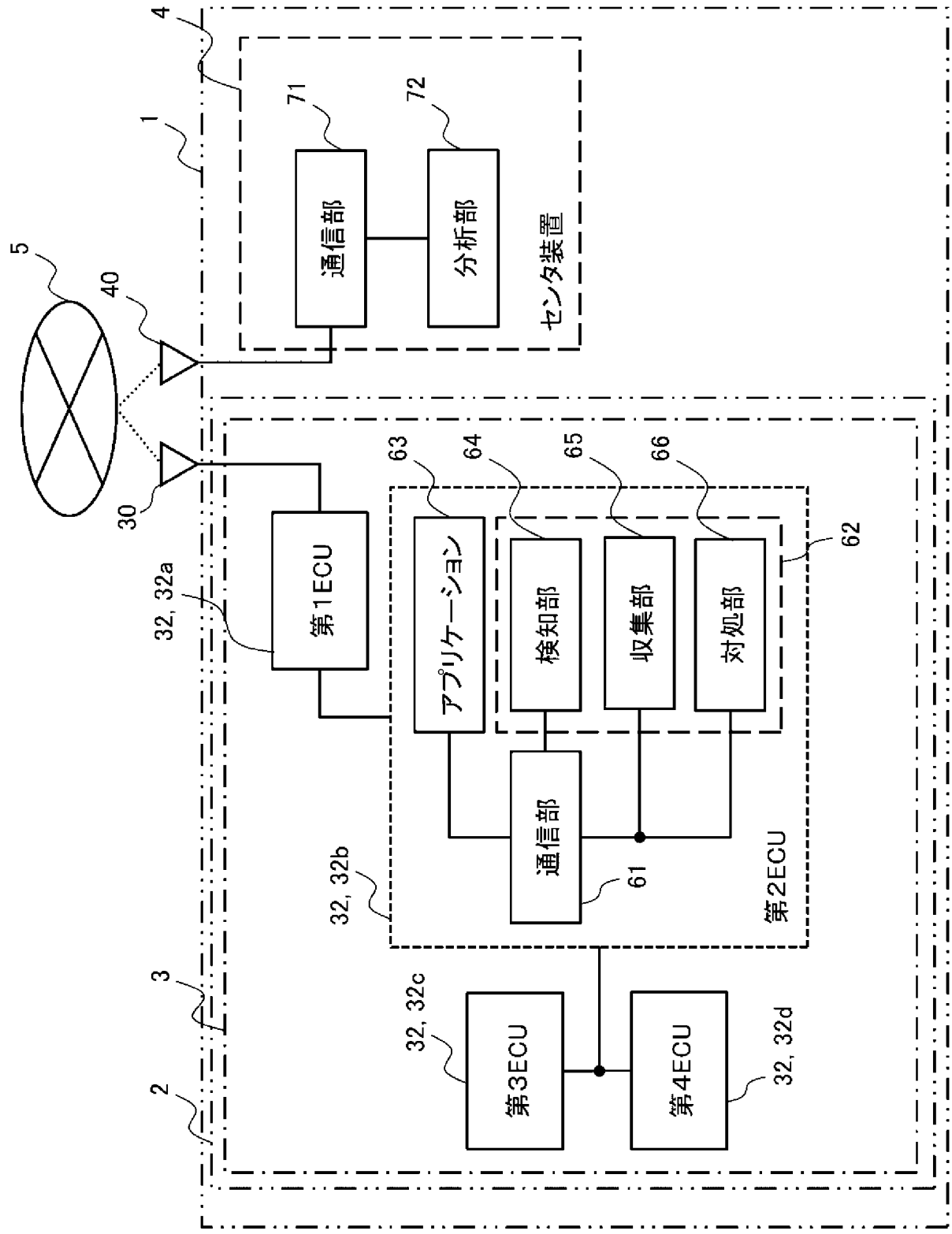
[請求項10] 請求項１に記載の車両制御システムにおいて、

前記第２対処は、前記センタ装置に前記車両を遠隔操縦させ前記車両を安全に停止させる処理である車両制御システム。

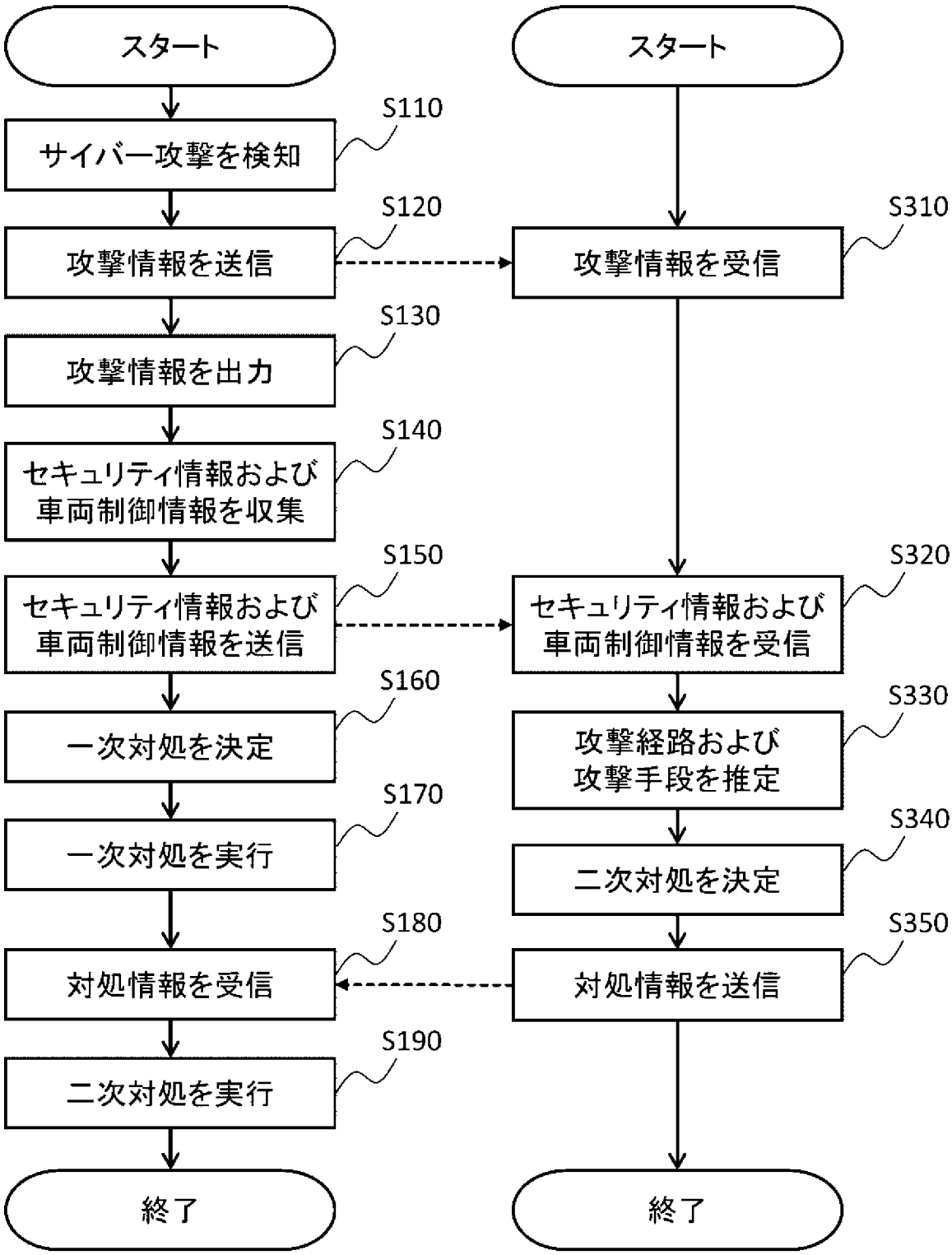
[図1]


