

(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
2024年8月15日(15.08.2024)



(10) 国際公開番号

WO 2024/166158 A1

(51) 国際特許分類:
G06F 21/55 (2013.01)

(21) 国際出願番号: PCT/JP2023/003740

(22) 国際出願日: 2023年2月6日(06.02.2023)

(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: 住友電気工業株式会社
(SUMITOMO ELECTRIC INDUSTRIES, LTD.)
[JP/JP]; 〒5410041 大阪府大阪市中央区北浜四丁目5番33号 Osaka (JP). 株式会社オートネットワーク技術研究所(AUTONETWORKS TECHNOLOGIES, LTD.) [JP/JP]; 〒5108503 三重県四日市市西末広町1番14号 Mie

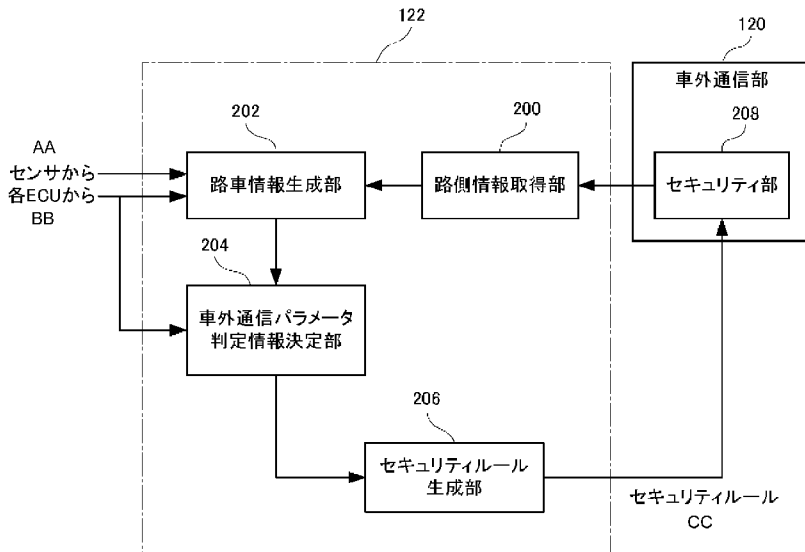
(JP). 住友電装株式会社(SUMITOMO WIRING SYSTEMS, LTD.) [JP/JP]; 〒5108503 三重県四日市市西末広町1番14号 Mie (JP).

(72) 発明者: 栗山 健太 (KURIYAMA, Kenta); 〒5410041 大阪府大阪市中央区北浜四丁目5番33号 住友電気工業株式会社内 Osaka (JP). 小川 明紘(OGAWA, Akihiro); 〒5410041 大阪府大阪市中央区北浜四丁目5番33号 住友電気工業株式会社内 Osaka (JP).

(74) 代理人: 清水 敏, 外 (SHIMIZU, Satoshi et al.); 〒5300002 大阪府大阪市北区曽根崎新地二丁目5番3号 堂島 T S S ビル 4 階 堂島特許事務所北新地支所内 Osaka (JP).

(54) Title: ON-BOARD DEVICE, SERVER COMPUTER, COMMUNICATION SYSTEM, CONTROL METHOD, AND COMPUTER PROGRAM

(54) 発明の名称: 車載装置、サーバコンピュータ、通信システム、制御方法およびコンピュータプログラム



120 External communication unit
200 Roadside information acquisition unit
202 Road/vehicle information generation unit
204 Exterior communication parameter determination information resolution unit
206 Security rule generation unit
208 Security unit
AA From sensor
BB From each ECU
CC Security rule

(57) Abstract: This on-board device is installed in a vehicle and causes a communication unit, which communicates with an external device located outside the vehicle, to restrict the communication with the external device in accordance with a security rule generated on the basis of road/vehicle information, including vehicle information about the vehicle and roadside information regarding outside of the vehicle, wherein the vehicle information includes application operation information for identifying an application operating in the vehicle and/or connection information indicating a communication connection state with the external device.

(57) 要約: 車載装置は、車両に搭載される車載装置であって、車両の車両情報および車両の外部に関する路側情報を含む路車情報に基づいて生成されたセキュリティルールに従って、車両の外部にある外部装置と通信する通信部に、外部装置との通信を制限させ、車両情報は、車両において稼働しているアプリケーションを特定するアプリケーション稼働情報および外部装置との通信接続状態を表す接続情報の少なくとも1つを含む。

[続葉有]

(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, 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, 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:

一 国際調査報告(条約第21条(3))

明 細 書

発明の名称：

車載装置、サーバコンピュータ、通信システム、制御方法およびコンピュータプログラム

技術分野

[0001] 本開示は、車載装置、サーバコンピュータ、通信システム、制御方法およびコンピュータプログラムに関する。

背景技術

[0002] 悪意のある第三者によるコンピュータシステムおよびネットワークへのサイバーセキュリティ攻撃には、セキュリティルール（例えば、通信アクセス許可リストおよび通信フィルタしきい値等）を適切に設定することにより対策可能であることが知られている。下記特許文献1には、DDoS（Distributed Denial of Service）攻撃に関連するトラフィックデータの特徴量を用いて機械学習によりセキュリティ設定パラメータの予測値を算出するセキュリティ設定支援装置が開示されている。セキュリティ設定支援装置は、予測値に基づくセキュリティ設定を事前に評価した結果に基づいてセキュリティ設定支援を行う。

先行技術文献

特許文献

[0003] 特許文献1：国際公開第2022/009274号

発明の概要

[0004] 本開示のある局面に係る車載装置は、車両に搭載される車載装置であって、車両の車両情報および車両の外部に関する路側情報を含む路車情報に基づいて生成されたセキュリティルールに従って、車両の外部にある外部装置と通信する通信部に、外部装置との通信を制限させ、車両情報は、車両において稼働しているアプリケーションを特定するアプリケーション稼働情報および外部装置との通信接続状態を表す接続情報の少なくともいずれか1つを含

む。

図面の簡単な説明

[0005] [図1]図 1 は、本開示の実施形態に係る通信システムの構成を示す模式図である。

[図2]図 2 は、図 1 に示した車載システムのハードウェア構成を示すブロック図である。

[図3]図 3 は、図 1 に示した路側機のハードウェア構成を示すブロック図である。

[図4]図 4 は、図 1 に示したサーバ（即ちサーバコンピュータ）のハードウェア構成を示すブロック図である。

[図5]図 5 は、図 2 に示した車載システムの機能構成を示すブロック図である。

[図6]図 6 は、車載システムの動作のうち、セキュリティルールの決定に関する動作を示すフローチャートである。

[図7]図 7 は、車載システムの動作のうち、通信に関する動作を示すフローチャートである。

[図8]図 8 は、車両におけるアプリケーション稼働状況の変化に伴うセキュリティルールの変化を示す第 1 例を示す図である。

[図9]図 9 は、車両の位置を示す図である。

[図10]図 10 は、車両におけるアプリケーション稼働状況の変化に伴うセキュリティルールの変化を示す第 2 例を示す図である。

[図11]図 11 は、車両における通信接続状況の変化に伴うセキュリティルールの変化を示す第 3 例を示す図である。

[図12]図 12 は、車両におけるアプリケーション稼働状況および通信接続状況の変化に伴うセキュリティルールの変化を示す第 4 例を示す図である。

[図13]図 13 は、変形例に係る車載システムの機能構成を示すブロック図である。

[図14]図 14 は、アプリケーションの仕様からセキュリティルールテーブル

が生成される例を示す図である。

発明を実施するための形態

[0006] [本開示が解決しようとする課題]

車載ネットワークにおいては、車両において稼働しているアプリケーションプログラム（例えばユーザ向けのアプリケーションプログラムであり、以下、単にアプリケーションという）の切替えが行われる。また、車外装置（例えばサーバコンピュータ等）との接続状態等に応じて車外通信パラメータ（例えば、通信先IPアドレス、ポート番号等のネットワーク情報、通信量等）が変動する。したがって、サイバーセキュリティ攻撃への対策を行うには、車載装置の限られたリソースを用いてセキュリティルールを動的に制御する必要がある。しかし、特許文献1に開示された方法は、特徴量の機械学習における計算コストが高く（即ち、演算処理による負荷が大きく）、多くのリソースが必要である。また、機械学習結果を利用する際にも多くのリソースが必要である。そのため、リソースが限られている車載装置において、特許文献1に開示された方法を適用することは困難である。

[0007] したがって、本開示は、低い計算コストによりセキュリティルールを決定でき、搭載されている車両におけるアプリケーションの稼働状況および車外装置との接続状態の少なくともいずれか1つに応じてセキュリティルールを動的に制御できる車載装置、サーバコンピュータ、通信システム、制御方法およびコンピュータプログラムを提供することを目的とする。

[0008] [発明の効果]

本開示によれば、低い計算コストによりセキュリティルールを決定でき、搭載されている車両におけるアプリケーションの稼働状況および車外装置との接続状態の少なくともいずれか1つに応じてセキュリティルールを動的に制御できる車載装置、サーバコンピュータ、通信システム、制御方法およびコンピュータプログラムを提供できる。

[0009] [本開示の実施形態の説明]

本開示の実施形態の内容を列記して説明する。以下に記載する実施形態の

少なくとも一部を任意に組合せてもよい。

- [0010] (1) 本開示の第1の局面に係る車載装置は、車両に搭載される車載装置であって、車両の車両情報および車両の外部に関する路側情報を含む路車情報に基づいて生成されたセキュリティルールに従って、車両の外部にある外部装置と通信する通信部に、外部装置との通信を制限させ、車両情報は、車両において稼働しているアプリケーションを特定するアプリケーション稼働情報および外部装置との通信接続状態を表す接続情報の少なくともいずれか1つを含む。これにより、低い計算コストによりセキュリティルールを決定でき、車載装置が搭載されている車両におけるアプリケーションの稼働状況および外部装置との接続状態に応じてセキュリティルールを動的に制御できる。
- [0011] (2) 上記(1)において、車載装置は、セキュリティルールを外部装置から受信できる。これにより、車載装置におけるセキュリティルールを決定するための演算処理による負荷を削減できる。
- [0012] (3) 上記(1)において、車載装置は、外部装置から、路側情報を取得する路側情報取得部と、路側情報に車両情報を加えて路車情報を生成する路車情報生成部と、路車情報に基づいて車外通信パラメータ判定情報を決定する決定部と、車外通信パラメータ判定情報に基づいてセキュリティルールを生成するセキュリティルール生成部とをさらに含んでもよい。これにより、車両におけるアプリケーションの稼働状況および外部装置との接続状態に応じて適切なセキュリティルールを決定できる。
- [0013] (4) 上記(3)において、路車情報は、アプリケーション稼働情報および接続情報の少なくともいずれか1つに加えて、位置情報および地図情報の少なくとも1つを含んでもよい。これにより、適切なセキュリティルールを生成するための車外通信パラメータを決定できる。
- [0014] (5) 上記(3)または(4)において、車外通信パラメータ判定情報は、アプリケーション稼働情報および接続情報の少なくとも1つを含んでもよい。これにより、適切なセキュリティルールを生成できる。

[0015] (6) 上記(5)において、車外通信パラメータ判定情報は、少なくともアプリケーション稼働情報を含んでいてもよく、セキュリティルール生成部は、アプリケーション稼働情報により稼働しているアプリケーションがないことを特定した場合、第1通信フィルタしきい値を含むセキュリティルールを生成し、アプリケーション稼働情報により車両のドア開閉を制御するアプリケーションを特定した場合、第1通信フィルタしきい値よりも大きい第2通信フィルタしきい値を含むセキュリティルールを生成してもよい。これにより、車両の駐車時且つ認証前(即ち、稼働アプリケーションがない)において、想定される通信量(即ち第1通信フィルタしきい値)を超えるデータが車載システムに対して送信された場合、送信データをフィルタ可能になる。したがって、例えばDoS(Denial of Service)攻撃に対策可能になる。

[0016] (7) 上記(5)または(6)において、車外通信パラメータ判定情報は、少なくともアプリケーション稼働情報を含んでいてもよく、セキュリティルール生成部は、アプリケーション稼働情報により稼働しているアプリケーションがないことを特定した場合、アクセス許可を含まないセキュリティルールを生成し、アプリケーション稼働情報により運転支援アプリケーションが稼働していることを特定した場合、運転支援アプリケーションにサービスを提供する外部装置へのアクセス許可を含むセキュリティルールを生成してもよい。これにより、車両が、運転支援サービス対象外のエリアに位置する場合に(即ち、稼働アプリケーションがない場合に)、車載システムに想定しない通信先からのアクセスがあった際に、そのアクセスを制限できる。例えば、通信先を偽ったアクセス(即ち、なりすまし)への対策が可能になる。

[0017] (8) 上記(5)から(7)のいずれか1つにおいて、車外通信パラメータ判定情報は、少なくとも接続情報を含んでいてもよく、セキュリティルール生成部は、路車情報から特定される車両の位置が、複数の交差点を含む第1領域内にある場合に、第1領域に対応する接続情報により特定される第3

通信フィルタしきい値を含むセキュリティルールを生成し、路車情報から特定される車両の位置が、第1領域よりも狭く、1つの交差点を含む第2領域内にある場合に、第2領域に対応する接続情報により特定される第4通信フィルタしきい値を含むセキュリティルールを生成してもよく、第4通信フィルタしきい値は、第3通信フィルタしきい値よりも大きくてもよい。これにより、車両が、第1領域（例えばクラウド通信エリア）内に位置する場合に、接続状態から想定される通信量（即ち第3通信フィルタしきい値）を超えるデータが車載システムに対して送信された場合、送信データをフィルタ可能になる。したがって、例えばD o S攻撃に対策可能になる。

[0018] (9) 上記(5)において、車外通信パラメータ判定情報は、アプリケーション稼働情報を含んでもよく、セキュリティルール生成部は、車外通信パラメータ判定情報により、車両において複数のアプリケーションが稼働していることを特定した場合、稼働している複数のアプリケーションの各々に関するセキュリティルールテーブルを生成し、複数のセキュリティルールテーブルを統合してセキュリティルールを生成してもよい。これにより、1つの通信部の通信を制限するセキュリティルールを効率よく生成できる。

[0019] (10) 上記(4)から(9)のいずれか1つにおいて、決定部は、路車情報が接続情報を含んでいなければ、当該路車情報から、車外通信パラメータ判定情報として接続情報を生成してもよい。これにより、路車情報から稼働情報、接続情報を生成でき、適切なセキュリティルールを生成できる。

[0020] (11) 上記(1)から(10)のいずれか1つにおいて、セキュリティルールは、通信部による通信に関するアクセス頻度、通信速度、セッション数、SYNパケット数、通信先の通信アドレス、および、通信先のポート番号の少なくとも1つに関する制限を含んでもよい。これにより、通信部による通信の安全性を向上できる。

[0021] (12) 上記(1)から(11)のいずれか1つにおいて、車載装置は、セキュリティルールを更新する更新部をさらに含んでもよく、更新部は、通信部により、車両において稼働させる新たなアプリケーション、または

、車両において稼働しているアプリケーションの更新アプリケーションが受信されたことを受けて、セキュリティルールを更新してもよい。これにより、セキュリティルールを適切な状態に維持できる。

[0022] (13) 上記(12)において、新たなアプリケーションまたは更新アプリケーションに対応する新たなセキュリティルールは、外部装置から受信されてもよく、更新部は、新たなセキュリティルールを用いて、セキュリティルールを更新してもよい。これにより、アプリケーションの稼働状況に応じてセキュリティルールを決定するための演算処理による負荷をより軽減できる。

[0023] (14) 本開示の第2の局面に係るサーバコンピュータは、車両に搭載される車載装置に、車載装置による車両の外部との通信を制限するセキュリティルールを、車両の車両情報および車両の外部に関する路側情報を含む路車情報に基づいて生成する生成部と、車載装置に、セキュリティルールを送信する通信部とを含み、車両情報は、車両において稼働しているアプリケーションを特定するアプリケーション稼働情報および外部装置との通信接続状態を表す接続情報の少なくともいずれか1つを含む。これにより、車載システムは、車両におけるアプリケーションの稼働状況および外部装置との接続状態に応じたセキュリティルールに従って、車外との通信を動的に制御できる。

