(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
2021年1月7日(07.01.2021)

WIPO | PCT

(10) 国際公開番号
WO 2021/002013 A1

(51) 国際特許分類:
G06F 21/31 (2013.01) *G06F 21/62* (2013.01)

(21) 国際出願番号： PCT/JP2019/026722

(22) 国際出願日： 2019年7月4日(04.07.2019)

(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: パナソニック インテレクチュアル プロパティ コーポレーション オブ アメリカ(**PANASONIC INTELLECTUAL PROPERTY CORPORATION OF AMERICA**) [US/US]; 90503 カリフォルニア州トーランス, スイート ２００, マリナー アベニュー ２００００ California (US).

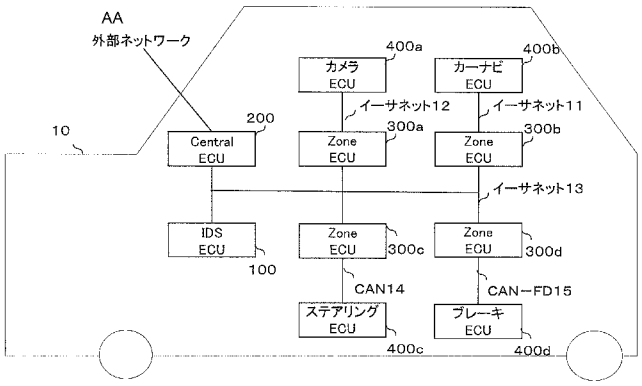
(72) 発明者: 平野 亮(**HIRANO, Ryo**); 〒5718501 大阪府門真市大字門真１００６番地 パナソニック株式会社内 Osaka (JP). 岸川 剛(**KISHIKAWA, Takeshi**). 氏家 良浩(**UJIIE, Yoshihiro**). 芳賀 智之(**HAGA, Tomoyuki**).

(74) 代理人: 新居 広守, 外 (**NII, Hiromori** et al.); 〒5320011 大阪府大阪市淀川区西中島５丁目３番１０号タナカ・イトーピア新大阪ビル６階新居国際特許事務所内 Osaka (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH,

(54) **Title:** ABNORMALITY DETECTION DEVICE, AND ABNORMALITY DETECTION METHOD

(54) 発明の名称： 異常検知装置および異常検知方法



11, 12, 13	Ethernet
200	Central ECU
300a, 300b, 300c, 300d	Zone ECU
400a	Camera ECU
400b	Car navigation ECU
400c	Steering ECU
400d	Brake ECU
AA	External network

(57) **Abstract:** Because vehicles are electronically controlled, there is a threat of being fraudulently operated by the imitation of a control command. Because a similar threat exists for service-oriented communications, detection devices that detect an abnormality in a communication encryption device, a transmission source or a transmission destination have been proposed. However, there is a problem that it is not easy to maintain the safety of service-oriented communications while maintaining software portability, which is an advantage of using service-oriented communications. Provided is an abnormality detection device, and by using the same in an in-vehicle network, SOME/IP-SD communication frames are monitored and detection rules are dynamically generated, thereby eliminating the need to set, in advance, a transmission destination IP address and a transmission source IP address. By adopting a method that uses the dynamically generated detection rules to monitor the SOME/IP communication frames and to detect an abnormal frame, it is possible to provide safe automatic driving and an advanced driving assistance system without losing the portability of service-oriented communications.

WO 2021/002013 A1

［続葉有］

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)）

(57) 要約：自動車は、電子制御化されており、制御コマンドをなりすますことにより不正に操作される脅威がある。サービス指向型通信においても同様の脅威があるため、通信の暗号化装置や送信元や送信先の異常を検出する検知装置が提案されている。しかしながら、サービス指向型通信を利用する利点であるソフトウェアの可搬性を維持したまま、サービス指向型通信の安全性を維持することは容易ではない課題がある。車載ネットワークにおける異常検知装置によれば、ＳＯＭＥ／ＩＰ－ＳＤの通信フレームを監視して検知ルールを動的に生成することで、送信先ＩＰアドレスと送信元ＩＰアドレスの事前設定を不要とし、動的生成した検知ルールを用いてＳＯＭＥ／ＩＰの通信フレームを監視して異常なフレームとして検知する方法を取ることで、サービス指向型通信の可搬性を失わずに、安全な自動運転や先進運転支援システムを提供することができる。