センタ装置
入出力インタフェース
不揮発性メモリ
揮発性メモリ
演算装置
第1ECU
第2ECU
第3ECU
第4ECU
1
2
3
4
5
30
40
41
42
43
44
51
52
53
54
32, 32a
32, 32b
32, 32c
32, 32d

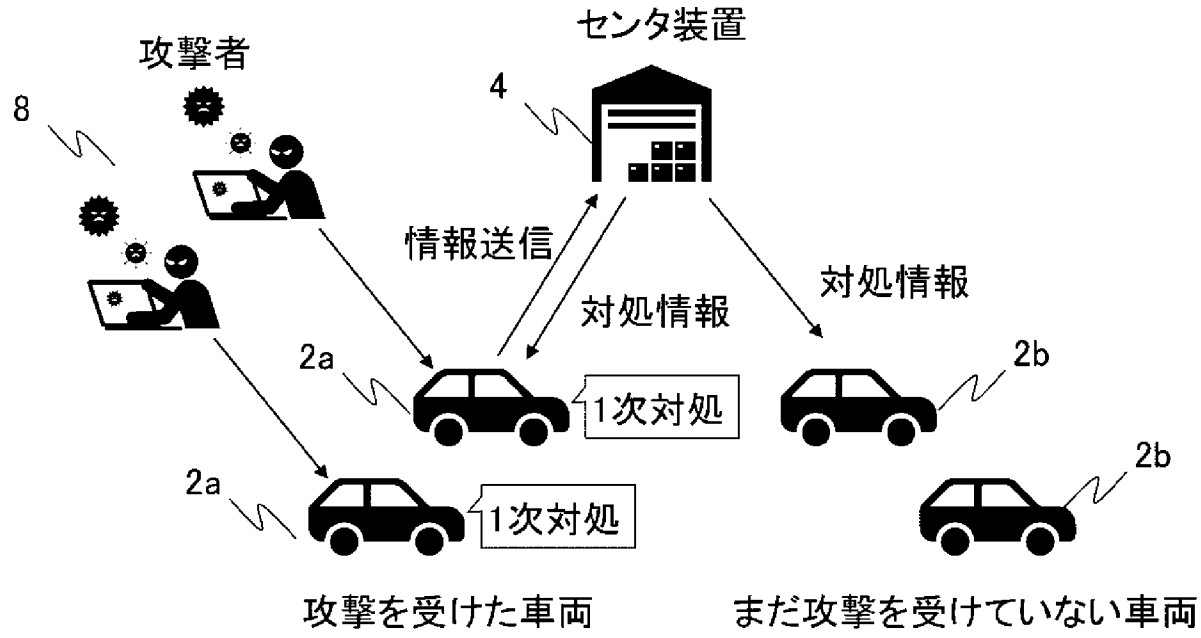
[図2]