[0024] (15) 上記(14)において、通信部は、車載装置から、車両情報を受信することができ、サーバコンピュータは、路側情報に、通信部により受信された車両情報を加えて路車情報を生成する路車情報生成部と、路車情報に基づいて車外通信パラメータ判定情報を決定する決定部とさらに含むことができ、生成部は、車外通信パラメータ判定情報に基づいてセキュリティルールを生成することができる。これにより、車載装置においてセキュリティルールを決定するための演算処理による負荷を削減できる。

[0025] (16) 本開示の第3の局面に係る通信システムは、上記(1)から(13)のいずれか1つに記載の車載装置と、上記(14)に記載のサーバコン

ピュータとを含み、車載装置は、車両に搭載された通信部に、サーバコンピュータを外部装置として通信させる。これにより、車載装置は、車両におけるアプリケーションの稼働状況および外部装置との接続状態に応じてセキュリティルールを動的に制御できる。

[0026] (17) 本開示の第4の局面に係る通信システムは、上記(1)または(2)に記載の車載装置と、上記(15)に記載のサーバコンピュータとを含み、車載装置は、車両に搭載された通信部に、サーバコンピュータを外部装置として通信させる。これにより、車載装置は、車両におけるアプリケーションの稼働状況および外部装置との接続状態に応じてセキュリティルールを動的に制御できる。

[0027] (18) 本開示の第5の局面に係る制御方法は、車両に搭載される車載システムの制御方法であって、車載システムに含まれる車載装置が、車両の車両情報および車両の外部に関する路側情報を含む路車情報に基づいて生成されたセキュリティルールに従って、車両の外部にある外部装置と通信する通信部に、外部装置との通信を制限させるステップを含み、車両情報は、車両において稼働しているアプリケーションを特定するアプリケーション稼働情報および外部装置との通信接続状態を表す接続情報の少なくともいずれか1つを含む。これにより、車載装置は、車両におけるアプリケーションの稼働状況および外部装置との接続状態に応じてセキュリティルールを動的に制御できる。

[0028] (19) 本開示の第6の局面に係るコンピュータプログラムは、車両に搭載されるコンピュータに、車両の車両情報および車両の外部に関する路側情報を含む路車情報に基づいて生成されたセキュリティルールに従って、車両の外部にある外部装置と通信する通信部に、外部装置との通信を制限させる機能を実現させ、車両情報は、車両において稼働しているアプリケーションを特定するアプリケーション稼働情報および外部装置との通信接続状態を表す接続情報の少なくともいずれか1つを含む。これにより、車載装置は、車両におけるアプリケーションの稼働状況および外部装置との接続状態に応じ

てセキュリティルールを動的に制御できる。

[0029] [本開示の実施形態の詳細]

以下の実施形態においては、同一の部品には同一の参照番号を付してある。それらの名称および機能も同一である。したがって、それらについての詳細な説明は繰返さない。

[0030] [全体構成]

図1を参照して、本開示の実施形態に係る通信システム100は、車載システム102が搭載された車両104と、基地局108およびネットワーク110を介して車載システム102と通信可能なサーバ（即ちサーバコンピュータ）112とを含む。通信システム100は、路側に固定して設置された、センサを含む路側機106を含んでいてもよい。サーバ112は、車載システム102に運転支援情報を送信する等のサービスを提供する。車載システム102および路側機106は、サーバ112により送信される運転支援情報の生成に利用されるデータをサーバ112に送信する（以下、アップロードともいう）。

[0031] 基地局108は、例えば、4G（即ち第4世代移動通信システム）回線および5G（即ち第5世代移動通信システム）回線等による移動通信サービスを提供している。基地局108はネットワーク110に接続されている。車両104に搭載されている車載システム102は、基地局108がサービスしている通信仕様（即ち4G回線、5G回線等）による通信機能を有している。路側機106も、基地局108を介してネットワーク110に接続されている。なお、サーバ112と車載システム102および路側機106との通信は、ネットワーク110を介した通信に限定されず、Wi-Fi等の無線通信であってもよい。また、サーバ112と固定設置される路側機106との通信は、基地局108を介さない有線による通信であってもよい。

[0032] 車両104が搭載しているセンサ（以下、車載センサともいう）により取得されたセンサデータは、車載システム102において解析され、解析結果は動的情報として記憶される。動的情報は、自車両の自動運転機能において

使用される。また、センサデータおよび動的情報は、車載システム 102 からサーバ 112 にアップロードされる。

[0033] 路側機 106 は路側に設置され、センサ（以下、インフラセンサともいう）により路側における情報を取得する。センサデータは、路側機 106 において解析され、動的物体等が検出される。センサデータおよび解析結果は、路側機 106 からサーバ 112 にアップロードされる。図 1 に示した車両 104 は、路側機 106 が有するインフラセンサの検出対象であり、動的物体として検出される。

[0034] 動的情報は、センサ（即ち、インフラセンサおよび車載センサ）により検出された動的物体に関する情報である。動的物体は、移動している物体（例えば、人および車両等）に限らず、移動機能を有しているが停止している物体をも含む。動的情報は、自車両の自動運転に用いるための運転支援情報として使用される。また、動的情報はサーバ 112 に送信されて、サーバ 112 から車両（車両 104 および車両 104 以外の車両を含む）に送信される運転支援情報の生成に利用される。

[0035] 図 1 には、1つの基地局 108、1つの路側機 106、車載システム 102 が搭載された1つの車両 104 を示している。しかしこれは例示に過ぎない。通常、複数の基地局が設けられ、車載システムが搭載されている複数台の車両が存在する。サーバ 112 と通信可能な車載システムを搭載していない車両が存在してもよい。車載システムを搭載していない車両は、動的物体として検出される。

[0036] [車載システムのハードウェア構成]

図 2 を参照して、車両 104 に搭載されている車載システム 102 のハードウェア構成の一例を示す。車載システム 102 は、車外通信部 120、車載装置 122、センサ 124、自動運転 ECU (Electronic Control Unit) 126、認証 ECU 128、駆動 ECU 130 およびバス 132 を含む。なお、車載システム 102 は、複数の ECU を含み、図 2 には一例として自動運転 ECU 126、認証 ECU 128 および駆動

ECU130を示している。

[0037] 車外通信部120は、車両104の外部装置と無線通信（例えば、基地局108を介したサーバ112等との通信）を行う。車外通信部120は、無線通信において採用されている変調および多重化を行うためのIC（Integrated Circuit）、所定周波数の電波を送信および受信するためのアンテナ、並びにRF（Radio Frequency）回路等を含む。車外通信部120は、車両104の現在位置を特定するための情報を取得するために、GPS（Global Positioning System）等のGNSS（Global Navigation Satellite System、全地球衛星測位システム）との通信機能をも有する。車外通信部120は、Wi-Fi等の通信機能も有していてもよい。

[0038] 車載装置122は、制御部140およびメモリ142を含む。制御部140は、CPU（Central Processing Unit）を含んで構成されており、メモリ142を制御する。メモリ142は、例えば、書換可能な不揮発性の半導体メモリであり、制御部140が実行するコンピュータプログラム（以下、単にプログラムという）を記憶している。メモリ142は、制御部140が実行するプログラムのワーク領域を提供する。制御部140は処理対象のデータを、車外通信部120からは直接取得し、車外通信部120以外からはバス132を介して取得する。制御部140は、車外通信部120から受信したデータおよびバス132を介して受信したデータを適宜メモリ142に記憶する。制御部140は、処理結果をメモリ142に記憶し、バス132に出力する。

[0039] 車載装置122は、車外との通信機能（具体的には通信仕様）と車内における通信機能（即ち通信仕様）とを接合するゲートウェイとしての役割（即ち通信プロトコル変換等）を担う。自動運転ECU126および認証ECU128等は、車載装置122および車外通信部120を介して、外部装置と通信できる。車載装置122は、後述するように、車外との通信に関するセキュリティルールの制御を実行する。また、車載装置122は、例えば、車

外通信部120を介して外部から受信する情報のうち、運転支援情報を、自動運転ECU126に伝送する。バス132は、車載システム内における通信機能を担う。車載装置122、センサ124、自動運転ECU126、認証ECU128および駆動ECU130に関して、相互間の通信（即ちデータ交換）は、バス132を介して行われる。バス132には、例えば、CAN（Controller Area Network）が使用される。

[0040] センサ124は、車両104に搭載され、車両104外部の情報を取得するためのセンサ（例えばビデオ映像の撮像装置（例えば、デジタルカメラ（CCD（Charge-Coupled Device）カメラ、CMOS（Complementary Metal-Oxide Semiconductor）カメラ））、レーザセンサ（LiDAR）等）を含む。なお、センサ124は、車両自体の情報を取得するためのセンサ（加速度センサ、荷重センサ等）を含んでいてもよい。センサ124は、検知範囲（カメラの場合であれば撮像範囲）内の情報を取得してセンサデータとして出力する。センサ124が、デジタルカメラであれば、デジタルの画像データを出力する。センサ124の検出信号（即ちアナログまたはデジタル信号）は、I/F部（図示せず）を介して、デジタルデータとしてバス132に出力され、車載装置122および自動運転ECU126等に送信される。

[0041] 自動運転ECU126は、車両104の走行を制御する。例えば、自動運転ECU126は、センサ124からセンサデータを取得し、それを解析して車両周囲の状況を把握し、自動運転に関連する機構である駆動ECU130に伝送する。駆動ECU130は駆動部134（例えば、エンジン、モータ、変速機、ステアリングおよびブレーキ等の機構）を制御する。自動運転ECU126は、車載装置122から取得した運転支援情報を自動運転に利用する。認証ECU128は、後述するように、車両104のドアロックの開錠等を許可するためにユーザ認証を実行する。

[0042] [路側機のハードウェア構成]

図3を参照して、路側機106のハードウェア構成の一例を示す。路側機

１０６は、通信部１５０、制御部１５２、センサ１５４、メモリ１５６およびバス１５８を含む。制御部１５２、センサ１５４およびメモリ１５６の間のデータ交換はバス１５８を介して行われる。通信部１５０は、サーバ１１２からデータを受信し、サーバ１１２に対してデータを送信する。通信部１５０は、送信データを制御部１５２から取得し、受信データを制御部１５２に出力する。通信部１５０による受信データは、適宜メモリ１５６に記憶される。

[0043] 制御部１５２は、例えばＣＰＵを含んで構成されている。メモリ１５６は、例えば、書換可能な不揮発性の半導体メモリであり、制御部１５２が実行するプログラムを記憶している。メモリ１５６は、制御部１５２が実行するプログラムのワーク領域を提供する。メモリ１５６は、ハードディスクドライブ等の大容量記憶装置を含んでいてもよい。センサ１５４は、路側機１０６外部の情報を取得するためのセンサであり、例えば、イメージセンサ（例えばデジタルの監視カメラ等）、レーダ（例えばミリ波レーダ等）、またはレーザセンサ（例えばＬｉＤＡＲ等）等を含む。センサ１５４は、検知範囲（例えば、カメラの場合であれば撮像範囲）内の情報を取得してセンサデータとして出力する。センサデータは、メモリ１５６に記憶される。

[0044] 制御部１５２は、メモリ１５６からセンサデータを読み出し、通信部１５０に出力する。これにより、センサ１５４のセンサデータは、通信部１５０からサーバ１１２に送信される。また、制御部１５２は、メモリ１５６からセンサデータを読み出して解析する。解析結果として、動的物体等が検出される。制御部１５２は、検出された動的物体等の情報を通信部１５０に出力する。これにより、制御部１５２の解析結果は、通信部１５０からサーバ１１２に送信され、サーバ１１２は、後述するように、車両１０４の外部に関する情報（以下、路側情報という）を生成できる。

[0045] [サーバのハードウェア構成]

図４を参照して、サーバ１１２は、各部を制御する制御部１６０と、データを記憶するメモリ１６２と、通信を行う通信部１６４と、各部の間におい

てデータを交換するためのバス１６６とを含む。制御部１６０は、ＣＰＵを含んで構成されており、各部を制御することにより、後述する機能を実現する。メモリ１６２は、書換可能な半導体の不揮発性メモリおよびハードディスクドライブ等の大容量記憶装置を含む。通信部１６４は、車載システム１０２および路側機１０６からアップロードされるデータを受信する。通信部１６４により受信されたデータは、メモリ１６２に伝送されて記憶される。サーバ１１２は、受信したデータを解析して路側情報を生成し、車載システム１０２に送信する。サーバ１１２が運転支援サービスを提供している場合、受信したデータを解析して運転支援情報を生成し、車両（即ち車載システム）に送信する。

[0046] [車載システムの機能的構成]

図５を参照して、車載装置１２２の機能、即ちセキュリティルールを制御する機能に関して説明する。車載装置１２２は、路側情報取得部２００、路車情報生成部２０２、車外通信パラメータ判定情報決定部２０４およびセキュリティルール生成部２０６を含む。路側情報取得部２００、路車情報生成部２０２、車外通信パラメータ判定情報決定部２０４およびセキュリティルール生成部２０６の各機能は、図２に示した制御部１４０およびメモリ１４２により実現される。車外通信部１２０は、パケットフィルタ等の通信のセキュリティを実行するセキュリティ部２０８を含む。車載装置１２２は、後述するように、決定されたセキュリティルールをセキュリティ部２０８に出力し、セキュリティ部２０８に、入力されたルールに従って車外通信部１２０により実行される通信を制限させる。

[0047] 路側情報取得部２００は、車外通信部１２０によりサーバ１１２から送信される路側情報を取得する。路側情報は、車載システム１０２の外部に関する情報であり、地図情報を含む。地図情報は、例えば、車載システム１０２の周囲の道路地図、および、車載システム１０２と通信可能なサーバ等の車外装置の配置情報（以下、車外装置マップという）を含む。車外装置マップに基づき、各サーバ等の通信領域が明らかとなり、車外装置と車両の通信接

続状態を導出できる。車外装置マップは、後述する接続情報（即ち、外部装置との通信接続状態を表す情報）を直接取得できない場合に利用される。取得された路側情報は、メモリ 142 に記憶される。

[0048] 路車情報生成部 202 は、車外通信部 120、自動運転 ECU 126 および駆動 ECU 130 等から取得した情報（以下、車両情報という）に、路側情報取得部 200 により取得された路側情報を加えて、路車情報を生成する。生成された路車情報は、メモリ 142 に記憶される。車両情報は、例えば、車両 104 の位置を表す位置情報、車両 104 において稼働しているユーザ向けのアプリケーションを特定するアプリケーション稼働情報、および、外部装置との通信接続状態を表す接続情報とを含む。したがって、路車情報は、例えば、位置情報、地図情報、アプリケーション稼働情報、および接続情報を含む。路車情報生成部 202 は、例えばバス 132 を介して車載システム 102 内の各部と通信することにより車両 104 において稼働しているアプリケーションを特定し、アプリケーション稼働情報を生成できる。これにより、後述するように、適切なセキュリティルールを生成するための車外通信パラメータを決定できる。

[0049] アプリケーションとは、例えば、サーバ 112 から提供されるサービスを受けるために車載システム 102 において実行されるプログラムである。アプリケーションは、車両 104 において実行され得るプログラムであればよく、車載装置 122 が実行するプログラムに限らず、自動運転 ECU 126、認証 ECU 128 および駆動 ECU 130 等の ECU が実行するプログラムをも含む。

[0050] なお、路車情報が接続情報を含んでいない場合、即ち、路車情報生成部 202 が接続情報を取得できない場合がある。そのような場合であっても、後述するように、路車情報に含まれる情報から、接続情報を生成できる。したがって、路車情報は、上記した情報のうち、少なくとも一部を含んでいればよい。

[0051] 車外通信パラメータ判定情報決定部 204 は、路車情報生成部 202 によ

り作成された路車情報から車外通信パラメータ判定情報を決定する。決定された車外通信パラメータ判定情報は、メモリ 142 に記憶される。車外通信パラメータ判定情報は、車外通信部 120 と車両 104 の外部との無線通信に関するセキュリティルールを決定するための情報、即ち、車外との通信に関する車外通信パラメータのうち、セキュリティルールにより制限するパラメータを判定するために利用される情報である。車外通信パラメータ判定情報は、例えば、アプリケーション稼働情報および接続情報を含む。これにより、後述するように、適切なセキュリティルールを生成できる。路車情報がアプリケーション稼働情報および接続情報のいずれかを含む場合、車外通信パラメータ判定情報決定部 204 は、路車情報に含まれるその情報を、車外通信パラメータ判定情報として決定する。