明　細　書

発明の名称 ： 異常検知装置および異常検知方法

技術分野

[0001] 本開示は、車載ネットワークシステムにおいて、異常な通信を検知する装置および方法に関する。

背景技術

[0002] 近年、自動車の中のシステムには、電子制御装置（ＥＣＵ：Ｅｌｅｃｔｒｏｎｉｃ　Ｃｏｎｔｒｏｌ　Ｕｎｉｔ）と呼ばれる装置が多数配置されている。これらのＥＣＵをつなぐネットワークは車載ネットワークと呼ばれる。車載ネットワークには、多数の規格が存在する。車載ネットワークの１つに、ＩＥＥＥ　８０２．３で規定されているＥｔｈｅｒｎｅｔ（登録商標）という規格が存在する。先進運転支援システムや自動運転においては、カメラやＬＩＤＡＲ（Ｌｉｇｈｔ　Ｄｅｔｅｃｔｉｏｎ　ａｎｄ　Ｒａｎｇｉｎｇ）などのセンサーやダイナミックマップなど膨大な情報を処理する必要があるため、データ伝送速度が高いＥｔｈｅｒｎｅｔの導入が進んでいる。そして、Ｅｔｈｅｒｎｅｔ上の通信プロトコルとして、ＳＯＭＥ／ＩＰ（Ｓｃａｌａｂｌｅ　Ｓｅｒｖｉｃｅ－Ｏｒｉｅｎｔｅｄ　ＭｉｄｄｌｅｗａｒＥ　ｏｖｅｒ　ＩＰ）という規格が存在する。ＳＯＭＥ／ＩＰでは、Ｅｔｈｅｒｎｅｔに接続される各ノードがヘッダに記載されるサービスＩＤによって通信内容を決定するため、サービス指向型通信と呼ばれる。さらに、ＳＯＭＥ／ＩＰでは、ＳＯＭＥ／ＩＰ－ＳＤ（Ｓｅｒｖｉｃｅ　Ｄｉｓｃｏｖｅｒｙ）と呼ばれるＳＯＭＥ／ＩＰ通信を開始する前に行われるノード間の通信確立フェーズが存在し、事前に利用したいサービスのサービスＩＤまたは提供可能なサービスのサービスＩＤを記憶していれば、通信先ノードのＩＰアドレスやＭＡＣアドレスを動的に取得できる。そのため、システム環境に依存するＩＰアドレスやＭＡＣアドレスなどの情報を事前に設定する必要はなく、可搬性に優れたソフトウェアを容易に設計することが可能であることから

次世代の通信方式として利用の拡大が期待されている。

先行技術文献

非特許文献

[0003] 非特許文献1：“ＳＯＭＥ／ＩＰ，Ｐｕｂｌｉｃａｔｉｏｎｓ，Ｓｐｅｃｉｆｉｃａｔｉｏｎｓ／Ｓｔａｎｄａｒｄｓ”、［ｏｎｌｉｎｅ］、［令和１年０６月１８日検索］、インターネット＜ＵＲＬ：ｈｔｔｐ：／／ｓｏｍｅ－ｉｐ．ｃｏｍ／ｐａｐｅｒｓ．ｓｈｔｍｌ／＞

非特許文献2：Ｎ．Ｈｅｒｏｌｄ，ｅｔ ａｌ、“Ａｎｏｍａｌｙ Ｄｅｔｅｃｔｉｏｎ ｆｏｒ ＳＯＭＥ／ＩＰｕｓｉｎｇ Ｃｏｍｐｌｅｘ Ｅｖｅｎｔ Ｐｒｏｃｅｓｓｉｎｇ”、ＮＯＭＳ ２０１６，ＩＥＥＥ／ＩＦＩＰ Ｎｅｔｗｏｒｋ Ｏｐｅｒａｔｉｏｎｓ ａｎｄ Ｍａｎａｇｅｍｅｎｔ Ｓｙｍｐｏｓｉｕｍ、２０１６

発明の概要

発明が解決しようとする課題

[0004] ＳＯＭＥ／ＩＰ等のサービス指向型通信において、セキュリティ対策が何も施されていない場合、一つのノードが不正に乗っ取られると、乗っ取られたノードが送信するサービスＩＤの通信を不正に送受信できるだけでなく、乗っ取られたノード以外の他のノードが送信するはずのサービスＩＤを含む通信を送信することで、他のノードになりすまして、不正な通信を成立させることや、通信を停止させることができる脅威がある。

[0005] 特に、車載ネットワークにおいては車両の「走る、曲がる、止まる」に関わる特に重要なサービスが存在するため、これらのサービスを不正に制御することや、不正に停止することが可能であることは大きな脅威となる。