4
1
71
72
通信部
分析部
センタ装置
5
40
30
63
64
65
66
62
32, 32a
第1ECU
アプリケーション
検知部
収集部
対処部
通信部
61
32, 32b
第2ECU
3
32, 32c
第3ECU
第4ECU
32, 32d
2

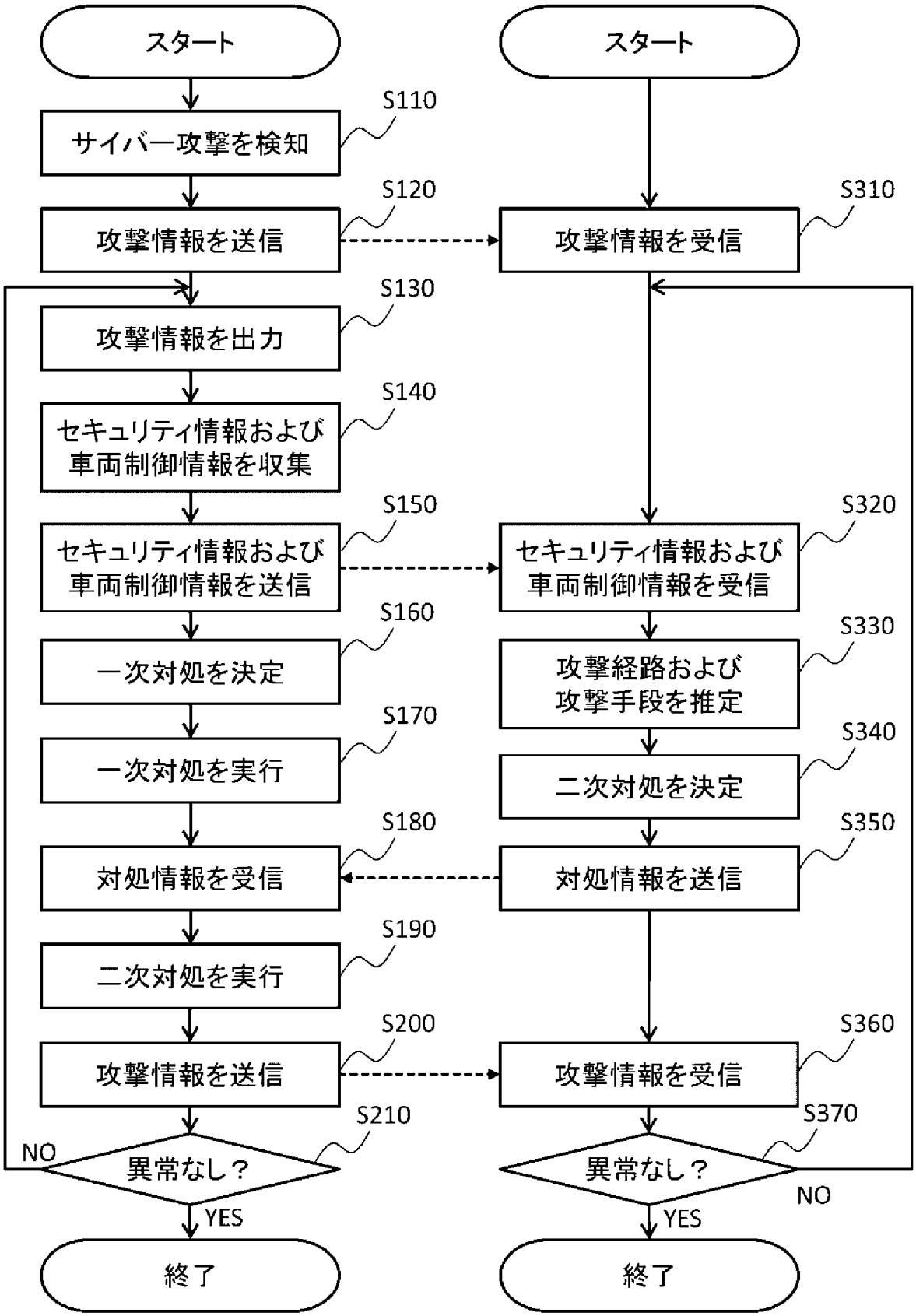
[図3]


スタート
サイバー攻撃を検知
S110
攻撃情報を送信
S120
攻撃情報を出力
S130
セキュリティ情報および
車両制御情報を収集
S140
セキュリティ情報および
車両制御情報を送信
S150
一次対処を決定
S160
一次対処を実行
S170
対処情報を受信
S180
二次対処を実行
S190
終了
スタート
攻撃情報を受信
S310
セキュリティ情報および
車両制御情報を受信
S320
攻撃経路および
攻撃手段を推定
S330
二次対処を決定
S340
対処情報を送信
S350
終了