[0052] 上記したように、路車情報は、接続情報を含んでいない場合もある。その場合には、車外通信パラメータ判定情報決定部 204 は、路車情報に含まれていない接続情報を間接的に決定する。即ち、車外通信パラメータ判定情報決定部 204 は、路車情報に含まれている情報から、含まれていない接続情報を推定する。例えば、車外通信パラメータ判定情報決定部 204 は、路車情報に含まれる位置情報および地図情報（車外装置マップを含む）により、車外通信部 120 が通信接続している外部装置（例えば、IP アドレスおよびポート番号）およびその通信状態（例えば、通信速度）を推測でき、したがって接続情報を決定できる。これにより、路車情報から接続情報を生成でき、適切なセキュリティルールを生成できる。

[0053] セキュリティルール生成部 206 は、車外通信パラメータ判定情報決定部 204 により決定された車外通信パラメータ判定情報から、セキュリティルールを生成する。車外通信部 120 による通信に関するパラメータである車外通信パラメータは、例えば、外部からのアクセス頻度、通信量（即ち通信速度）、通信確立されたセッションの数、通信確立するために通信される SYN パケットの数、通信先 IP アドレス、および通信先ポート番号を含む。これにより、後述するように、車外通信部 120 による通信の安全性を向上

できる。車外通信パラメータは、これらに限定されない。セキュリティルール生成部206は、車外通信パラメータ判定情報（例えば、アプリケーション稼働情報および接続情報）から、制限すべき車外通信パラメータを特定し、その制限内容を決定し、例えば、車外通信パラメータと制限内容とを対応させたテーブル（以下、セキュリティルールテーブルという）を生成し、セキュリティルールとする。セキュリティルール生成部206は、決定したセキュリティルールを車外通信部120のセキュリティ部208に出力する。また、セキュリティルール生成部206は、生成したセキュリティルールをメモリ142に記憶する。

- [0054] アプリケーション稼働情報によりアプリケーションが特定されるので、そのアプリケーションによる車外通信の仕様が分かれば、セキュリティルール生成部206は車外通信パラメータを決定でき、アプリケーション毎のセキュリティルールテーブルを生成し、メモリ142に記憶できる。したがって、予め各アプリケーションの通信仕様がメモリ142に記憶されていればよい。例えば、各アプリケーションが解析されて通信仕様がメモリ142に記憶されてもよい。車載システム102にダウンロードされて記憶されているアプリケーションを解析することにより、そのアプリケーションの通信条件（例えば、通信先IPアドレス、通信先ポート番号、通信量等）を特定でき、セキュリティルールテーブルを生成できる。また、後述するように、アプリケーションの通信仕様は、サーバからダウンロードされてメモリ142に記憶されていてもよい。なお、複数のアプリケーションが起動される場合には、各アプリケーションに対応する車外通信パラメータが得られるが、制限される車外通信経路は1つの車外通信部120であるので、セキュリティルール生成部206は、複数のセキュリティルールテーブルを統合する。例えば、複数のセキュリティルールテーブルの各々に通信量が含まれる場合、それらの合計値を含むセキュリティルールが生成される。複数のセキュリティルールテーブルの各々に通信先IPアドレスおよび通信先ポート番号の組が含まれる場合、それら全てを含むセキュリティルールが生成される。これに

より、車外通信部１２０の通信を制限するセキュリティルールを効率よく生成できる。

[0055] セキュリティ部２０８は入力されたセキュリティルールを内部メモリに記憶し、セキュリティルールに従って、車外通信部１２０により実行される通信を制限する。したがって、車外通信部１２０による通信の安全性を向上できる。路側情報取得部２００、路車情報生成部２０２、車外通信パラメータ判定情報決定部２０４、セキュリティルール生成部２０６およびセキュリティルール生成部２０６による上記の処理は、繰返し実行され、セキュリティルールは繰返し生成される。車両１０４におけるアプリケーションの稼働状況および外部装置との接続状態の変化に応じて路車情報が変化し、その変化に応じて車外通信パラメータ判定情報が変化する。したがって、車両１０４におけるアプリケーションの稼働状況および外部装置との接続状態の変化に応じて、セキュリティルールは変化する。セキュリティ部２０８は、新たにセキュリティルール生成部２０６からセキュリティルールが入力されると、内部メモリに記憶しているセキュリティルールを、新たなセキュリティルールにより書き換えて更新する。

[0056] これにより、車載システム１０２（具体的には車載装置１２２）は、搭載されている車両１０４におけるアプリケーションの稼働状況および外部装置との接続状態に応じて適切なセキュリティルールを決定できる。また、車載システム１０２は、車両１０４におけるアプリケーションの稼働状況および外部装置との接続状態の変化に応じてセキュリティルールを動的に制御できる。したがって、サイバーセキュリティ攻撃に対策でき、外部との通信の安全性を向上できる。セキュリティルールの決定は、車両１０４の内部において取得可能な情報、およびサーバから取得可能な情報を処理することにより可能であるので、機械学習等の多くのリソースが必要な処理を実行することなく、低い計算コストにより実現できる。

[0057] なお、上記においては、セキュリティルール生成部２０６が、アプリケーション毎のセキュリティルールテーブルを記憶する場合を説明したが、これ

に限定されない。セキュリティルール生成部 206 は、アプリケーション毎に、セキュリティルールを生成するために用いられる車外通信パラメータを記憶していればよい。記憶形式はテーブル以外の形式であってもよい。

[0058] [車載装置の動作]

図 6 を参照して、車載装置 122 によるセキュリティルールの制御動作に関して、図 5 に示した機能を参照しつつ説明する。図 6 に示した処理は、車載バッテリー等から車載システム 102 に電力が供給され、車載装置 122 の制御部 140（図 2 参照）が所定のプログラムをメモリ 142 から読出して実行することにより実現される。なお、以下に示す処理が実行された結果は、適宜メモリ 142 に記憶される。

[0059] ステップ 300 において、制御部 140 は、車外通信部 120 を介して路側情報を受信したか否かを判定する。受信したと判定された場合、制御はステップ 302 に移行する。そうでなければ、制御はステップ 304 に移行する。路側情報は、例えばサーバ 112 から送信される。

[0060] ステップ 302 において、制御部 140 は、ステップ 300 により受信した路側情報をメモリ 142 に記憶する。その後、制御はステップ 304 に移行する。ステップ 300 およびステップ 302 の処理は、図 5 の路側情報取得部 200 の機能に対応する。

[0061] ステップ 304 において、制御部 140 は、車載システム 102 が搭載されている車両 104 の車両情報を取得する。制御部 140 は、取得した車両情報をメモリ 142 に記憶する。その後、制御はステップ 306 に移行する。車両情報は、例えば、車両 104 の位置情報、アプリケーション稼働情報および接続情報を含む。車両 104 は、車両情報を車外通信部 120、自動運転 ECU 126 および駆動 ECU 130 等から取得する。

[0062] ステップ 306 において、制御部 140 は、ステップ 304 により取得した車両情報およびステップ 300 により受信した路側情報をメモリ 142 から読出し、車両情報と路側情報とを合わせて路車情報を生成し、メモリ 142 に記憶する。車両情報および路側情報に重複する情報が含まれていれば、

制御部 140 は、路車情報には重複する情報のうちの 1 つを残す。その後、制御はステップ 308 に移行する。ステップ 304 およびステップ 306 の処理は、図 5 の路車情報生成部 202 の機能に対応する。

[0063] ステップ 308 において、制御部 140 は、ステップ 306 により生成された路車情報に基づいて、車外通信パラメータ判定情報を決定し、メモリ 142 に記憶する。その後、制御はステップ 310 に移行する。ステップ 308 の処理は、図 5 に示した車外通信パラメータ判定情報決定部 204 の機能に対応する。

[0064] ステップ 310 において、制御部 140 は、ステップ 308 により決定された車外通信パラメータ判定情報に基づいてセキュリティルールを生成する。その後、制御はステップ 312 に移行する。

[0065] ステップ 312 において、制御部 140 は、セキュリティルールをセキュリティ部 208 に出力する。その後、制御はステップ 314 に移行する。ステップ 310 およびステップ 312 の処理は、図 5 に示したセキュリティルール生成部 206 の機能に対応する。

[0066] ステップ 314 において、制御部 140 は、終了するか否かを判定する。終了すると判定された場合、本プログラムは終了する。そうでなければ、制御はステップ 300 に戻り、上記した処理が繰返される。終了の指示は、例えば、車載装置 122 への電力供給が停止されることにより成される。

[0067] [セキュリティ部の動作]

図 7 を参照して、車外通信部 120 のセキュリティ部 208（図 5 参照）による通信を制限する動作に関して説明する。図 7 に示した処理は、例えば、セキュリティ部 208 内部の制御部（例えば CPU）がセキュリティ部 208 の内部メモリから所定のプログラムを讀出して実行することにより実現される。

[0068] ステップ 400 において、セキュリティ部 208 は、車載装置 122 からセキュリティルールを取得したか否かを判定する。取得したと判定された場合、制御はステップ 402 に移行する。そうでなければ、制御はステップ 4

04に移行する。セキュリティルールは、図6に示したステップ312により、車載装置122からセキュリティ部208に出力される。

[0069] ステップ402において、セキュリティ部208は、現在使用しているセキュリティルールを更新する。具体的には、セキュリティ部208は、現在使用しているセキュリティルールを、ステップ400により取得したセキュリティルールにより代替する（例えば、セキュリティ部208の内部メモリにおいて上書きする）。その後、制御はステップ404に移行する。

[0070] ステップ404において、セキュリティ部208は、セキュリティルールに反する通信があったか否かを判定する。あったと判定された場合、制御はステップ406に移行する。そうでなければ、制御はステップ408に移行する。セキュリティルールに反する通信とは、セキュリティルールとして規定されている車外通信パラメータの範囲を逸脱する通信を意味する。例えば、セキュリティルールが、車外通信パラメータとして通信量を含み、そのしきい値（即ち上限値）が a （bps）に設定されていれば、車両104の外部から a （bps）を超えるデータを受信した場合、セキュリティ部208はセキュリティルールに反する通信があったと判定する。例えば、セキュリティルールが、車外通信パラメータとして通信先IPアドレスを含んでいれば、通信先IPアドレスとは異なるIPアドレスを送信元アドレスとして含むパケットデータを受信した場合、セキュリティ部208はセキュリティルールに反する通信があったと判定する。

[0071] なお、ステップ404の処理を実行する期間は、セキュリティルールに含まれる車外通信パラメータによって変わり得る。例えば、セキュリティルールが、車外通信パラメータとして通信先IPアドレスを含んでいれば、セキュリティ部208は、受信したパケット毎に、当該パケットに含まれる送信元アドレスが通信先IPアドレスであるか否かを判定すればよい。一方、セキュリティルールが、車外通信パラメータとして通信量（しきい値は a （bps））を含む場合、所定期間にわたって受信したパケットをバッファし、その合計値が a （bps）以下であるか否かを判定する。

- [0072] ステップ406において、セキュリティ部208は、セキュリティルールに則ったデータのみを通信可能とする。即ち、セキュリティ部208は、ステップ404によりセキュリティルールに反すると判定された受信パケットを破棄し、そのパケットをアプリケーションには渡さない。セキュリティ部208は、ステップ404によりセキュリティルールに反しないと判定された受信パケットを、そのパケットに含まれるポート番号に対応するアプリケーションに渡す。その後、制御はステップ410に移行する。
- [0073] ステップ408において、セキュリティ部208は、受信した全データを通信可能とし、各パケットを、そのパケットに含まれるポート番号に対応するアプリケーションに渡す。その後、制御はステップ410に移行する。
- [0074] ステップ410において、セキュリティ部208は、終了するか否かを判定する。終了すると判定された場合、本プログラムは終了する。そうでなければ、制御はステップ400に戻り、上記した処理が繰返される。終了の指示は、例えば車外通信部120への電力供給が停止されることにより成される。
- [0075] 以上により、車載システム102（具体的には車載装置122）は、搭載されている車両104におけるアプリケーションの稼働状況および外部装置との接続状態に応じた適切なセキュリティルールを決定できる。また、車載システム102は、車両104におけるアプリケーションの稼働状況および外部装置との接続状態の変化に応じて、セキュリティルールを動的に制御できる。したがって、車載システム102は、サイバーセキュリティ攻撃に対策でき、外部との通信の安全性を向上できる。セキュリティルールの決定は、車両104の内部において取得可能な情報、およびサーバから取得可能な情報を処理することにより可能であるので、機械学習等の多くのリソースが必要な処理を実行することなく、低い計算コストにより実現できる。
- [0076] 上記においては、ゲートウェイとしての役割を担う車載装置122がセキュリティルールを制御する機能を有する場合を説明したが、これに限定されない。車載システム102を構成する車載装置122以外の要素（例えば車

外通信部 120) がセキュリティルールを制御する機能を有していてもよい。また、車載システム 102 は、セキュリティルールを制御するための専用 ECU を有していてもよい。車外通信部 120 および専用 ECU 等も、車両 104 に搭載されており車載装置に含まれる。

[0077] 図 8 から図 12 を参照して具体例を示す。

[第 1 例]

図 8 を参照して、セキュリティルールの生成に利用される車外通信パラメータ判定情報に含まれるアプリケーション稼働情報を直接的に決定する例に関して説明する。ここでは、車両 104 の駐車時に車両 104 のドアがロックされており、認証後に車両 104 のドアを開閉（即ち開錠および施錠）するアプリケーションが起動するとする。図 8 の左側には、車両 104 の駐車時且つ認証前の情報を示している。図 8 の右側には、車両 104 の駐車時且つ認証後の情報を示している。認証には、例えばユーザのスマートフォンが利用され、車載システム 102 の認証 ECU 128（図 2 参照）は、車外通信部 120 を介してユーザのスマートフォンと通信する。例えば、ユーザのスマートフォンから送信される認証用トリガ信号を、車載システム 102 の認証 ECU 128 が受信する。

[0078] 路車情報は、アプリケーション稼働情報を含む。上記したように、車載装置 122 は、車載システム 102 の各部と通信し、路車情報に含まれるアプリケーション稼働情報を取得できる。車両 104 は停車中でありドアが施錠されており、稼働しているアプリケーションはなく、路車情報に含まれるアプリケーション稼働情報には、稼働しているアプリケーションがないことを表す情報（例えば「なし」）が設定されている。車載装置 122 は、認証前であることを、認証 ECU 128 が認証用トリガ信号を受信していないことにより特定できる。車載装置 122 は、路車情報に含まれるアプリケーション稼働情報から直接、車外通信パラメータ判定情報のアプリケーション稼働情報を「なし」と決定する。その結果、車載装置 122 は、セキュリティルールとして、通信量の制限に対応する通信フィルタしきい値（即ち上限値）

をTh1に設定する。Th1は、車載装置122が車外通信部120を介して外部（即ち、ユーザのスマートフォン）から認証用トリガ信号を受信できるだけの小さい値である。Th1は、適切な値が予め設定されていればよい。

- [0079] 認証ECU128が認証用トリガ信号を受信すると認証が行われ、車載装置122は、認証ECU128から認証後を表す情報を取得する。車載装置122は、車両104が、駐車時且つ認証後であると特定できる。また、車載装置122は、車載システム102の各部との通信を試み、ドア開閉アプリケーションが稼働していることを特定し、路車情報に含まれるアプリケーション稼働情報に、ドア開閉アプリケーションを特定する情報（即ち「ドア開閉」）を設定する。車載装置122は、路車情報に含まれるアプリケーション稼働情報から直接、車外通信パラメータ判定情報のアプリケーション稼働情報を「ドア開閉」と決定する。図8においては、アプリケーションを特定する情報としてアプリケーションの名称を用いる場合を示しているが、各アプリケーションに一意に対応する数字、記号、またはそれらの組合せ等を用いてもよい。車外通信パラメータ判定情報から、車載装置122は、セキュリティルールとして、通信量の制限に関する通信フィルタしきい値をTh2に設定する。Th2は、Th1よりも大きい値である。例えば、ユーザによるスマートフォンの画面操作（例えば、タッチパネルに表示されている施錠ボタンまたは開錠ボタンへのタッチ操作）によりスマートフォンから送信されるデータ（例えば、施錠または開錠を特定するコードを含む）を受信できる値に、Th2が設定されていればよい。また、ドア開閉アプリケーション以外のアプリケーションが稼働することを想定して、それらによる通信データ量をも考慮して、Th2が決定されてもよい。なお、予め、車載システム102において起動され得るアプリケーションとその車外通信パラメータ（例えば、通信量、通信先IPアドレスおよび通信先ポート番号等）とを対応させてメモリ142に記憶しておけば、アプリケーション稼働情報に基づいてセキュリティルールを生成できる。