[0006] これらの脅威に対して、ＩＰＳｅｃ（Ｓｅｃｕｒｉｔｙ Ａｒｃｈｔｅｃｔｕｒｅ ｆｏｒ Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）等を用いてＳＯＭＥ／ＩＰ通信を暗号化する対策や、非特許文献２に開示されている対策がある。

[0007] ＩＰＳｅｃを用いる場合、ノード間で共有された鍵を用いて通信を暗号化することで、通信内容の盗聴を防ぐことができる。

[0008] しかし、鍵が車両内の各々のＥＣＵで共通であった場合、特定のＥＣＵが不正に乗っ取られると鍵も漏洩し、不正な通信が成立させることができる課題がある。

[0009] また、ＥＣＵごとに異なる鍵や公開鍵を用いる場合、鍵の管理が煩雑になることに加えて、通信の暗号化処理と復号処理のオーバヘッドが増加する課題がある。

[0010] セキュリティ対策のために、ＩＰＳｅｃを用いると、ＳＯＭＥ／ＩＰを利用する利点である可搬性が失われる。

[0011] 次に、非特許文献２に開示されている対策では、ＳＯＭＥ／ＩＰの通信フレームに対して、事前にサービスＩＤと対応する送信先ＩＰアドレス、送信元ＩＰアドレスを正常ルールとして事前に設定し、通信フレームを監視し、正常ルールに従わない通信フレームを異常なフレームとして検知する。

[0012] しかしながら、ＩＰアドレス等の情報は車種や車両ごとに異なるため、システム環境に依存する情報を事前に設定することは、ＳＯＭＥ／ＩＰを利用する利点である可搬性を低下させる課題がある。

[0013] 本開示は、従来の課題を解決するもので、ＳＯＭＥ／ＩＰ－ＳＤの通信フレームを監視して検知ルールを動的生成することで、送信先ＩＰアドレスと送信元ＩＰアドレスの事前設定を不要とし、動的生成した検知ルールを用いてＳＯＭＥ／ＩＰの通信フレームを監視して異常なフレームを検知する方法を取ることで、サービス指向型通信の可搬性を失わずに、安全な自動運転や先進運転支援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

[0014] 上記課題を解決するために、イーサネット（登録商標）で構成される車載ネットワークシステムにおける異常検知装置であって、サービス指向型通信の通信確立フェーズにおけるフレームを監視し、サービス指向型通信において通信内容を示す通信ＩＤごとに、送信先ＩＰアドレスと送信元ＩＰアドレ

スを含む検知ルールを生成する検知ルール生成部と、サービス指向型通信のフレームを監視し、送信先ＩＰアドレスまたは送信元ＩＰアドレスが異なるフレームを異常なフレームとして検出する異常検知部と、を備える異常検知装置である。

発明の効果

[0015] 本開示の車載ネットワークシステムにおける異常検知装置によれば、サービス指向型通信の利点であるソフトウェア可搬性を失わずに、異常な通信フレームを検知することができる。その結果、サービス指向型通信において、不正に乗っ取られたノードが正規の他ノードになりすまして、他ノードが送信するはずのサービスＩＤを含む通信を送信することで、不正な通信を成立させる場合や通信を停止させる場合に、その不正な通信フレームを異常フレームとして検知することが可能となるとともに、システム環境に依存するＩＰアドレスの設定が不要となるため、他車種および他車両へ展開する際のソフトウェア変更コストが低減され、自動車の安全性に貢献できる。