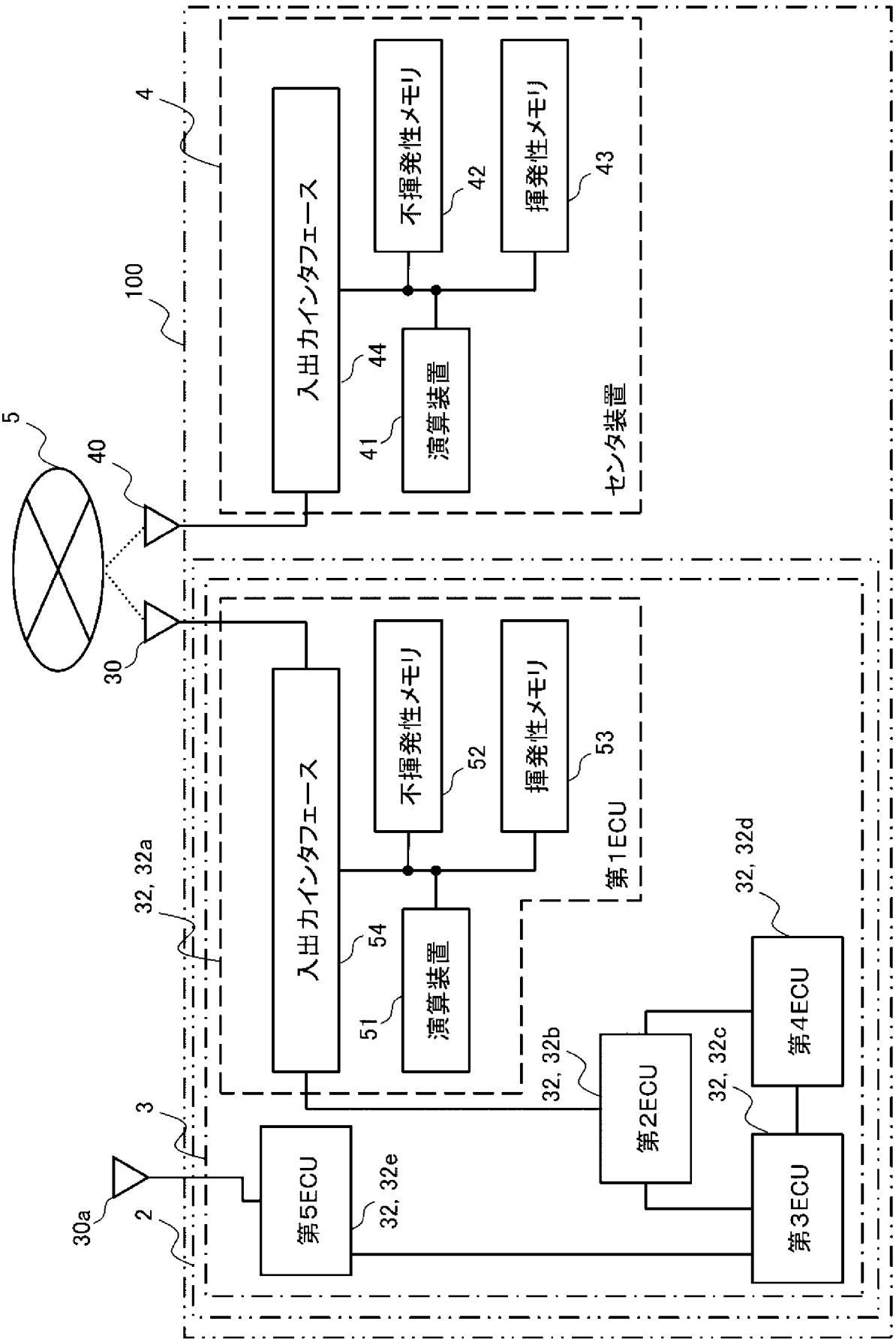
[図4]