[0080] これにより、車両 104 の駐車時且つ認証前において、想定される通信量（即ち T_h1 ）を超えるデータが車載システム 102 に対して送信された場合、送信データをフィルタ可能になる。したがって、例えば D o S 攻撃に対策可能になる。

[0081] [第 2 例]

セキュリティルールの生成に利用される車外通信パラメータ判定情報に含まれるアプリケーション稼働情報を直接的に決定する、図 8 と異なる例を、図 9 および図 10 に示す。ここでは、図 9 を参照して、交差点を含むエッジサービス領域 222 において、エッジサーバ（図示せず）による運転支援サービスが提供されており、エッジサービス領域 222 を含む広いクラウドサービス領域 220 においてはサービスが提供されていないとする。図 9 において、現在の車両の位置を実線により示し、過去の位置を破線により示している。車両 104 B および車両 104 A は、同じ車両 104 の現在および過去の車両位置を示している。各車両の走行方向を矢印により示している。

[0082] 図 10 を参照して、左側には、車両 104 A が、エッジサービス領域 222 外の直線道路に位置しているときの情報を示している。図 10 の右側には、車両 104 B が、エッジサービス領域 222 内に位置しているときの情報を示している。路車情報は、アプリケーション稼働情報を含む。エッジサービス領域 222 外の直線道路に位置している車両 104 A の車載装置 122 は、車載システム 102 の各部との通信を試み、稼働しているアプリケーションはないことを特定し、路車情報に含まれるアプリケーション稼働情報には「なし」を設定する。これにより、車載装置 122 は、路車情報に含まれるアプリケーション稼働情報から直接、車外通信パラメータ判定情報のアプリケーション稼働情報を「なし」と決定する。その結果、車載装置 122 は、セキュリティルールとして、通信アクセス許可はなし、即ち、車外との通信を許可しないことを設定する。

[0083] エッジサービス領域 222 内の交差点の右折ラインに位置している車両 104 B の車載装置 122 は、車載システム 102 の各部との通信を試み、右

折支援アプリケーションが稼働していることを特定し、路車情報に含まれるアプリケーション稼働情報に、右折支援アプリケーションを特定する情報（即ち「右折支援」）を設定する。これにより、車載装置１２２は、路車情報に含まれるアプリケーション稼働情報から直接、車外通信パラメータ判定情報のアプリケーション稼働情報を「右折支援」と決定する。この車外通信パラメータ判定情報から、車載装置１２２は、右折支援情報のサービスを提供しているエッジサーバとの通信アクセスを許可する。即ち、車載装置１２２は、通信先ＩＰアドレスおよび通信先ポート番号に、エッジサーバのＩＰアドレスおよびポート番号を含むセキュリティルールを生成する。

[0084] これにより、車両１０４が、サービス対象外のエリアに位置している場合に、車載システム１０２に想定しない通信先からのアクセスがあった際に、そのアクセスを制限できる。例えば、通信先を偽ったアクセス（即ち、なりすまし）への対策が可能になる。

[0085] [第３例]

図１１を参照して、セキュリティルールの生成に利用される車外通信パラメータ判定情報に含まれる接続情報（即ち、外部装置との通信接続状態を表す情報）を間接的に決定する例に関して説明する。ここでは、車両１０４の位置は、第２例（図９参照）と同様に変化するとする。但し、第３例においては、第２例と異なり、エッジサービス領域２２２外のクラウドサービス領域２２０において、車載システム１０２がクラウドサーバ（図示せず）と通信するとする。なお、ここでは、接続情報に関して説明し、稼働アプリケーション情報に関しては省略する。

[0086] 図１１を参照して、左側には、車両１０４Ａが、クラウドサービス領域２２０内であるがエッジサービス領域２２２外の道路に位置しているときの情報を示し、右側には、車両１０４Ｂが、エッジサービス領域２２２内の道路に位置しているときの情報を示している。路車情報は、例えば、位置情報および地図情報を含み、接続情報を含まない。車両１０４Ａの車載装置１２２は、路車情報（例えば、位置情報および地図情報）から、車両位置を、エッ

ジサービス領域 2 2 2 外のクラウドサービス領域 2 2 0（即ち、クラウド通信エリア）と特定できる。車載装置 1 2 2 は、車外通信パラメータ判定情報の接続情報をクラウド接続と決定する。その結果、車載装置 1 2 2 は、セキュリティルールとして、通信量の制限に対応する通信フィルタしきい値（即ち上限値）を T h 3 に設定する。T h 3 は、クラウドサーバが提供しているサービスに基づいて予め設定されていればよい。

[0087] 車両 1 0 4 B の車載装置 1 2 2 は、路車情報から、車両位置を、エッジサービス領域 2 2 2 内（即ち、エッジサーバ通信エリア）と特定できる。車載装置 1 2 2 は、車外通信パラメータ判定情報の接続情報をエッジサーバ接続と決定する。その結果、車載装置 1 2 2 は、セキュリティルールとして、通信量の制限に対応する通信フィルタしきい値を T h 4 に設定する。T h 4 は、エッジサーバが提供しているサービス（例えば、右折支援サービス）に基づいて予め設定されていればよい。一般に、車載システムと、交差点等の狭域におけるサービスを提供するエッジサーバとの通信は、車両の近くに人等の動的物体が多く、広域におけるサービスを提供するクラウドサーバとの通信よりもリアルタイム性は高いと考えられる。したがって、例えば T h 4 > T h 3 と設定される。

[0088] これにより、車両 1 0 4 が、クラウド通信エリア内に位置する場合に、接続状態から想定される通信量を超えるデータが車載システム 1 0 2 に対して送信された場合、送信データをフィルタ可能になる。したがって、例えば D o S 攻撃に対策可能になる。

[0089] [第 4 例]

図 1 2 を参照して、複数のアプリケーションが稼働している状態を含む場合にセキュリティルールが生成される例に関して説明する。ここでは、車両 1 0 4 の位置は、第 2 例（図 9 参照）と同様に変化するとする。但し、第 4 例においては、第 2 例と異なり、エッジサービス領域 2 2 2 を含むクラウドサービス領域 2 2 0 において、車載システム 1 0 2 が経路案内アプリケーションを稼働してクラウドサーバと通信するとする。

[0090] 図12を参照して、左側には、車両104Aの位置が、クラウドサービス領域220内であるがエッジサービス領域222外の道路に位置しているときの情報を示し、右側には、車両104Bの位置が、エッジサービス領域222内の道路に位置しているときの情報を示している。路車情報は、例えば、位置情報、地図情報およびアプリケーション稼働情報を含む。車両104Aの車載装置122は、路車情報に含まれる位置情報および地図情報から、車両位置を、クラウドサービス領域220（即ち、クラウド通信エリア）と特定できる。これにより、車載装置122は、車外通信パラメータ判定情報の接続情報に「クラウド接続」を設定する。また、車載装置122は、車載システム102の各部との通信を試み、経路案内アプリケーションが稼働していることを特定し、路車情報に含まれるアプリケーション稼働情報に、経路案内アプリケーションを特定する情報（即ち「経路案内」）を設定する。これにより、車載装置122は、路車情報に含まれるアプリケーション稼働情報から直接、車外通信パラメータ判定情報のアプリケーション稼働情報に「経路案内」を設定する。この車外通信パラメータ判定情報（即ち、接続情報が「クラウド接続」、アプリケーション稼働情報が「経路案内」）から、車載装置122は、経路案内のサービスを提供しているクラウドサーバとの通信アクセスを許可する。即ち、車載装置122は、通信先IPアドレスおよび通信先ポート番号に、クラウドサーバのIPアドレスおよびポート番号を含み、通信量の制限に対応する通信フィルタしきい値（即ち上限値）がa（Mbps）であるセキュリティルールを生成する。a（Mbps）は、経路案内サービスに基づいて予め設定されていればよい。

[0091] 車両104Bの車載装置122は、路車情報に含まれる位置情報および地図情報から、車両位置を、クラウドサービス領域220に含まれるエッジサービス領域222内の交差点の右折ラインと特定できる。これにより、車載装置122は、車外通信パラメータ判定情報の接続情報に「クラウド接続」および「エッジサーバ接続」を設定する。また、車載装置122は、車載システム102の各部との通信を試み、既に稼働している経路案内アプリケー

ションに加えて、右折支援アプリケーションが稼働していることを特定し、路車情報に含まれるアプリケーション稼働情報に、「経路案内」と右折支援アプリケーションを特定する情報（即ち「右折支援」）とを設定する。これにより、車載装置 122 は、路車情報に含まれるアプリケーション稼働情報から直接、車外通信パラメータ判定情報のアプリケーション稼働情報に、「経路案内」および「右折支援」を設定する。この車外通信パラメータ判定情報（即ち、接続情報が「クラウド接続」および「エッジサーバ接続」、アプリケーション稼働情報が「経路案内」および「右折支援」）から、車載装置 122 は、経路案内のサービスを提供しているクラウドサーバ、および、右折支援のサービスを提供しているエッジサーバとの通信アクセスを許可する。即ち、車載装置 122 は、通信先 IP アドレスおよび通信先ポート番号に、クラウドサーバおよびエッジサーバの IP アドレスおよびポート番号を含み、通信量の制限に対応する通信フィルタしきい値（即ち上限値）が $a + b$ (Mbps) であるセキュリティルールを生成する。b (Mbps) は、右折支援サービスに基づいて予め設定された値である。

[0092] これにより、車両 104 がクラウド通信エリアに位置するときに、接続状態から想定される通信量を超えるデータが車載システム 102 に対して送信された場合、送信データをフィルタ可能になる。したがって、例えば D o S 攻撃に対策可能になる。また、車両 104 が、サーバからサービスが提供されるエリアに位置するときに、車載システム 102 に想定しない通信先からのアクセスがあった際に、そのアクセスを制限できる。例えば、通信先を偽った（即ち、成りすまし）アクセスへの対策が可能になる。

[0093] [変形例]

車両 104 において稼働するアプリケーションは、車載システム 102 により新規にサーバからダウンロードされる場合がある。また、既に、車載システム 102 に記憶されているアプリケーションが更新される場合、即ち、車載システム 102 が、新たなバージョンのアプリケーション（以下、更新アプリケーションという）をサーバからダウンロードする場合がある。いず

れの場合にも、車載システム１０２におけるセキュリティルールの生成に影響する。変形例に係る通信システムは、これに対応し、効率的にセキュリティルールを生成できる。

[0094] 変形例に係る通信システムは、図１に示した通信システム１００と同様に構成されており、車載システム、路側機およびサーバのハードウェア構成はそれぞれ図２、図３および図４と同様である。但し、変形例に係る通信システムは、通信システム１００とは異なり、車載システムの車載装置の機能構成を示す図５が図１３により代替され、サーバ１１２からアプリケーション（更新アプリケーションを含む）を送信する。以下においては、適宜、図１から図４に示した符号を参照する。

[0095] [変形例に係る車載システムの機能的構成]

図１３を参照して、変形例に係る車載装置１２２Ａの機能、即ちセキュリティルールの制御に関する機能に関して説明する。車載装置１２２Ａは、路側情報取得部２００、路車情報生成部２０２、車外通信パラメータ判定情報決定部２０４、セキュリティルール生成部２０６およびセキュリティルールテーブル更新部２３０を含む。車外通信部１２０は、パケットフィルタ等の通信のセキュリティを実行するセキュリティ部２０８を含む。図１３は、図５において、セキュリティルールテーブル更新部２３０を追加したものである。図１３において、図５に示した符号と同じ符号を付した要素の機能は、図５と同じである。したがって、以下においては、重複説明を繰返さず、主として、異なる点に関して説明する。

[0096] セキュリティルールテーブル更新部２３０の機能は、路側情報取得部２００、路車情報生成部２０２、車外通信パラメータ判定情報決定部２０４およびセキュリティルール生成部２０６と同様に、図２に示した制御部１４０およびメモリ１４２により実現される。路側情報取得部２００は、車外通信部１２０によりサーバ１１２から送信された路側情報を取得する。路車情報生成部２０２は、車外通信部１２０、自動運転ＥＣＵ１２６および駆動ＥＣＵ１３０等から取得した車両情報に、路側情報取得部２００により取得された

路側情報を加えて、路車情報を生成する。車外通信パラメータ判定情報決定部204は、路車情報生成部202により作成された路車情報から車外通信パラメータ判定情報を決定する。セキュリティルール生成部206は、車外通信パラメータ判定情報決定部204により決定された車外通信パラメータ判定情報から、セキュリティルールを生成し、生成したセキュリティルールを車外通信部120のセキュリティ部208に出力する。セキュリティルール生成部206は、アプリケーション毎のセキュリティルールテーブルを生成し、メモリ142に記憶している。セキュリティ部208は入力されたセキュリティルールに従って、車外通信部120により実行される通信を制限する。

[0097] セキュリティルールテーブル更新部230は、サーバ112から新規のアプリケーションまたは更新アプリケーションがダウンロードされたか否かを判定し、ダウンロードされたと判定した場合、セキュリティルールテーブルを更新する。具体的には、新規のアプリケーションがダウンロードされた場合、セキュリティルールテーブル更新部230は、ダウンロードされたアプリケーションの通信仕様から、そのアプリケーションの車外通信パラメータを決定し、セキュリティルールテーブルを生成してメモリ142に記憶する。更新アプリケーションがダウンロードされた場合、セキュリティルールテーブル更新部230は、ダウンロードされたアプリケーションの通信仕様から、そのアプリケーションの車外通信パラメータを決定し、セキュリティルールテーブルを生成し、既にメモリ142記憶されている旧バージョンのセキュリティルールテーブルに上書きする。

[0098] 図14を参照して、アプリケーションの仕様を表すアプリケーション仕様情報、および、セキュリティテーブルの例を示す。図14において、上側に表形式により、右折支援を受けるためのアプリケーション仕様情報を示す。アプリケーション仕様情報は、車載装置122がサーバ112からダウンロードしたアプリケーションが解析されることにより生成され得る。通信先の欄は、アプリケーションを実行する主体（即ち車載システム102）が通信

する相手を表し、車外サーバ（即ちサーバ１１２）のＩＰアドレス、および、サービスを特定するためのポート番号を含む。通信内容の欄は、サービスとしてサーバ１１２から送信される情報を表し、サーバ１１２がサービス対象とする交差点を含む所定エリア内における物体（主として動的物体）に関する情報である。通信量の欄には、サーバ１１２から車載システムへの送信の通信量を算出するための情報が含まれている。即ち、所定エリア内における１物体に関して最大 a (bit) が割当てられ、データが割当てられる物体数の上限は b であり、サーバ１１２から送信される情報の更新周期は c (ms) であることが含まれている。

[0099] セキュリティルールテーブル更新部２３０は、アプリケーション仕様情報から、図１４の下側に表形式により示すようなセキュリティテーブルを生成する。通信アクセス許可には、通信先である車外サーバ（即ちサーバ１１２）のＩＰアドレスおよびポート番号が設定されている。通信フィルタしきい値（即ち上限値）は、アプリケーション仕様情報の通信量の欄に含まれる情報から算出される値である。

[0100] これにより、ダウンロードされたアプリケーションが稼働すると、車外通信パラメータ判定情報決定部２０４は、メモリ１４２に新たに記憶された車外通信パラメータを用いて車外通信パラメータ特定情報を決定する。決定された車外通信パラメータ特定情報に基づいて、セキュリティルール生成部２０６は、メモリ１４２に記憶された新たなセキュリティルールテーブルを用いて、新たなセキュリティルールを生成する。

[0101] なお、更新アプリケーションが重要なアプリケーションであり、現在稼働しているアプリケーションに代えて速やかに更新アプリケーションを稼働させる必要がある場合がある。そのような場合には速やかに、稼働しているアプリケーションを停止して更新アプリケーションを稼働させ、車外通信パラメータ判定情報決定部２０４に、メモリ１４２に新たに記憶された車外通信パラメータを用いて車外通信パラメータ特定情報を決定させる。これにより、セキュリティルール生成部２０６は、新たなセキュリティルールを生成す