図面の簡単な説明

[0016] [図1]図１は、本開示の実施の形態１における車載ネットワークシステムの全体構成図である。

[図2]図２は、本開示の実施の形態１におけるＩＤＳＥＣＵの構成図である。

[図3]図３は、本開示の実施の形態１における車載ネットワークシステムにおけるヘッダフォーマットの一例を示した図である。

[図4]図４は、本開示の実施の形態１における事前設定検知ルールの一例を示した図である。

[図5]図５は、本開示の実施の形態１における動的設定検知ルールの一例を示した図である。

[図6]図６は、本開示の実施の形態１における検知ルール生成処理のシーケンスを示した図である。

[図7]図７は、本開示の実施の形態１における異常検知処理のシーケンスを示した図である。

[図8]図８は、本開示の実施の形態１における検知ルール生成処理のフローチャートを示した図である。

[図9]図９は、本開示の実施の形態１における異常検知処理のフローチャートである。

発明を実施するための形態

[0017] 上記課題を解決するために、本開示の一態様に係る異常検知装置は、イーサネットで構成される車載ネットワークシステムにおける異常検知装置であって、前記異常検知装置は、サービス指向型通信の通信確立フェーズにおける通信確立フレームを監視し、前記通信確立フレームに記載される通信ＩＤごとに、前記通信確立フレームに記載されるサーバーアドレスまたはクライアントアドレスを含む検知ルールを生成する検知ルール生成部と、サービス指向型通信の通信フェーズにおける通信フレームを監視し、前記通信フレームに含まれる通信ＩＤと対応する前記検知ルールを参照し、前記通信フレームに記載されたサーバーアドレスまたはクライアントアドレスが、前記検知ルールに記載されたサーバーアドレスまたはクライアントアドレスと異なる場合に、前記通信フレームを異常フレームとして検知する異常検知部と、前記異常フレームを検知した場合に、異常を通知する異常通知部を備える、異常検知装置である。

[0018] これにより、事前にＩＰアドレスを設定することなく、ソフトウェアの可搬性を維持したまま、動的にサーバーＩＰアドレスとクライアントＩＰアドレスを検知ルールとして生成して利用することができ、検知ルールに記載されたサーバーＩＰアドレスまたはクライアントＩＰアドレスとアドレスが異なる通信は、正規のサービス指向型通信の通信確立フェーズを経由していないフレームであることから、異常フレームであると判断できる。

[0019] また、前記検知ルール生成部は、前記通信確立フレームに記載される通信ＩＤごとに、前記通信確立フレームに記載される１以上のサーバーアドレスまたは１以上のクライアントアドレスを含む１以上の検知ルールを生成し、前記異常検知部は、前記通信フレームに記載された通信ＩＤと対応する前記

１以上の検知ルールを参照し、前記通信フレームに記載されたサーバーアドレスまたはクライアントアドレスが、前記１以上の検知ルールに記載されたサーバーアドレスまたはクライアントアドレスとすべて異なる場合に、前記通信フレームを異常フレームとして検知する。

[0020] これにより、一つの通信ＩＤに対して複数の検知ルールを保持することで、サービス指向型通信において、システム冗長化のために同一のサービスを提供する複数のサーバーが存在する場合、または同一のサービスを利用するクライアントが複数存在する場合であっても、誤検知を防ぐことができる。

[0021] また、前記検知ルール生成部は、前記通信確立フレームに記載される通信種別を確認し、前記通信種別がサービス提供またはサービス購読応答、サービス探索、サービス購読であれば、前記通信確立フレームに含まれる通信ＩＤとサーバーアドレスの組もしくは、前記通信ＩＤとクライアントアドレスの組と対応する検知ルールの通信確立状態をＯＮに変更し、前記通信種別がサービス提供停止またはサービス購読停止であれば、前記通信ＩＤと対応する検知ルールの通信確立状態をＯＦＦに変更し、前記異常検知部は、前記通信フレームに記載された通信ＩＤと対応する検知ルールを参照し、前記通信フレームに記載されたサーバーアドレスとクライアントアドレスが、前記検知ルールに記載されたサーバーアドレスとクライアントアドレスと一致する場合に、前記検知ルールの通信確立状態がＯＦＦであれば、前記通信フレームを異常フレームとして検知する。

[0022] これにより、サービス指向型通信において、通信ＩＤごとに通信フレームが通信してよい状態であるか通信してはいけない状態であるかを示す通信確立状態を保持することで、通信してはいけない状態で不正に通信された通信フレームを、異常として判断できる。

[0023] また、前記検知ルール生成部は、前記通信種別がサービス提供停止またはサービス購読停止であれば、所定時間待機した後、前記通信ＩＤと対応する前記検知ルールの通信確立状態をＯＦＦに変更する。

[0024] これにより、サービス提供停止またはサービス購読停止のフレームが送信

されてから所定時間待機してから検知ルールの通信確立状態を変更することで、サーバーが購読停止を受け取っていないまたはクライアント側がサービス提供停止を受け取っていない時間帯において、誤検知を防ぐことができる。

[0025] また、前記検知ルール生成部は、前記通信確立フレームの通信種別を確認し、前記通信種別がサービス提供停止であれば、前記通信ＩＤとサーバーアドレスと対応する検知ルールを確認し、前記検知ルールが存在しない場合に異常と判定し、前記通信種別がサービス購読停止であれば、前記通信ＩＤとクライアントアドレスと対応する検知ルールを確認し、前記検知ルールが存在しない場合に異常と判定する。

[0026] これにより、通信確立フェーズにおいてサービス提供またはサービス購読を実施していないのにかかわらず、サービス提供停止またはサービス購読停止が実施された場合は、不正な通信であると分かるため、異常として判断できる。