センタ装置
攻撃者
8
4
情報送信
対処情報
対処情報
2a
1次対処
2b
2a
1次対処
2b
攻撃を受けた車両
まだ攻撃を受けていない車両

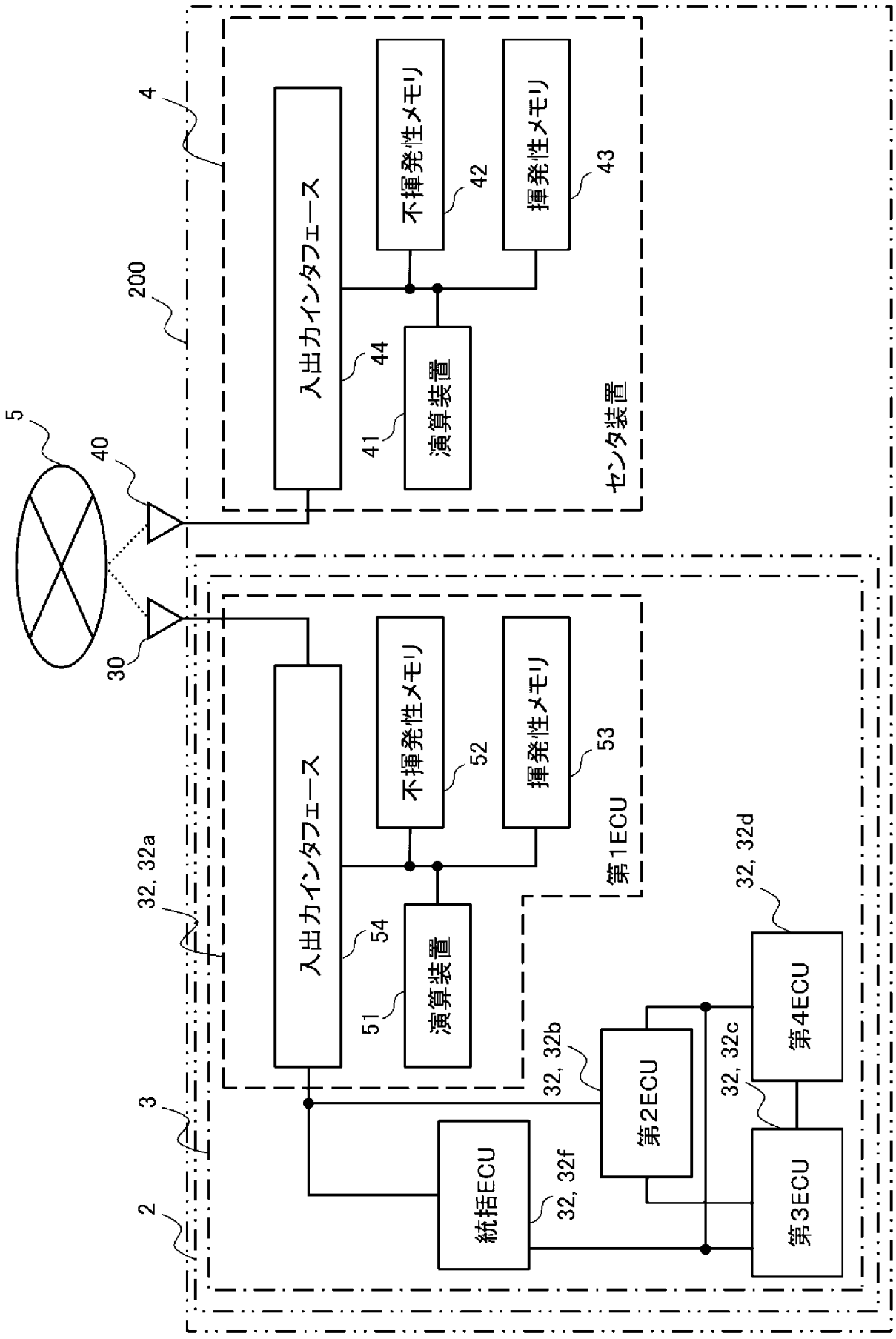
[図5]


スタート
サイバー攻撃を検知
S110
攻撃情報を送信
S120
攻撃情報を出力
S130
セキュリティ情報および
車両制御情報を収集
S140
セキュリティ情報および
車両制御情報を送信
S150
一次対処を決定
S160
一次対処を実行
S170
対処情報を受信
S180
二次対処を実行
S190
攻撃情報を送信
S200
異常なし？
S210
NO
YES
終了
スタート
攻撃情報を受信
S310
セキュリティ情報および
車両制御情報を受信
S320
攻撃経路および
攻撃手段を推定
S330
二次対処を決定
S340
対処情報を送信
S350
攻撃情報を受信
S360
異常なし？
S370
NO
YES
終了

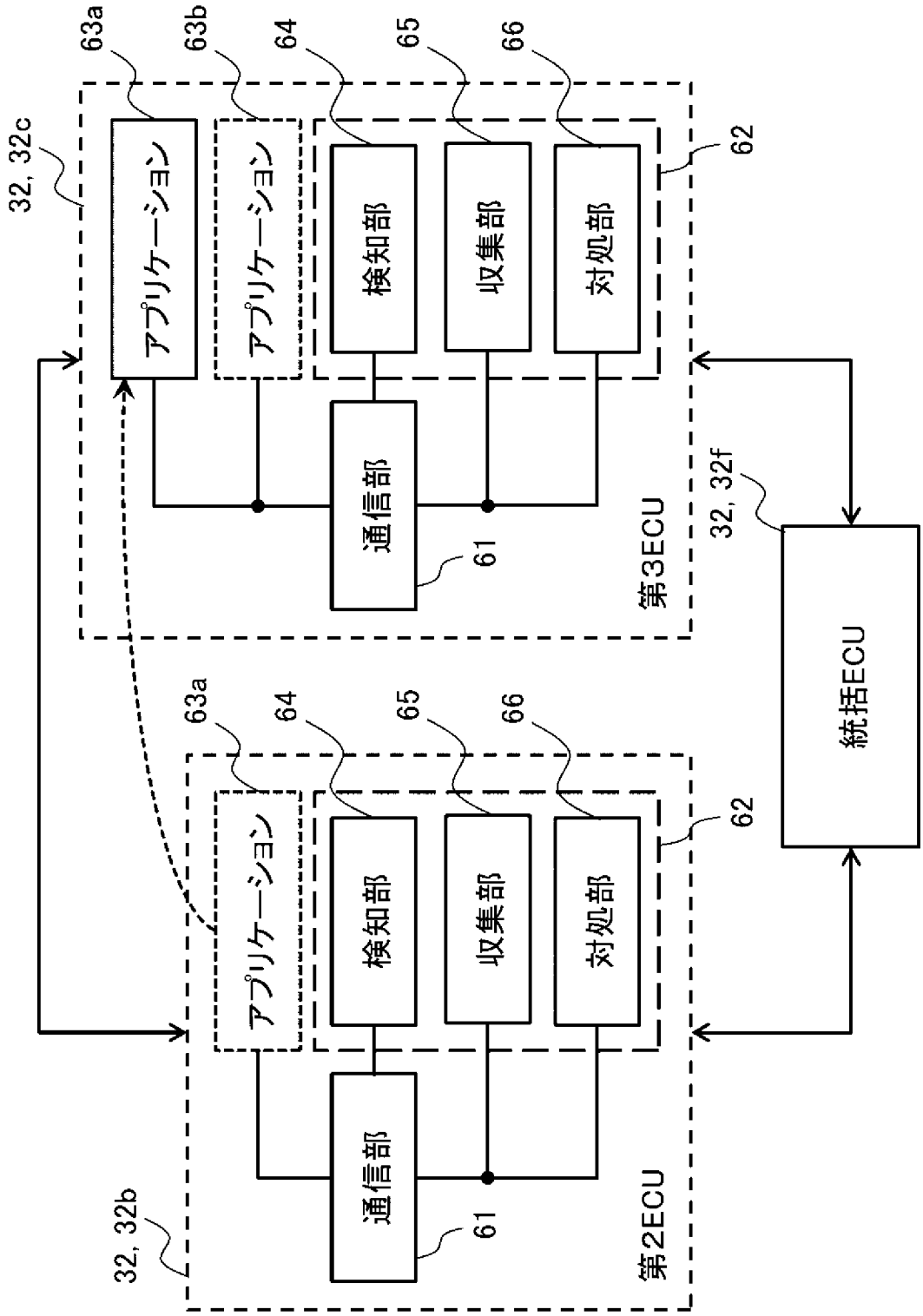
[図6]