る。

[0102] このように、アプリケーション（新規アプリケーションおよび更新アプリケーションを含む）のダウンロードにより、セキュリティルール（具体的にはセキュリティルールテーブル）を更新することにより、セキュリティルールを適切な状態に維持できる。

[0103] 上記においては、車載装置 1 2 2 が、サーバ 1 1 2 からダウンロードしたアプリケーションを解析することにより、アプリケーション仕様情報が生成される場合を説明したが、これに限定されない。アプリケーション仕様情報は、サーバ 1 1 2 から車載装置 1 2 2 に送信されてもよい。アプリケーションを送信するサーバ 1 1 2 は、アプリケーションの仕様を記憶しているので、アプリケーション仕様情報を生成して車載装置 1 2 2 に送信できる。これにより、車載装置 1 2 2 におけるセキュリティルールを決定するための演算処理による負荷を削減できる。

[0104] 例えば、サーバ 1 1 2 は、新規アプリケーションおよび更新アプリケーションを車載システム 1 0 2 に送信する際に、アプリケーションの仕様情報を送信する。車載装置 1 2 2 は、車載システム 1 0 2 において実行されるアプリケーションの仕様情報を車載システム 1 0 2 の外部の装置から受信することにより、セキュリティルールを生成するために、稼働するアプリケーションを解析することが不要になる。したがって、車載装置 1 2 2 は、アプリケーションの稼働状況に応じてセキュリティルールを決定するための演算処理による負荷をより軽減できる。

[0105] 上記においては、車載システム 1 0 2（具体的には車載装置 1 2 2）がセキュリティルールを生成し、それに従って、車外との通信を制限する場合を説明したが、これに限定されない。車両 1 0 4 の外部装置（例えば、サーバ 1 1 2 または路側機 1 0 6）が、車載システム 1 0 2 のセキュリティルールを生成して車載システム 1 0 2 に送信し、車載システム 1 0 2 が受信したセキュリティルールに従って、車外との通信を制限してもよい。例えば、サーバ 1 1 2 は、車載システム 1 0 2 による車両 1 0 4 の外部との通信を制限す

るセキュリティルールを、車両 104 の外部に関する情報および車両 104 の車両情報を含む路車情報に基づいて生成する生成部と、車載システム 102 に、セキュリティルールを送信する通信部とを含むことができる。これにより、車載システム 102 は、サーバ 112 から受信したセキュリティルールに従って、車外との通信を動的に制御できる。

[0106] また、サーバ 112 の通信部 164 は、車載システム 102 から、車両 104 の車両情報を受信できる。サーバ 112 は、車両 104 の外部に関する情報である路側情報に、通信部 164 により受信された車両情報を加えて路車情報を生成する路車情報生成部と、路車情報に基づいて車外通信パラメータ判定情報を決定する決定部とさらに含むことができ、生成部は、車外通信パラメータ判定情報に基づいてセキュリティルールを生成することができる。これにより、車載システム 102 においてセキュリティルールを決定するための演算処理による負荷を削減できる。

[0107] なお、上述の実施形態の各処理（各機能）は、1 または複数のプロセッサを含む処理回路（Circuitry）により実現されてもよい。上記処理回路は、上記 1 または複数のプロセッサに加え、1 または複数のメモリ、各種アナログ回路および各種デジタル回路のいずれかが組み合わされた集積回路等により構成されてもよい。上記 1 または複数のメモリは、上記各処理を上記 1 または複数のプロセッサに実行させるプログラム（命令）を格納する。上記 1 または複数のプロセッサは、上記 1 または複数のメモリから読出した上記プログラムに従い上記各処理を実行してもよいし、予め上記各処理を実行するように設計された論理回路に従って上記各処理を実行してもよい。上記プロセッサは、CPU、GPU（Graphics Processing Unit）、DSP（Digital Signal Processor）、FPGA（Field Programmable Gate Array）、ASIC（Application Specific Integrated Circuit）等、コンピュータの制御に適合する種々のプロセッサであってよい。

[0108] また、車載システム 102 の処理（具体的には、車載装置 122 が実行する処理（例えば、図 6 に示した処理））をコンピュータに実行させるプログラムを記録した記録媒体を提供できる。記録媒体は、例えば光ディスク（DVD（Digital Versatile Disc）等）、着脱可能な半導体メモリ（USB（Universal Serial Bus）メモリ等）である。コンピュータプログラムは通信回線により伝送され得るが、記録媒体は非一時的な記録媒体を意味する。記録媒体に記憶されたプログラムを車両に搭載されたコンピュータに読込ませることにより、コンピュータは、上記したように、車載システムが、路側装置等の外部装置にデータをアップロードする際に、遅延時間および通信帯域を考慮して、外部装置が提供するサービスにより有効に利用され得るデータを送信することを可能とする。

[0109] （付記）

即ち、コンピュータ読取り可能な非一時的な記録媒体は、

車両に搭載されるコンピュータに、前記車両の車両情報および前記車両の外部に関する情報である路側情報を含む路車情報に基づいて生成されたセキュリティルールに従って、前記車両の外部にある外部装置と通信する通信部に、前記外部装置との通信を制限するセキュリティ機能を実現させ、前記車両情報は、前記車両において稼働しているアプリケーションを特定するアプリケーション稼働情報および前記外部装置との通信接続状態を表す接続情報の少なくともいずれか 1 つを含む、コンピュータプログラムを記憶している。

[0110] 以上、実施の形態を説明することにより本開示を説明したが、上記した実施の形態は例示であって、本開示は上記した実施の形態のみに制限されるわけではない。本開示の範囲は、発明の詳細な説明の記載を参酌した上で、請求の範囲の各請求項によって示され、そこに記載された文言と均等の意味および範囲内での全ての変更を含む。

符号の説明

- [0111] 1 0 0 通信システム
- 1 0 2 車載システム
- 1 0 4、1 0 4 A、1 0 4 B 車両
- 1 0 6 路側機
- 1 0 8 基地局
- 1 1 0 ネットワーク
- 1 1 2 サーバ
- 1 2 0 車外通信部
- 1 2 2、1 2 2 A 車載装置
- 1 2 4、1 5 4 センサ
- 1 2 6 自動運転 E C U
- 1 2 8 認証 E C U
- 1 3 0 駆動 E C U
- 1 3 2、1 5 8、1 6 6 バス
- 1 3 4 駆動部
- 1 4 0、1 5 2、1 6 0 制御部
- 1 4 2、1 5 6、1 6 2 メモリ
- 1 5 0、1 6 4 通信部
- 2 0 0 路側情報取得部
- 2 0 2 路車情報生成部
- 2 0 4 車外通信パラメータ判定情報決定部
- 2 0 6 セキュリティルール生成部
- 2 0 8 セキュリティ部
- 2 2 0 クラウドサービス領域
- 2 2 2 エッジサービス領域
- 2 3 0 セキュリティルールテーブル更新部
- 3 0 0、3 0 2、3 0 4、3 0 6、3 0 8、3 1 0、3 1 2、3 1 4、4 0 0、4 0 2、4 0 4、4 0 6、4 0 8、4 1 0 ステップ

請求の範囲

- [請求項1] 車両に搭載される車載装置であって、
- 前記車両の車両情報および前記車両の外部に関する路側情報を含む路車情報に基づいて生成されたセキュリティルールに従って、前記車両の外部にある外部装置と通信する通信部に、前記外部装置との通信を制限させ、
- 前記車両情報は、前記車両において稼働しているアプリケーションを特定するアプリケーション稼働情報および前記外部装置との通信接続状態を表す接続情報の少なくともいずれか1つを含む、車載装置。
- [請求項2] 前記セキュリティルールを前記外部装置から受信する、請求項1に記載の車載装置。
- [請求項3] 前記外部装置から、前記路側情報を取得する路側情報取得部と、
- 前記路側情報に前記車両情報を加えて前記路車情報を生成する路車情報生成部と、
- 前記路車情報に基づいて車外通信パラメータ判定情報を決定する決定部と、
- 前記車外通信パラメータ判定情報に基づいて前記セキュリティルールを生成するセキュリティルール生成部とをさらに含む、請求項1に記載の車載装置。
- [請求項4] 前記路車情報は、前記アプリケーション稼働情報および前記接続情報の少なくともいずれか1つに加えて、位置情報および地図情報の少なくとも1つを含む、請求項3に記載の車載装置。
- [請求項5] 前記車外通信パラメータ判定情報は、前記アプリケーション稼働情報および前記接続情報の少なくとも1つを含む、請求項3または請求項4に記載の車載装置。
- [請求項6] 前記車外通信パラメータ判定情報は、少なくとも前記アプリケーション稼働情報を含み、
- 前記セキュリティルール生成部は、

前記アプリケーション稼働情報により稼働しているアプリケーションがないことを特定した場合、第1通信フィルタしきい値を含む前記セキュリティルールを生成し、

前記アプリケーション稼働情報により前記車両のドア開閉を制御するアプリケーションを特定した場合、前記第1通信フィルタしきい値よりも大きい第2通信フィルタしきい値を含む前記セキュリティルールを生成する、請求項5に記載の車載装置。

[請求項7] 前記車外通信パラメータ判定情報は、少なくとも前記アプリケーション稼働情報を含み、

前記セキュリティルール生成部は、

前記アプリケーション稼働情報により稼働しているアプリケーションがないことを特定した場合、アクセス許可を含まない前記セキュリティルールを生成し、

前記アプリケーション稼働情報により運転支援アプリケーションが稼働していることを特定した場合、前記運転支援アプリケーションにサービスを提供する外部装置へのアクセス許可を含む前記セキュリティルールを生成する、請求項5または請求項6に記載の車載装置。

[請求項8] 前記車外通信パラメータ判定情報は、少なくとも前記接続情報を含み、

前記セキュリティルール生成部は、

前記路車情報から特定される前記車両の位置が、複数の交差点を含む第1領域内にある場合に、前記第1領域に対応する前記接続情報により特定される第3通信フィルタしきい値を含む前記セキュリティルールを生成し、

前記路車情報から特定される前記車両の位置が、前記第1領域よりも狭く、1つの交差点を含む第2領域内にある場合に前記第2領域に対応する前記接続情報により特定される第4通信フィルタしきい値を含む前記セキュリティルールを生成し、

前記第4通信フィルタしきい値は、前記第3通信フィルタしきい値よりも大きい、請求項5から請求項7のいずれか1項に記載の車載装置。

[請求項9] 前記車外通信パラメータ判定情報は、前記アプリケーション稼働情報を含み、

前記セキュリティルール生成部は、前記車外通信パラメータ判定情報により、前記車両において複数のアプリケーションが稼働していることを特定した場合、

稼働している前記複数のアプリケーションの各々に関するセキュリティルールテーブルを生成し、

複数の前記セキュリティルールテーブルを統合して前記セキュリティルールを生成する、請求項5に記載の車載装置。

[請求項10] 前記決定部は、前記路車情報が前記接続情報を含んでいなければ、当該路車情報から、前記車外通信パラメータ判定情報として接続情報を生成する、請求項4から請求項9のいずれか1項に記載の車載装置。

[請求項11] 前記セキュリティルールは、前記通信部による通信に関するアクセス頻度、通信速度、セッション数、SYNパケット数、通信先の通信アドレス、および、通信先のポート番号の少なくとも1つに関する制限を含む、請求項1から請求項10のいずれか1項に記載の車載装置。

[請求項12] 前記セキュリティルールを更新する更新部をさらに含み、
前記更新部は、前記通信部により、前記車両において稼働させる新たなアプリケーション、または、前記車両において稼働しているアプリケーションの更新アプリケーションが受信されたことを受けて、前記セキュリティルールを更新する、請求項1から請求項11のいずれか1項に記載の車載装置。

[請求項13] 前記新たなアプリケーションまたは前記更新アプリケーションに対

応する新たなセキュリティルールは、前記外部装置から受信され、

前記更新部は、前記新たなセキュリティルールを用いて、前記セキュリティルールを更新する、請求項 12 に記載の車載装置。

[請求項14]

車両に搭載される車載装置に、前記車載装置による前記車両の外部との通信を制限するセキュリティルールを、前記車両の車両情報および前記車両の外部に関する路側情報を含む路車情報に基づいて生成する生成部と、

前記車載装置に、前記セキュリティルールを送信する通信部とを含み、

前記車両情報は、前記車両において稼働しているアプリケーションを特定するアプリケーション稼働情報および前記外部装置との通信接続状態を表す接続情報の少なくともいずれか1つを含む、サーバコンピュータ。

[請求項15]

前記通信部は、前記車載装置から前記車両情報を受信し、

前記路側情報に、前記通信部により受信された前記車両情報を加えて前記路車情報を生成する路車情報生成部と、

前記路車情報に基づいて車外通信パラメータ判定情報を決定する決定部とさらに含み、

前記生成部は、前記車外通信パラメータ判定情報に基づいて前記セキュリティルールを生成する、請求項 14 に記載のサーバコンピュータ。

[請求項16]

請求項 1 から請求項 13 のいずれか1項に記載の車載装置と、

請求項 14 に記載のサーバコンピュータとを含み、

前記車載装置は、前記車両に搭載された前記通信部に、前記サーバコンピュータを前記外部装置として通信させる、通信システム。

[請求項17]

請求項 1 または請求項 2 に記載の車載装置と、

請求項 15 に記載のサーバコンピュータとを含み、

前記車載装置は、前記車両に搭載された前記通信部に、前記サーバ

コンピュータを前記外部装置として通信させる、通信システム。

[請求項18]

車両に搭載される車載システムの制御方法であって、

前記車載システムに含まれる車載装置が、前記車両の車両情報および前記車両の外部に関する路側情報を含む路車情報に基づいて生成されたセキュリティルールに従って、車両の外部にある外部装置と通信する通信部に、前記外部装置との通信を制限させるステップを含み、

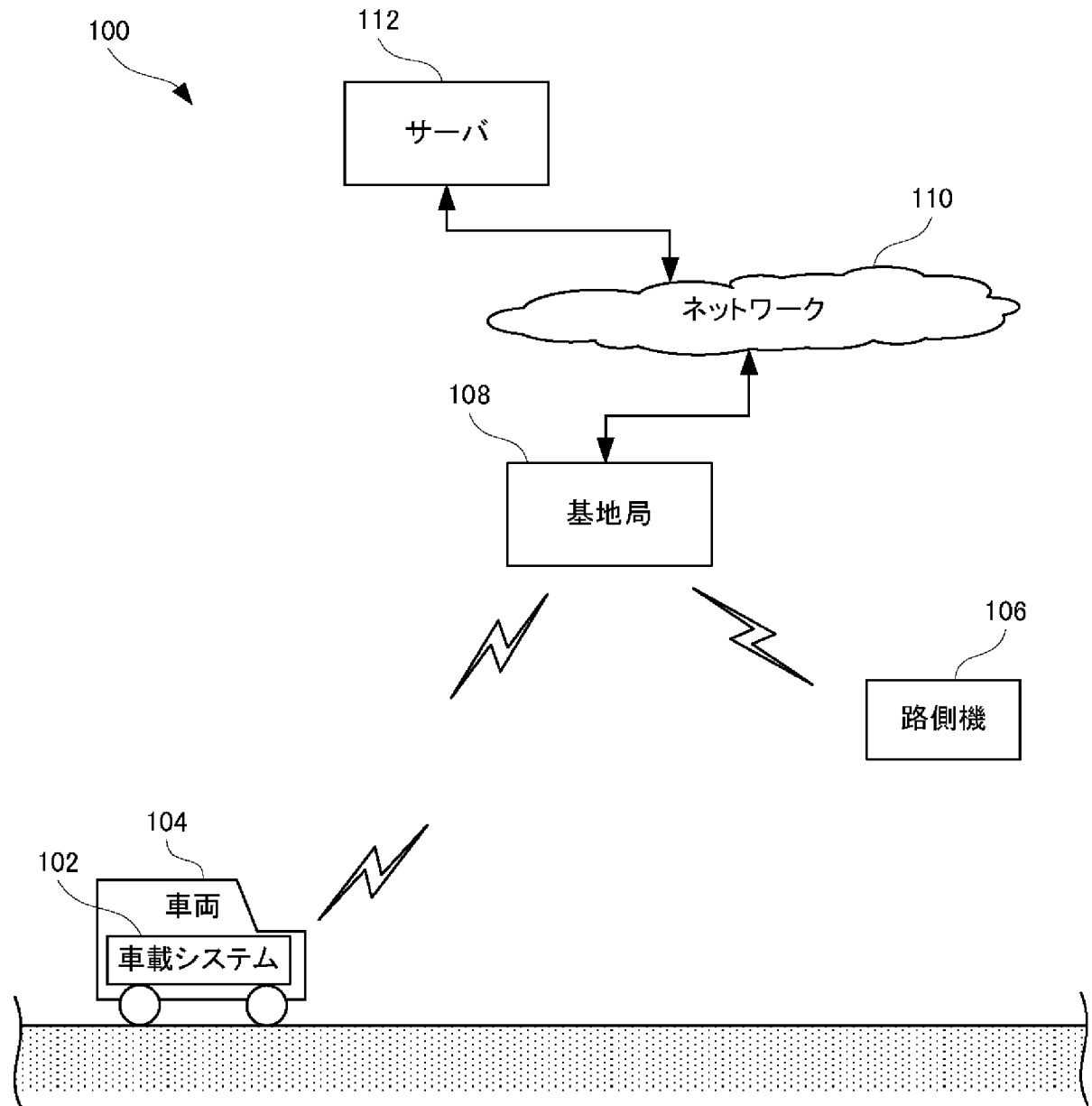
前記車両情報は、前記車両において稼働しているアプリケーションを特定するアプリケーション稼働情報および前記外部装置との通信接続状態を表す接続情報の少なくともいずれか1つを含む、制御方法。