[0027] また、前記検知ルール生成部は、通信ＩＤごとに利用するサーバー数を表す通信ＩＤ別サーバー数と通信ＩＤごとに利用するクライアント数を表す通信ＩＤ別クライアント数のうち少なくとも１つを事前に記憶し、前記通信確立フレームに記載された通信ＩＤとサーバーアドレスの組または、前記通信ＩＤとクライアントアドレスの組と、前記通信ＩＤと対応する検知ルールを確認し、前記通信ＩＤと前記アドレスの組が一致しない場合に、通信ＩＤ別サーバー数または通信ＩＤ別クライアント数を確認し、現在検知ルールに登録されているサーバーの種類数よりも通信ＩＤ別サーバー数の方が大きければ、異常として検知し、または、現在検知ルールに登録されているクライアントの種類数よりも通信ＩＤ別クライアント数の方が大きければ、異常として検知する。

[0028] これにより、ＩＰアドレスよりも設定が容易である、サーバー数とクライアント数を事前に設定しておくことで、不正に通信確立フレームが送信された場合に、正常よりも通信確立フレームの種類数が増加することから、異常

であると判断できる。

[0029] また、前記検知ルール生成部は、前回生成した前回検知ルールを記憶し、前記検知ルール生成時に、異常として検知した場合に、前記通信ＩＤとサーバーアドレスの組または通信ＩＤとクライアントアドレスの組と一致する前回検知ルールを参照し、前記通信ＩＤとサーバーアドレスの組または通信ＩＤとクライアントアドレスの組と対応する検知ルール記載の内容を前回検知ルール記載の内容に書き換える。

[0030] これにより、不正に通信確立フレームが送信された場合に、前回の検知ルールを優先することで、例えば、出荷前は正規の通信確立フレームが流れており正しい検知ルールが作成できており、出荷後に不正な通信確立フレームが送信された場合に、出荷前の正しい検知ルールを優先することができ、より正しい検知ルールを用いることができる。

[0031] また、前記検知ルール生成部は、通信ＩＤごとに通信許可される車両状態を事前に記憶し、前記通信確立フレームを受信すると、車両状態を取得し、通信ＩＤごとに通信許可される車両状態でない場合に、異常と検知し、前記異常検知部は、前記通信フレームを受信すると、車両状態を取得し、通信ＩＤごとに通信許可される車両状態でない場合に、異常と検知する。

[0032] これにより、不正な車両状態において、通信確立フレームまたは通信フレームが送信された場合に、異常と判断することができる。

[0033] また、前記車両状態は、イグニションの状態、ネットワーク接続状態、シフト状態、運転支援モードの状態、自動運転の状態、人物または物体検知の状態のうち少なくとも１つを含む。

[0034] これにより、イグニションＯＮの状態でしか発生しないカメラ映像処理のフレームや、ネットワーク接続状態かつパーキングシフトの状態でしか発生しないソフトアップデートのフレームや、自動駐車モードの状態でしか発生しない操舵指示フレームや、自動運転モードかつ人物または物体検知の状態でしか発生しないブレーキ制御指示フレームなどが不正な状態で発生した場合に、異常な通信フレームを検知することができる。

[0035] また、前記サービス指向型通信における通信フェーズはＳＯＭＥ／ＩＰであり、通信確立フェーズはＳＯＭＥ／ＩＰ－ＳＤであり、通信ＩＤは、Ｓｅｒｖｉｃｅ ＩＤおよびＭｅｔｈｏｄ ＩＤであり、通信種別におけるサービス提供、サービス購読、サービス探索、サービス購読応答、サービス提供停止、サービス購読停止は、それぞれＳｅｒｖｉｃｅ Ｏｆｆｅｒ、Ｓｅｒｖｉｃｅ Ｓｕｂｓｃｒｉｂｅ、Ｓｅｒｖｉｃｅ Ｆｉｎｄ、Ｓｅｒｖｉｃｅ ＳｕｂｓｃｒｉｂｅＡｃｋ、Ｓｔｏｐ Ｏｆｆｅｒ、Ｓｔｏｐ Ｓｕｂｓｃｒｉｂｅである。

[0036] これにより、ＳＯＭＥ／ＩＰにおいて、通信確立フェーズで動的にルールを作成して、異常な通信フレームを検知することができる。

[0037] なお、これらの全般的または具体的な態様は、システム、方法、集積回路、コンピュータプログラムまたはコンピュータで読み取り可能なＣＤ－ＲＯＭ等の記録媒体で実現されても良く、システム、方法、集積回路、コンピュータプログラムまたは記録媒体の任意な組み合わせで実現されてもよい。