センタ装置
入出力インタフェース
不揮発性メモリ
揮発性メモリ
演算装置
第1ECU
第2ECU
第3ECU
第4ECU
第5ECU
100
4
40
5
30
3
30a
2
41
42
43
44
51
52
53
54
32, 32a
32, 32b
32, 32c
32, 32d
32, 32e

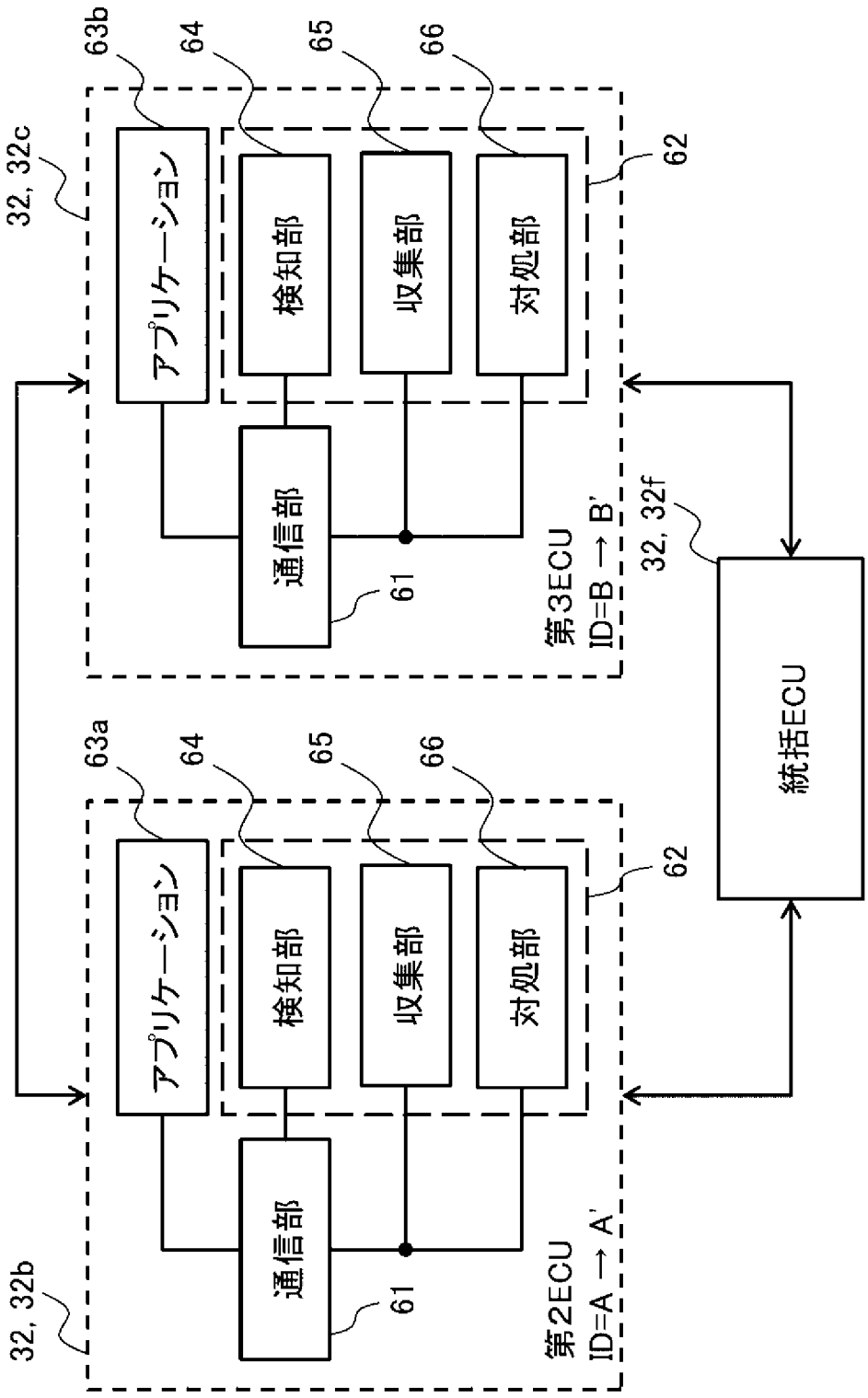
[図7]