[請求項19]

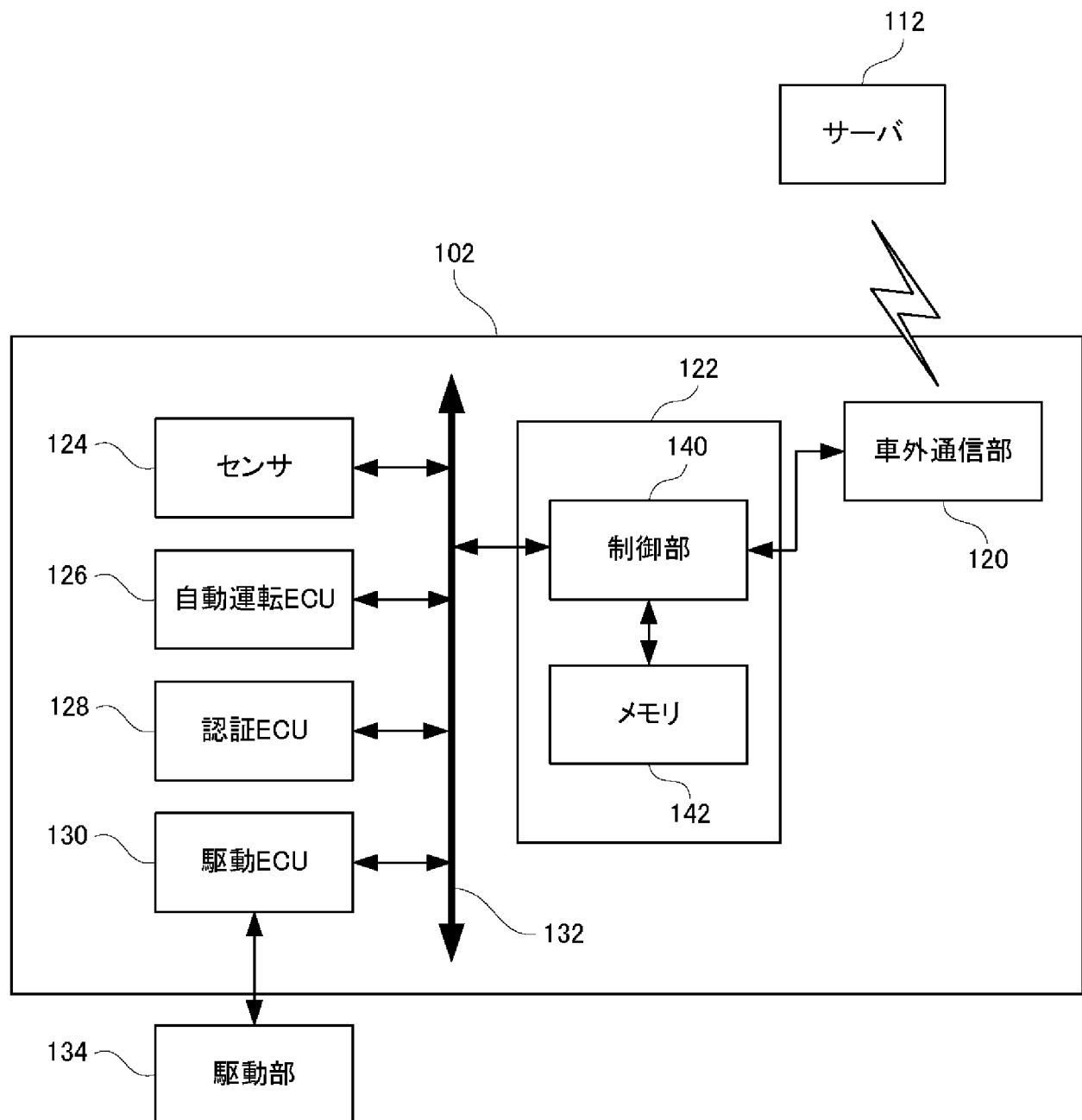
車両に搭載されるコンピュータに、前記車両の車両情報および車両の外部に関する路側情報を含む路車情報に基づいて生成されたセキュリティルールに従って、前記車両の外部にある外部装置と通信する通信部に、前記外部装置との通信を制限させる機能を実現させ、

前記車両情報は、前記車両において稼働しているアプリケーションを特定するアプリケーション稼働情報および前記外部装置との通信接続状態を表す接続情報の少なくともいずれか1つを含む、コンピュータプログラム。

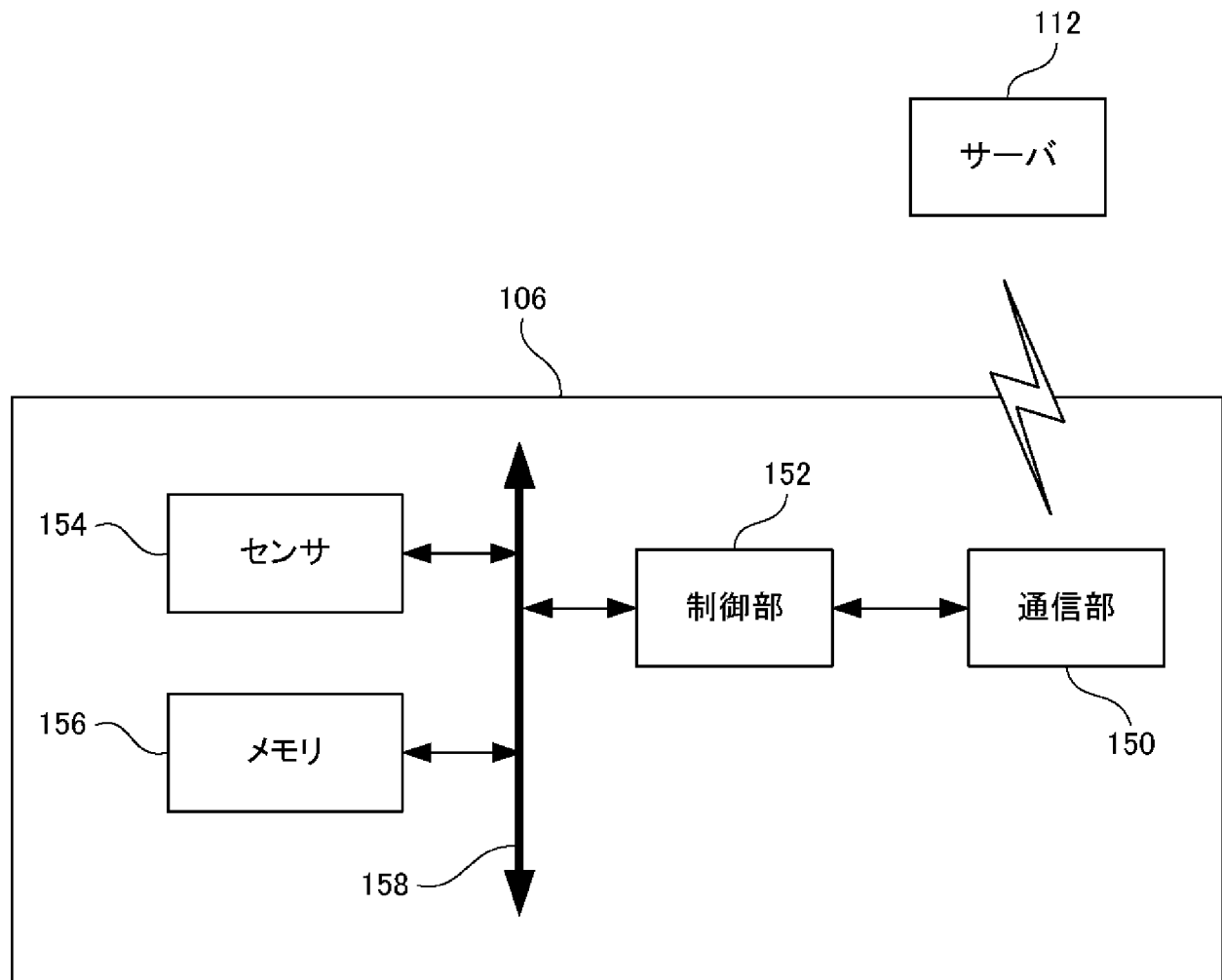
[図1]



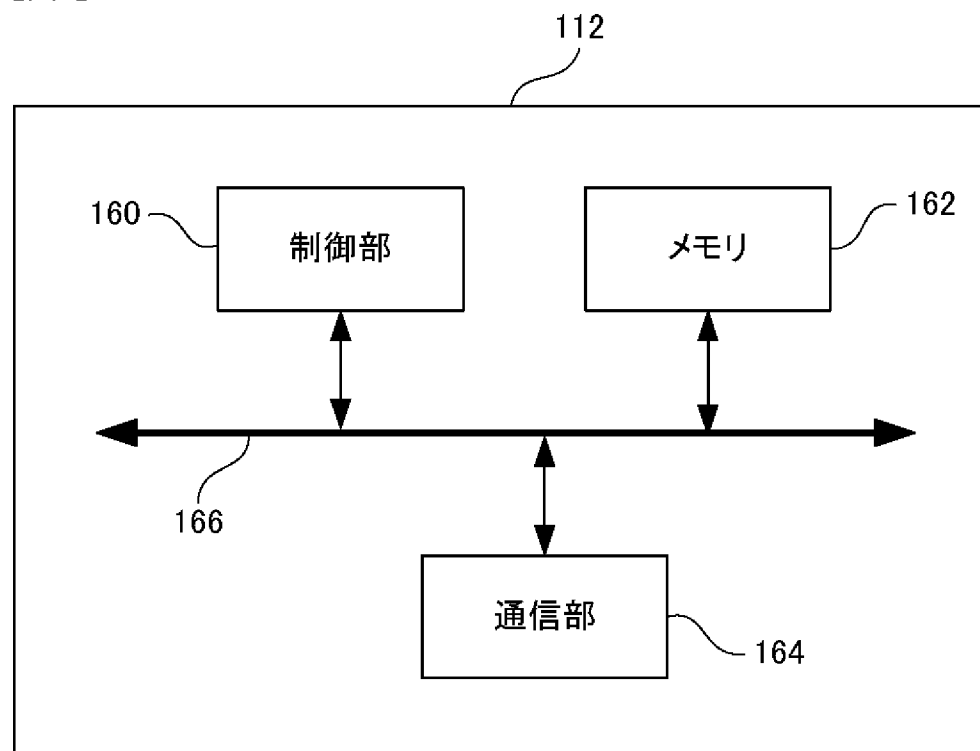
[図2]



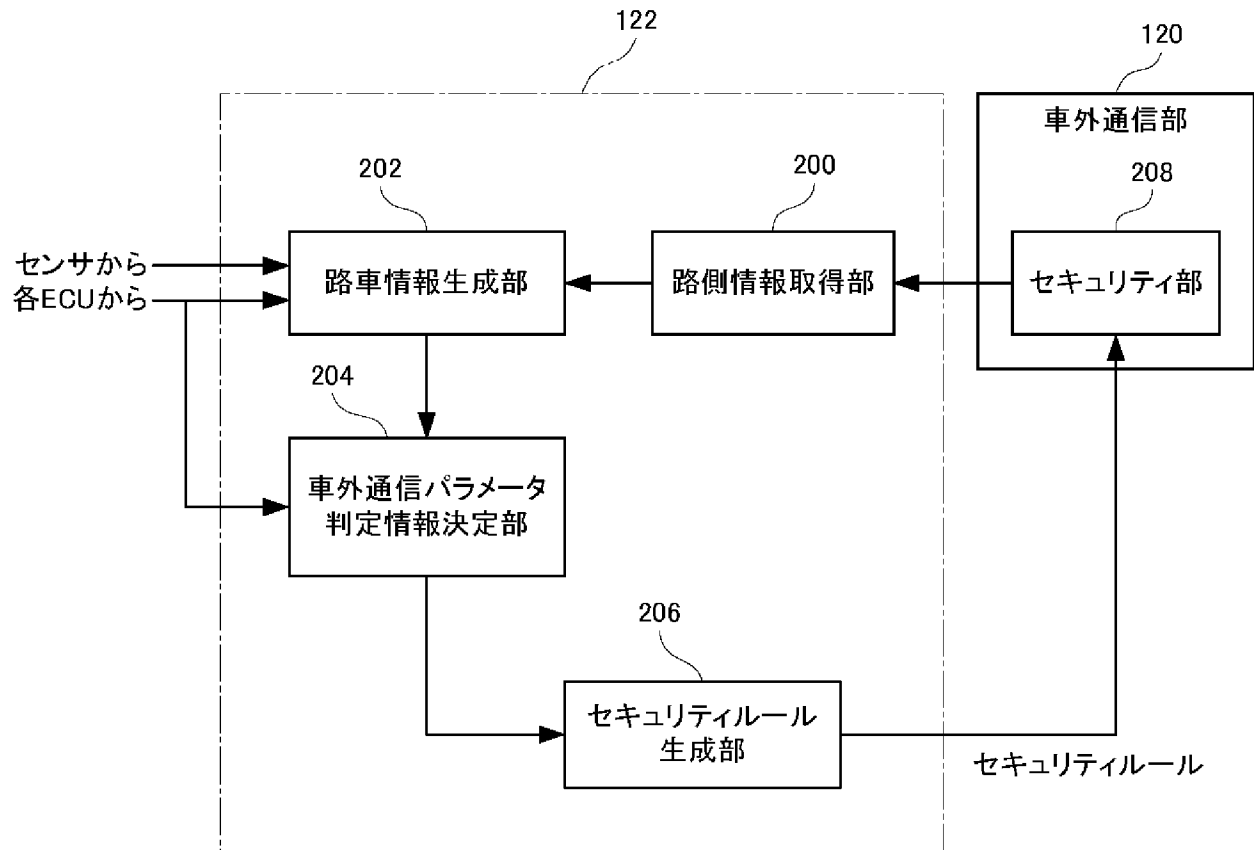
[図3]