[0038] 以下、実施の形態に係る異常検知装置について図面を参照しながら説明する。ここで示す実施の形態は、いずれも本開示の一具体例を示すものである。従って、以下の実施の形態で示される数値、構成要素、構成要素の配置および接続形態、並びに、処理の要素としてのステップおよびステップの順序等は、一例であって本開示を限定するものではない。以下の実施の形態における構成要素のうち、独立請求項に記載されていない構成要素については、任意に付加可能な構成要素である。また、各図は、模式図であり、必ずしも厳密に図示されたものではない。

[0039] （実施の形態１）

[車載ネットワークシステム１０の全体構成図]

図１は、本開示の実施の形態１における車載ネットワークシステム１０の全体構成図である。

[0040] 図１において、車載ネットワークシステム１０は、ＩＤＳＥＣＵ１００と、ＣｅｎｔｒａｌＥＣＵ２００と、ＺｏｎｅＥＣＵ３００ａと、ＺｏｎｅＥ

ＣＵ３００ｂと、ＺｏｎｅＥＣＵ３００ｃと、ＺｏｎｅＥＣＵ３００ｄと、カメラＥＣＵ４００ａと、カーナビＥＣＵ４００ｂと、ステアリングＥＣＵ４００ｃと、ブレーキＥＣＵ４００ｄを備える。

[0041] ＩＤＳＥＣＵ１００と、ＣｅｎｔｒａｌＥＣＵ２００と、ＺｏｎｅＥＣＵ３００ａと、ＺｏｎｅＥＣＵ３００ｂと、ＺｏｎｅＥＣＵ３００ｃと、ＺｏｎｅＥＣＵ３００ｄは、イーサネット（登録商標）１３を介して接続される。

[0042] カメラＥＣＵ４００ａとＺｏｎｅＥＣＵ３００ａはイーサネット１２を介して接続され、カーナビＥＣＵ４００ｂとＺｏｎｅＥＣＵ３００ｂはイーサネット１１を介して接続され、ステアリングＥＣＵ４００ｃとＺｏｎｅＥＣＵ３００ｃはＣＡＮ１４を介して接続され、ブレーキＥＣＵ４００ｄとＺｏｎｅＥＣＵ３００ｄはＣＡＮ－ＦＤ１５を介して接続される。

[0043] ＣｅｎｔｒａｌＥＣＵ２００は、イーサネット１３に加えて、インターネット等の外部ネットワークにも接続される。

[0044] ＩＤＳＥＣＵ１００は、イーサネット１３を流れるサービス指向通信プロトコルに従う通信を監視し、異常なフレームを検出し、ＣｅｎｔｒａｌＥＣＵ２００を介してインターネット上のサーバーへ異常フレームの情報を通知し、ＺｏｎｅＥＣＵ３００ｂを介してカーナビＥＣＵ４００ｂに異常を表示することでドライバーへ異常フレームの情報を通知する機能を有する異常検知装置である。異常検知方法については後述する。

[0045] ＣｅｎｔｒａｌＥＣＵ２００は、ＺｏｎｅＥＣＵ３００ａ、３００ｂ、３００ｃ、３００ｄと、ＩＤＳＥＣＵ１００と、イーサネット１３を介して、サービス指向通信プロトコルに従って通信を行い、ＺｏｎｅＥＣＵ３００ａ、３００ｂ、３００ｃ、３００ｄを制御し、車載ネットワークシステム全体を制御する。

[0046] また、ＣｅｎｔｒａｌＥＣＵ２００は、内部にスイッチ機能を保持し、ＺｏｎｅＥＣＵ３００ａ、３００ｂ、３００ｃ、３００ｄとＣｅｎｔｒａｌＥＣＵ２００間で送信されるフレームおよび、ＺｏｎｅＥＣＵ３００ａ、３０

０ｂ、３００ｃ、３００ｄ間で通信されるフレームをＩＤＳＥＣＵ１００へ転送する機能を有し、また、ＩＤＳＥＣＵ１００から異常フレームの情報を受信し、外部ネットワークを介して、インターネット上のサーバーへ通知する機能を有する。

[0047] ＺｏｎｅＥＣＵ３００ａは、イーサネット１３を介して、Ｃｅｎｔｒａｌ ＥＣＵ２００およびＩＤＳＥＣＵ１００、ＺｏｎｅＥＣＵ３００ｂ、３００ｃ、３００ｄと通信し、イーサネット１２を介して、カメラＥＣＵ４００ａと通信し、カメラ映像のＯＮ／ＯＦＦを制御する。