4
200
入出力インタフェース
不揮発性メモリ
揮発性メモリ
42
43
44
41
演算装置
センタ装置
5
40
30
32, 32a
入出力インタフェース
不揮発性メモリ
揮発性メモリ
52
53
54
51
演算装置
第1ECU
32, 32d
第4ECU
32, 32b
第2ECU
32, 32c
第3ECU
3
2
統括ECU
32, 32f

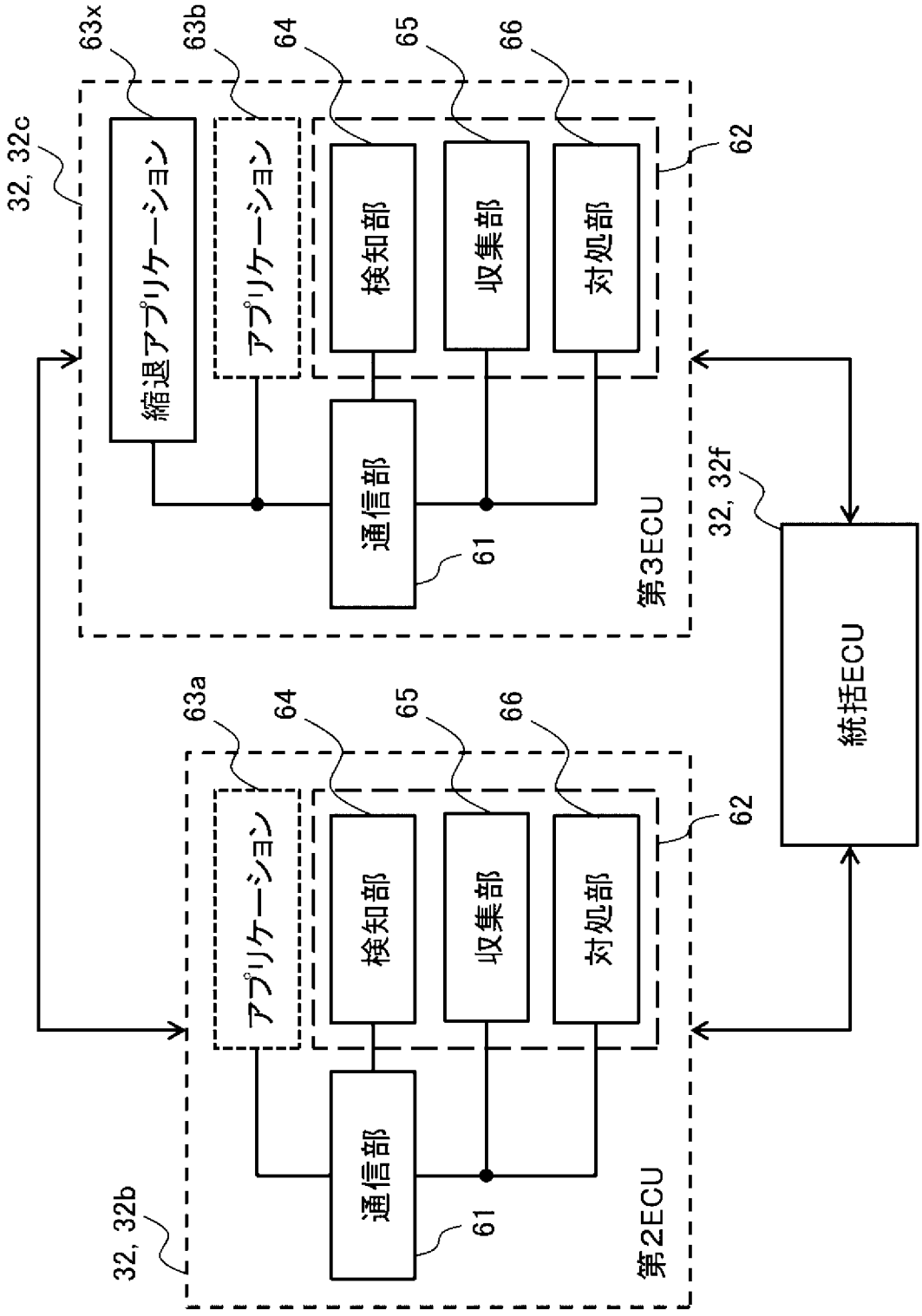
[図8]