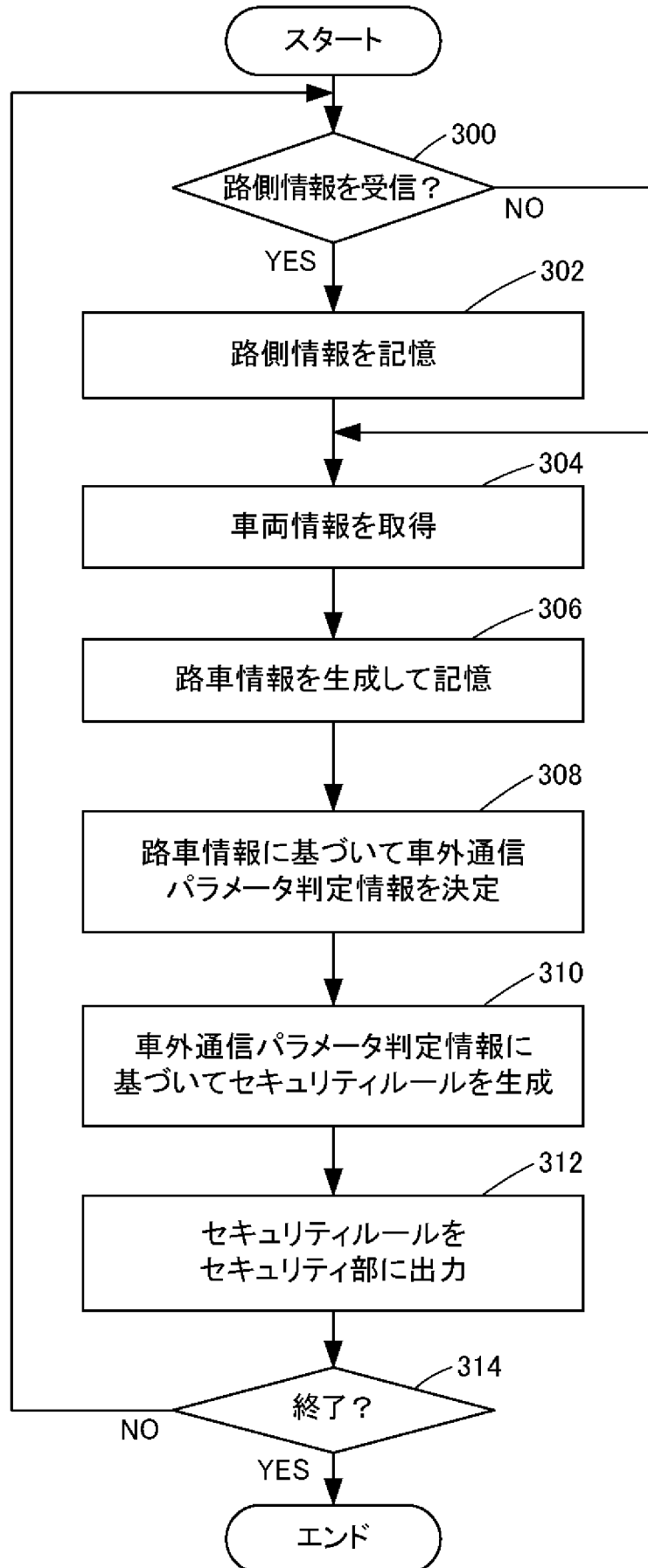
[図4]



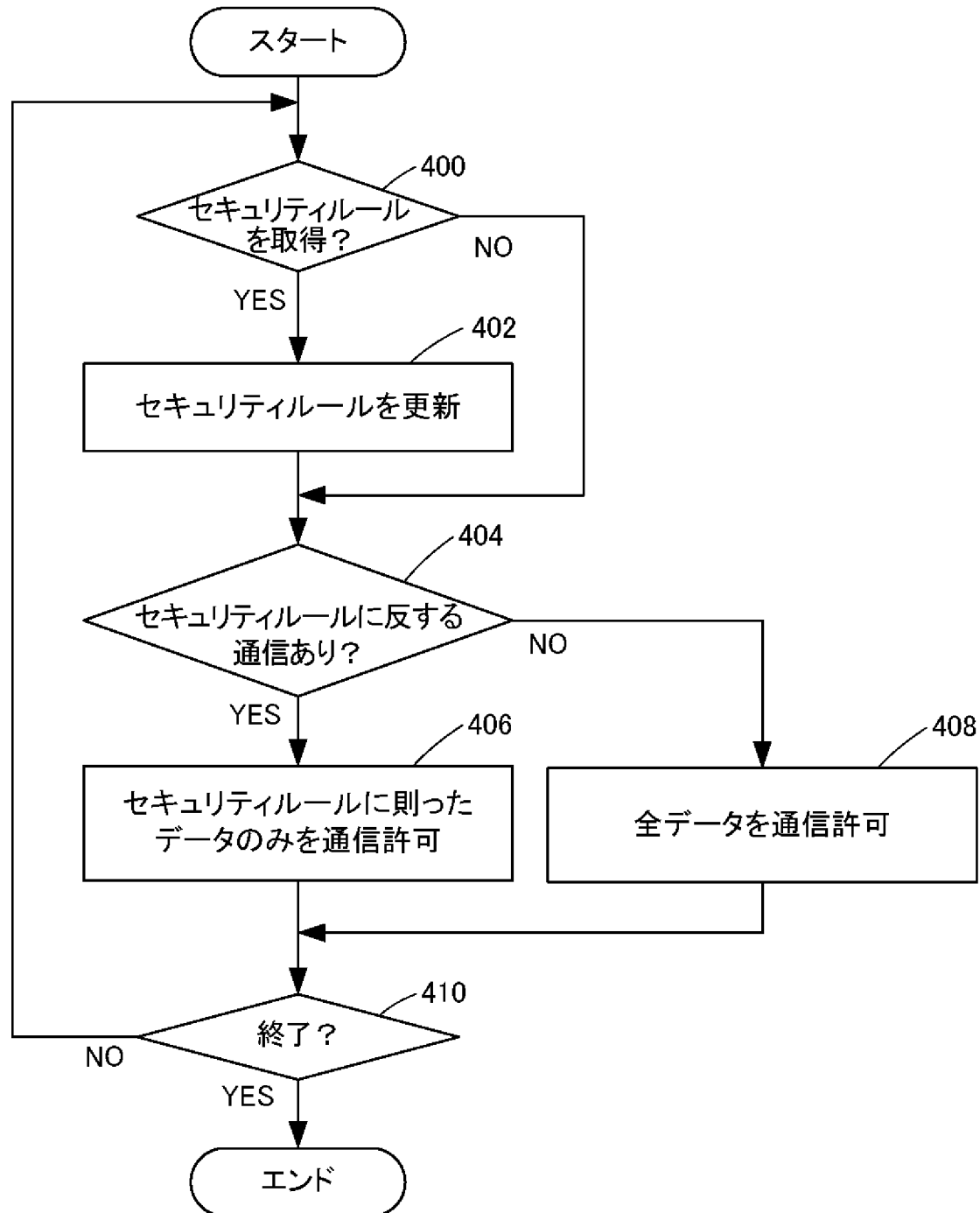
[図5]



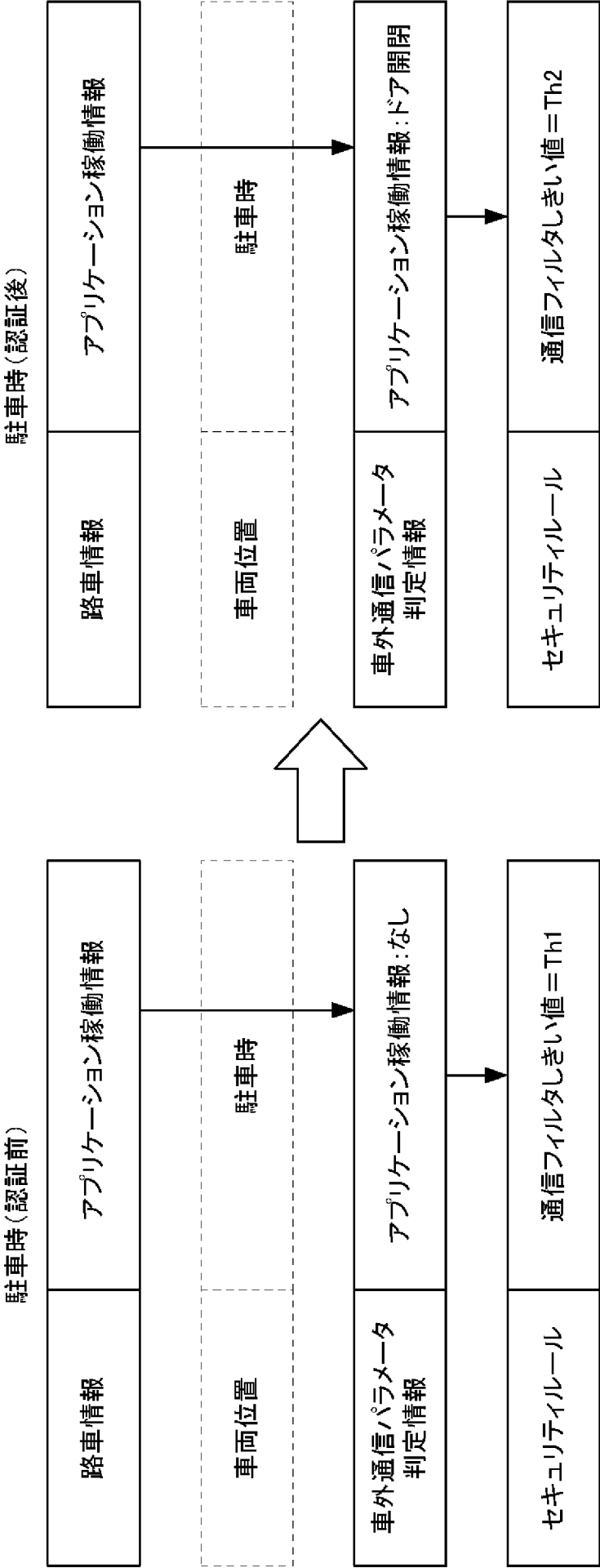
[図6]



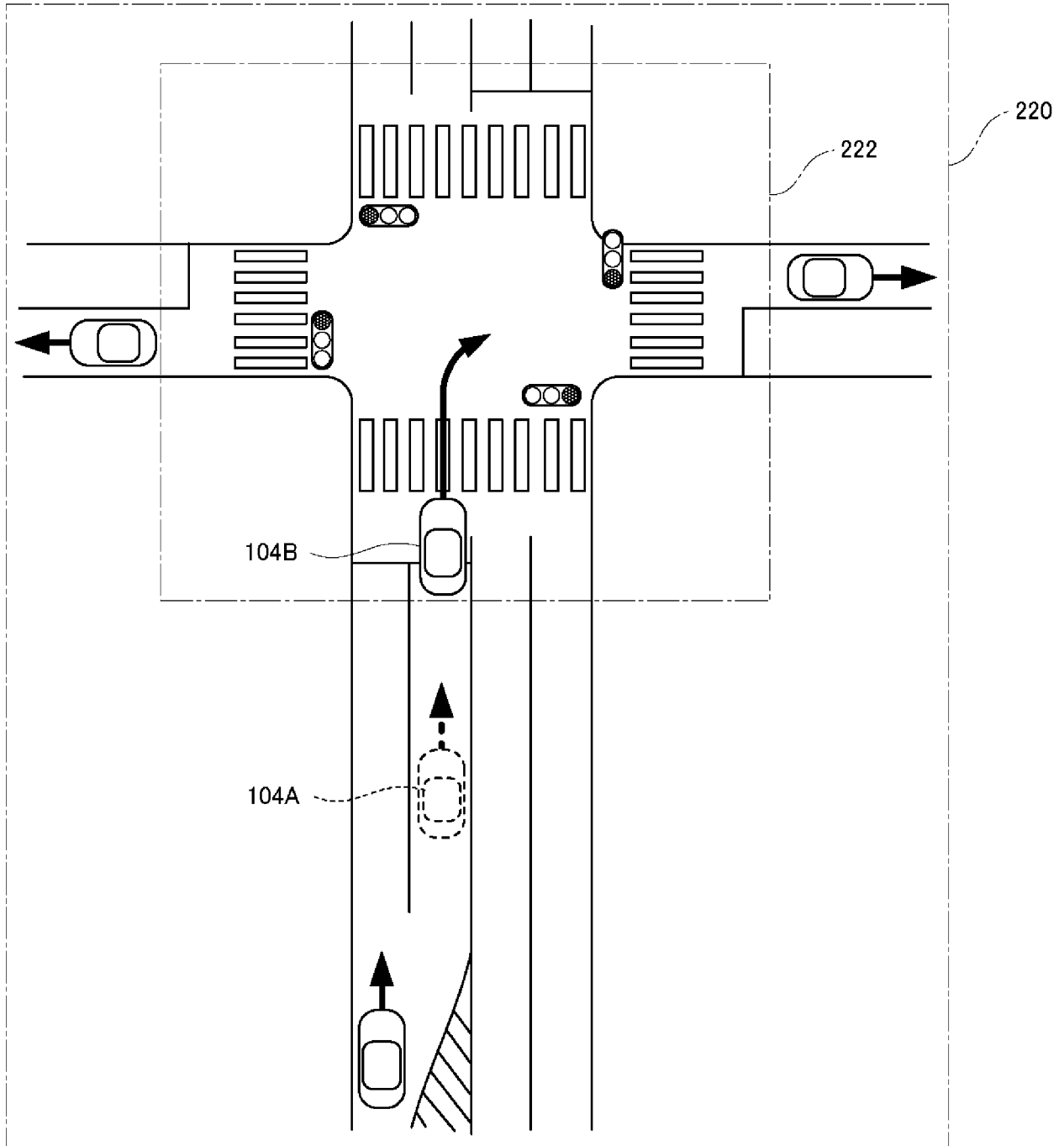
[図7]



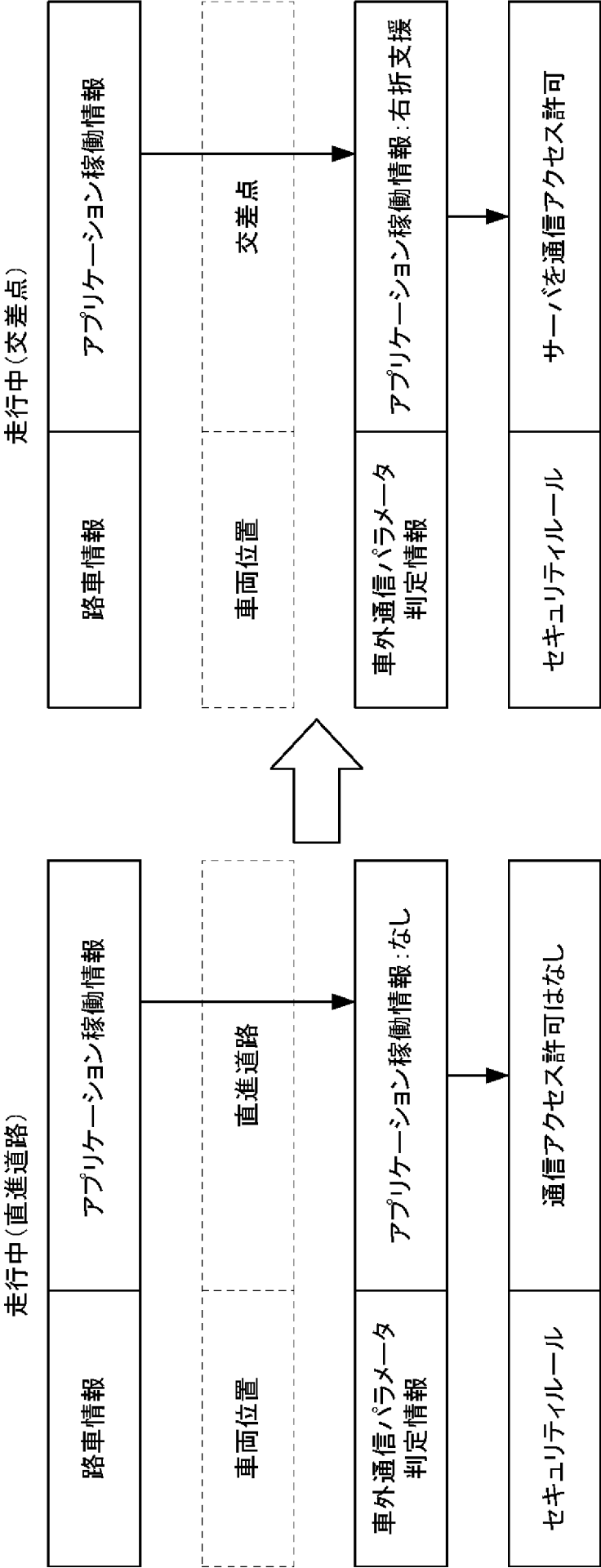
[図8]