[0048] ＺｏｎｅＥＣＵ３００ｂは、イーサネット１３を介して、Ｃｅｎｔｒａｌ ＥＣＵ２００およびＩＤＳＥＣＵ１００、ＺｏｎｅＥＣＵ３００ａ、３００ｃ、３００ｄと通信し、イーサネット１１を介して、カーナビＥＣＵ４００ｂと通信し、カーナビの表示を制御する。

[0049] ＺｏｎｅＥＣＵ３００ｃは、イーサネット１３を介して、Ｃｅｎｔｒａｌ ＥＣＵ２００およびＩＤＳＥＣＵ１００、ＺｏｎｅＥＣＵ３００ａ、３００ｂ、３００ｄと通信し、ＣＡＮ１４を介して、ステアリングＥＣＵ４００ｃと通信し、ステアリングの操舵を制御する。

[0050] ＺｏｎｅＥＣＵ３００ｄは、イーサネット１３を介して、Ｃｅｎｔｒａｌ ＥＣＵ２００およびＩＤＳＥＣＵ１００、ＺｏｎｅＥＣＵ３００ａ、３００ｂ、３００ｃと通信し、ＣＡＮ－ＦＤ１５を介して、ブレーキＥＣＵ４００ｄと通信し、ブレーキを制御する。

[0051] カメラＥＣＵ４００ａは、車両に搭載されるカメラの映像を制御する。

[0052] カーナビＥＣＵ４００ｂは、車両に搭載されるカーナビの表示を制御する。

[0053] ステアリングＥＣＵ４００ｃは、車両に搭載されるステアリングの操舵を制御する。

[0054] ブレーキＥＣＵ４００ｄは、車両に搭載されるブレーキを制御する。

[0055] ［ＩＤＳＥＣＵの構成図］

図２は、本開示の実施の形態１におけるＩＤＳＥＣＵ１００の構成図であ

る。図２において、ＩＤＳＥＣＵ１００は、通信部１１０と、転送部１２０と、検知ルール記憶部１３０と、検知ルール生成部１４０と、異常検知部１５０と、異常通知部１６０と、車両状態抽出部１７０を備える。

[0056] 通信部１１０は、イーサネット１３と接続され、イーサネット１３上に流れるサービス指向通信プロトコルに従うフレームを受信し、転送部１２０へ送信する機能を有する。ここで、サービス指向通信プロトコルはＳＯＭＥ／ＩＰである。ＳＯＭＥ／ＩＰのデータフォーマットの詳細は後述する。

[0057] 転送部１２０は、通信部１１０からサービス指向通信プロトコルに従うフレームを受信し、受信したフレームがＳＯＭＥ／ＩＰの通信フェーズにおける通信フレームであれば、転送部１２０は、受信したフレームを異常検知部１５０へ転送し、受信したフレームがＳＯＭＥ／ＩＰの通信確立フェーズにおける通信確立フレームであれば、転送部１２０は、受信したフレームを検知ルール生成部１４０へ転送する。また、受信したフレームが車両状態に関わる通信フレームであれば、転送部１２０は、受信したフレームを車両状態抽出部１７０へ転送する。

[0058] ここで、通信確立フレームとはＳＯＭＥ／ＩＰ－ＳＤヘッダを有するフレームであり、通信フレームとは、ＳＯＭＥ／ＩＰヘッダのみを有するフレームである。車両状態に関わる通信フレームとは、ネットワーク接続状態、車速、シフト状態、イグニション状態が格納されているフレームや、自動運転モード、自動駐車モードなどの走行状態が格納されているフレームである。

[0059] 検知ルール記憶部１３０は、検知ルール生成部１４０から検知ルールを受信し、現在の検知ルールとして保持し、前回起動時に検知ルール生成部１４０が生成した検知ルールを前回検知ルールとして保持し、通信ＩＤごとのサーバー数やクライアント数などの事前設定ルールを保持する。事前設定ルールおよび検知ルールの詳細については後述する。

[0060] 検知ルール生成部１４０は、転送部１２０から通信確立フレームを受信し、通信確立フレームのヘッダ情報に記載される通信ＩＤごとに検知ルールを生成し、検知ルール記憶部１３０に記憶する。また、検知ルール生成部１４

０は、車両状態抽出部１７０から車両状態を取得する。また、検知ルール生成部１４０は、検知ルール生成時に、異常と判定された通信確立フレームを異常通知部１６０へ送信する。検知ルールの生成方法については後述する。