63a
63b
64
65
66
32, 32c
アプリケーション
アプリケーション
検知部
収集部
対処部
62
通信部
61
第3ECU
32, 32f
統括ECU
63a
64
65
66
アプリケーション
検知部
収集部
対処部
62
通信部
61
32, 32b
第2ECU

[図9]


32, 32c
63b
64
65
66
62
アプリケーション
検知部
収集部
対処部
通信部
61
第3ECU
ID=B → B'
32, 32f
統括ECU
63a
64
65
66
62
アプリケーション
検知部
収集部
対処部
通信部
61
32, 32b
第2ECU
ID=A → A'

[図10]


63x
63b
64
65
66
32, 32c
縮退アプリケーション
アプリケーション
検知部
収集部
対処部
62
通信部
61
第3ECU
32, 32f
統括ECU
63a
64
65
66
アプリケーション
検知部
収集部
対処部
62
通信部
61
32, 32b
第2ECU

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2023/025835

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/55(2013.01)i
FI: G06F21/55

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)

G06F21/55

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 1971-2023
Registered utility model specifications of Japan 1996-2023
Published registered utility model applications of Japan 1994-2023

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	JP 2019-133599 A (CLARION CO. LTD.) 08 August 2019 (2019-08-08) paragraphs [0015], [0021]-[0023], [0050], [0070]-[0083], fig. 2, 7, 9	1-3, 8-9
Y	paragraphs [0015], [0021]-[0023], [0050], [0070]-[0083], fig. 2, 7, 9	4-7, 10
Y	JP 2018-166309 A (PANASONIC INTELLECTUAL PROPERTY MANAGEMENT CO., LTD.) 25 October 2018 (2018-10-25) paragraph [0013]	4-5
Y	JP 2021-60778 A (MITSUBISHI ELECTRIC CORPORATION) 15 April 2021 (2021-04-15) paragraph [0020]	4-5
Y	JP 2017-111796 A (PANASONIC IP CORP. AMERICA) 22 June 2017 (2017-06-22) paragraphs [0020], [0114]-[0116], fig. 2, 12	6-7
Y	JP 2019-46176 A (CLARION CO. LTD.) 22 March 2019 (2019-03-22) paragraphs [0091]-[0092]	10

☐ 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	Date of mailing of the international search report
07 August 2023	**22 August 2023**
Name and mailing address of the ISA/JP **Japan Patent Office (ISA/JP)** **3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915** **Japan**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2023/025835

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP 2019-133599 A	08 August 2019	US 2021/0044612 A1 paragraphs [0028], [0034]-[0036], [0063], [0083]-[0096], fig. 2, 7, 9 CN 111684446 A	
JP 2018-166309 A	25 October 2018	(Family: none)	
JP 2021-60778 A	15 April 2021	(Family: none)	
JP 2017-111796 A	22 June 2017	US 2018/0295147 A1 paragraphs [0042], [0136]-[0138], fig. 2, 12 CN 107925600 A	
JP 2019-46176 A	22 March 2019	US 2020/0361493 A1 paragraphs [0102]-[0103] CN 111094081 A	

国際調査報告

国際出願番号
PCT/JP2023/025835

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

G06F 21/55(2013.01)i
FI: G06F21/55

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））

G06F21/55

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	１９７１－２０２３年
日本国実用新案登録公報	１９９６－２０２３年
日本国登録実用新案公報	１９９４－２０２３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	JP 2019-133599 A (クラリオン株式会社) 08.08.2019 (2019-08-08) 段落[0015],[0021]-[0023],[0050],[0070]-[0083],図2,7,9	1-3,8-9
Y	段落[0015],[0021]-[0023],[0050],[0070]-[0083],図2,7,9	4-7,10
Y	JP 2018-166309 A (パナソニックＩＰマネジメント株式会社) 25.10.2018 (2018-10-25) 段落[0013]	4-5
Y	JP 2021-60778 A (三菱電機株式会社) 15.04.2021 (2021-04-15) 段落[0020]	4-5
Y	JP 2017-111796 A (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) 22.06.2017 (2017-06-22) 段落[0020],[0114]-[0116],図2,12	6-7
Y	JP 2019-46176 A (クラリオン株式会社) 22.03.2019 (2019-03-22) 段落[0091]-[0092]	10

☐ 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抵触するものではなく、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	国際調査報告の発送日
07.08.2023	22.08.2023

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
上島　拓也 5S 6293
電話番号 03-3581-1101 内線 3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2023/025835

引用文献	公表日	パテントファミリー文献	公表日
JP 2019-133599 A	08.08.2019	US 2021/0044612 A1 段落[0028],[0034]-[0036],[0063],[0083]-[0096],図2,7,9 CN 111684446 A	
JP 2018-166309 A	25.10.2018	（ファミリーなし）	
JP 2021-60778 A	15.04.2021	（ファミリーなし）	
JP 2017-111796 A	22.06.2017	US 2018/0295147 A1 段落[0042],[0136]-[0138],図2,12 CN 107925600 A	
JP 2019-46176 A	22.03.2019	US 2020/0361493 A1 段落[0102]-[0103] CN 111094081 A	