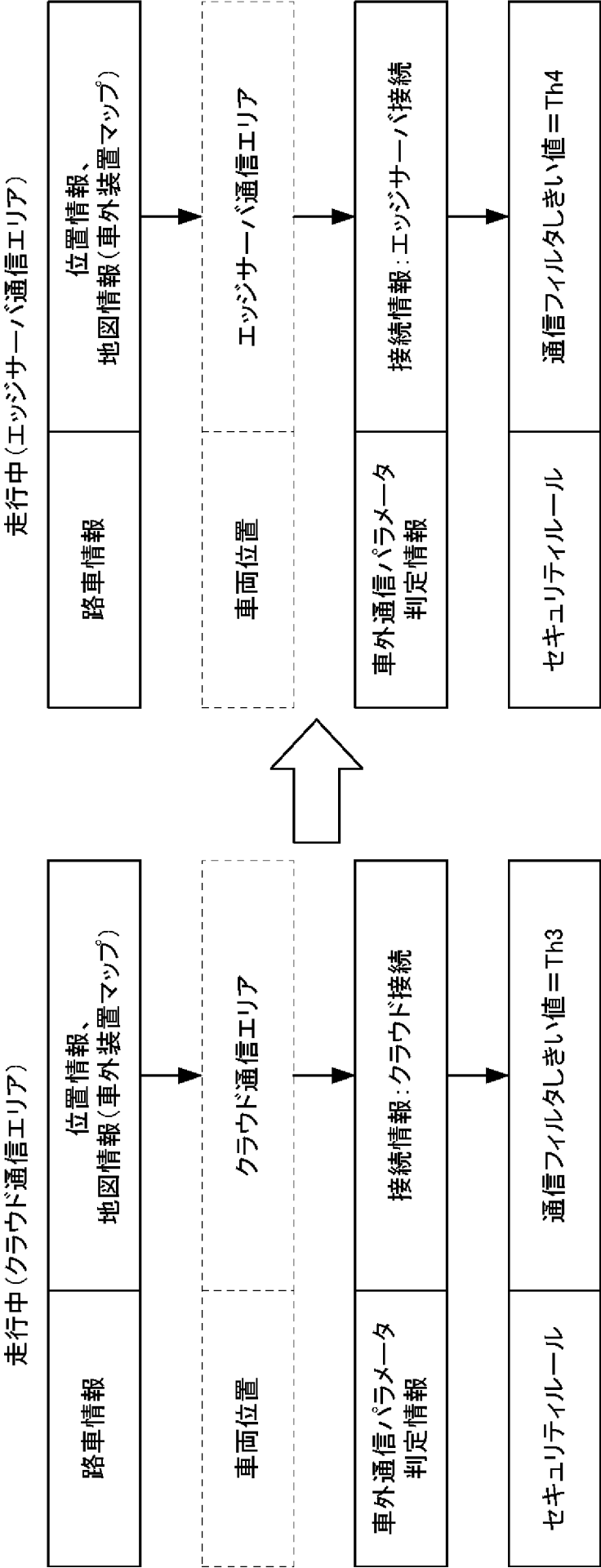
[図9]



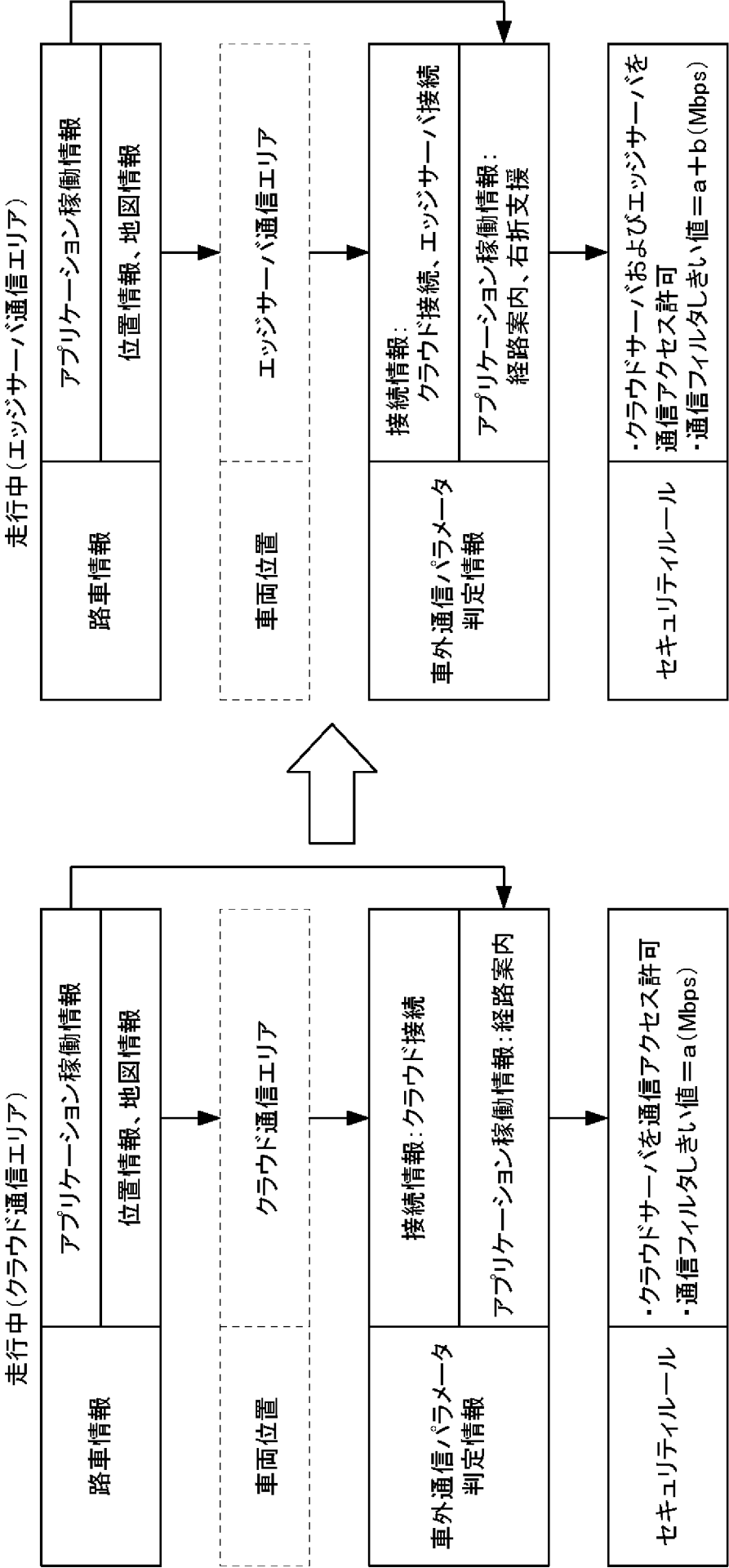
[図10]



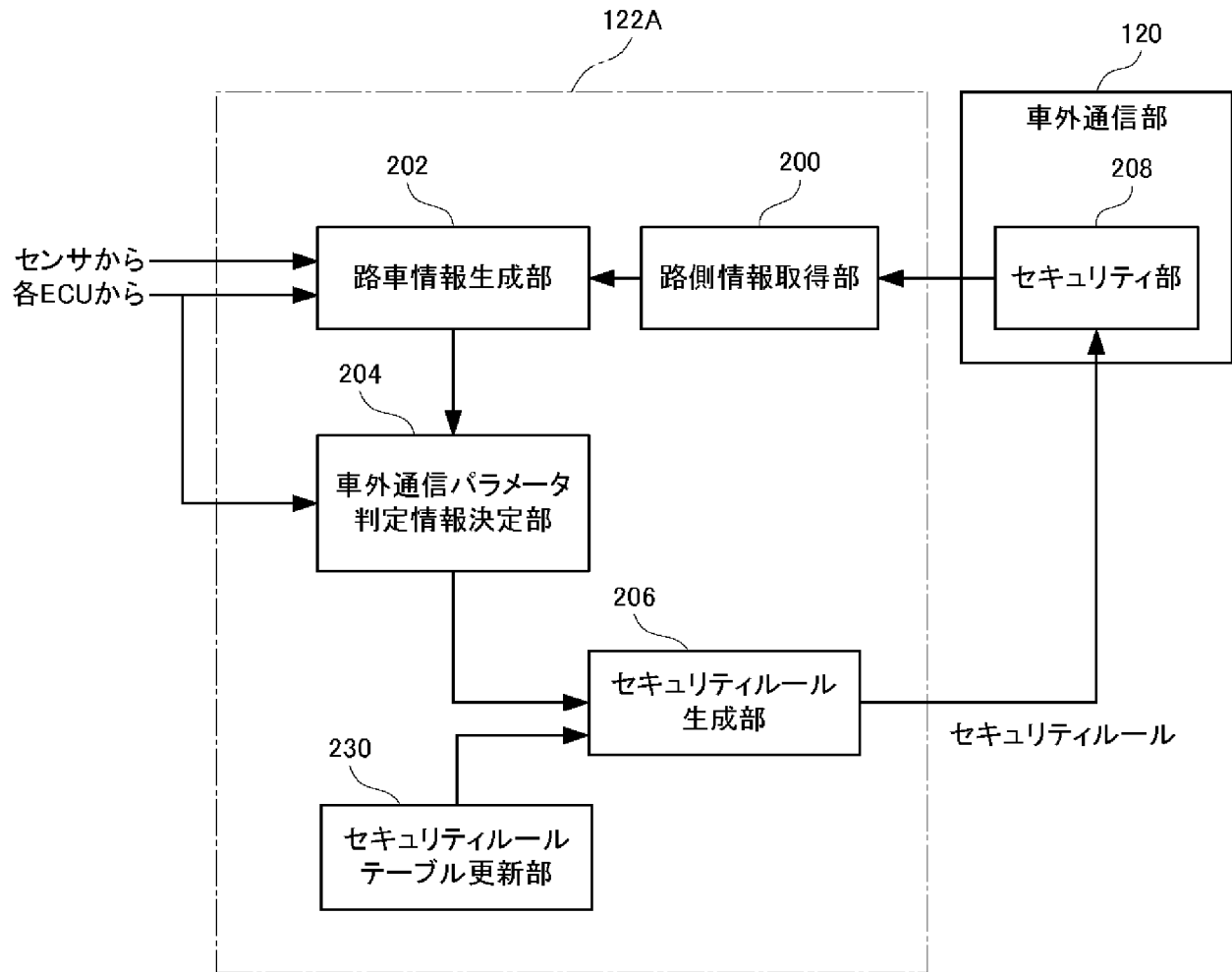
[図11]



[図12]



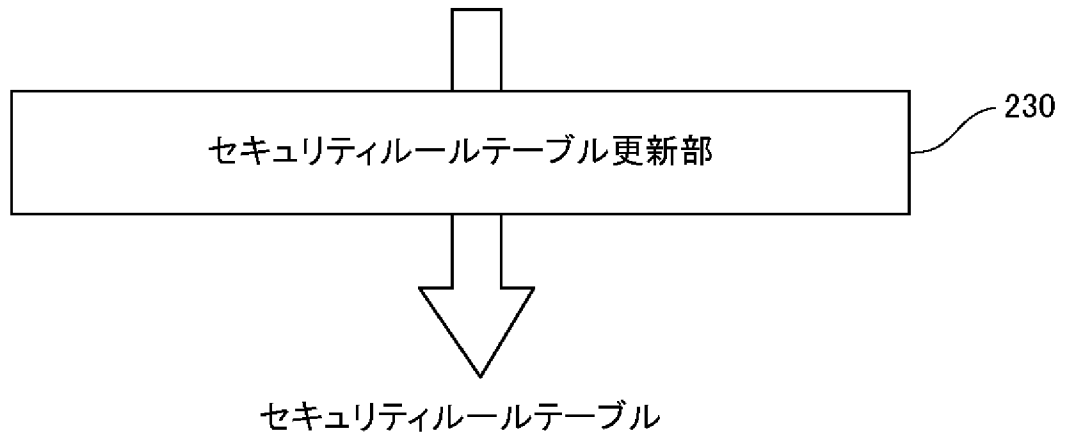
[図13]



[図14]

アプリケーション仕様情報

アプリケーション名	右折支援
通信先	車外サーバ(IPアドレス、ポート番号)
通信内容	交差点を含む所定エリアにおける物体情報
通信量	1物体につきa(bit)、最大b物体まで、 更新周期はc(ms)



アプリケーション名	右折支援
通信アクセス許可	車外サーバ(IPアドレス、ポート番号)
通信フィルタしきい値	$a \times b / c$ (kbps)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2023/003740

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 2022-45225 A (SOFTBANK CORP.) 18 March 2022 (2022-03-18) paragraphs [0014]-[0164], fig. 1-12	1-5, 10-11, 14-19
Y		9, 12-13
A		6-8
Y	WO 2021/145144 A1 (PANASONIC INTELLECTUAL PROPERTY CORPORATION OF AMERICA) 22 July 2021 (2021-07-22) paragraphs [0064]-[0069], fig. 3	9, 12-13
A	JP 2021-82064 A (AUTO NETWORK GIJUTSU KENKYUSHO KK) 27 May 2021 (2021-05-27) entire text, all drawings	1-19
A	JP 2020-17009 A (YANMAR CO., LTD.) 30 January 2020 (2020-01-30) entire text, all drawings	1-19
A	JP 2017-46080 A (MITSUBISHI ELECTRIC CORPORATION) 02 March 2017 (2017-03-02) entire text, all drawings	1-19



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

14 April 2023

Date of mailing of the international search report

25 April 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

International application No.

PCT/JP2023/003740

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2007-65893 A (MITSUBISHI ELECTRIC CORPORATION) 15 March 2007 (2007-03-15) entire text, all drawings	1-19

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2023/003740

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP	2022-45225	A	18 March 2022	WO 2022/054650 A1 paragraphs [0014]-[0164], fig. 1-12	
WO	2021/145144	A1	22 July 2021	US 2022/0182404 A1 paragraphs [0086]-[0091], fig. 3	
				EP 4092553 A1	
				CN 113924750 A	
JP	2021-82064	A	27 May 2021	US 2022/0396218 A1 entire text, all drawings	
				WO 2021/100451 A1	
				CN 114667241 A	
JP	2020-17009	A	30 January 2020	US 2021/0165858 A1 entire text, all drawings	
				WO 2020/021828 A1	
				EP 3828738 A1	
				CN 112470151 A	
				KR 10-2021-0037613 A	
JP	2017-46080	A	02 March 2017	(Family: none)	
JP	2007-65893	A	15 March 2007	US 2008/0140381 A1 entire text, all drawings	
				WO 2006/114925 A1	
				CN 101146697 A	

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 Y A	JP 2022-45225 A（ソフトバンク株式会社）18.03.2022（2022-03-18） 段落 [0014] - [0164]、[図1] - [図12]	1-5, 10-11, 14-19 9, 12-13 6-8
Y	WO 2021/145144 A1（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）22.07.2021（2021-07-22） 段落 [0064] - [0069]、[図3]	9, 12-13
A	JP 2021-82064 A（株式会社オートネットワーク技術研究所）27.05.2021（2021- 05-27） 全文、全図	1-19
A	JP 2020-17009 A（ヤンマー株式会社）30.01.2020（2020-01-30） 全文、全図	1-19
A	JP 2017-46080 A（三菱電機株式会社）02.03.2017（2017-03-02） 全文、全図	1-19
☒ 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、一般的な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 14.04.2023		国際調査報告の発送日 25.04.2023
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） 松平 英 5S 3146 電話番号 03-3581-1101 内線 3546

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
A	JP 2007-65893 A (三菱電機株式会社) 15.03.2007 (2007 - 03 - 15) 全文、全図	1-19

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/JP2023/003740

引用文献			公表日	パテントファミリー文献			公表日
JP	2022-45225	A	18.03.2022	WO	2022/054650	A1	
				段落 [0014] - [0164]、[図1] - [図12]			
WO	2021/145144	A1	22.07.2021	US	2022/0182404	A1	
				段落 [0086] - [0091]、FIG. 3			
				EP	4092553	A1	
				CN	113924750	A	
JP	2021-82064	A	27.05.2021	US	2022/0396218	A1	
				全文、全図			
				WO	2021/100451	A1	
				CN	114667241	A	
JP	2020-17009	A	30.01.2020	US	2021/0165858	A1	
				全文、全図			
				WO	2020/021828	A1	
				EP	3828738	A1	
				CN	112470151	A	
				KR	10-2021-0037613	A	
JP	2017-46080	A	02.03.2017	(ファミリーなし)			
JP	2007-65893	A	15.03.2007	US	2008/0140381	A1	
				全文、全図			
				WO	2006/114925	A1	
				CN	101146697	A	