[0061] 異常検知部１５０は、転送部１２０から通信フレームを受信し、通信フレームのヘッダ情報に記載される通信ＩＤとサーバーアドレスとクライアントアドレスの組を取得し、車両状態抽出部１７０から車両状態を取得し、検知ルール記憶部１３０が保持する現在の検知ルールを参照し、検知ルールを用いて、受信した通信フレームが異常フレームかどうかを検知する。異常フレームの検知方法については後述する。

[0062] 異常通知部１６０は、検知ルール生成部１４０から異常な通信確立フレームを受信し、異常検知部１５０から異常な通信フレームを受信し、ＣｅｎｔｒａｌＥＣＵ２００向けのフレームに異常フレームの情報を格納し、通信部１１０へ送信する。

[0063] 車両状態抽出部１７０は、転送部１２０から車両状態に関わる通信フレームを受信し、車両状態を抽出して、検知ルール生成部１４０と異常検知部１５０へ送信する。

[0064] [車載ネットワークシステム１０におけるヘッダフォーマット]

図３は、本開示の実施の形態１における車載ネットワークシステム１０のイーサネット１３におけるヘッダフォーマットである。ここで、ヘッダフォーマットは、サービス指向型通信であるＳＯＭＥ／ＩＰにおけるヘッダフォーマットである。

[0065] ＳＯＭＥ／ＩＰにおける通信フェーズの通信フレームには、ＳＯＭＥ／ＩＰヘッダのみが格納され、ＳＯＭＥ／ＩＰにおける通信確立フェーズの通信確立フレームには、ＳＯＭＥ／ＩＰヘッダおよびＳＯＭＥ／ＩＰ－ＳＤヘッダが格納される。

[0066] ＳＯＭＥ／ＩＰヘッダには、ＭｅｓｓａｇｅＩＤと、Ｌｅｎｇｔｈと、ＲｅｑｕｅｓｔＩＤと、ＰｒｏｔｏｃｏｌＶｅｒｓｉｏｎと、ＩｎｔｅｒｆａｃｅＶｅｒｓｉｏｎと、ＭｅｓｓａｇｅＴｙｐｅと、ＲｅｔｕｒｎＣｏｄｅ

が記載される。

[0067] ＭｅｓｓａｇｅＩＤには、ＳｅｒｖｉｃｅＩＤとＭｅｔｈｏｄＩＤが含まれる。ＭｅｓｓａｇｅＩＤは、車載ネットワークシステム１０においてユニークである。ＳｅｒｖｉｃｅＩＤは、サーバーが提供するサービスのアプリケーションを識別する番号を表し、ＭｅｔｈｏｄＩＤは、サーバーが提供するサービスのアプリケーションのメソッドの番号を表す。

[0068] Ｌｅｎｇｔｈは、ＲｅｑｕｅｓｔＩＤからＳＯＭＥ／ＩＰヘッダの最後までの長さが記載される。

[0069] ＲｅｑｕｅｓｔＩＤは、ＣｌｉｅｎｔＩＤとＳｅｓｓｉｏｎＩＤが記載される。ＣｌｉｅｎｔＩＤは、クライアントのアプリケーションを識別するための番号であり、ＳｅｓｓｉｏｎＩＤは、サーバーのアプリケーションとクライアントのアプリケーションとの通信を識別するための番号である。

[0070] ＰｒｏｔｏｃｏｌＶｅｒｓｉｏｎは、ＳＯＭＥ／ＩＰプロトコルのバージョン情報が記載され、ＩｎｔｅｒｆａｃｅＶｅｒｓｉｏｎは、ＳＯＭＥ／ＩＰプロトコルのインターフェイスのバージョンが記載され、ＭｅｓｓａｇｅＴｙｐｅは、ＳＯＭＥ／ＩＰの通信フレームにおける通信種別が記載され、ＲｅｔｕｒｎＣｏｄｅは、エラーコードなどの返り値が記載される。

[0071] ＭｅｓｓａｇｅＴｙｐｅは、具体的には、Ｒｅｑｕｅｓｔ、ＲｅｑｕｅｓｔＮｏＲｅｔｕｒｎ、Ｒｅｓｐｏｎｓｅ、Ｅｒｒｏｒ、ＴＰＲｅｑｕｅｓｔ、ＴＰＮｏｔｉｆｉｃａｔｉｏｎ、ＴＰＲｅｓｐｏｎｓｅ、ＴＰＥｒｒｏｒを識別する番号が記載される。

[0072] ここで、ＭｅｓｓａｇｅＩＤは、以降、通信ＩＤとも記載する。通信ＩＤに応じて、通信フレームの内容が定まる。例えば、カメラ映像を要求するサービスを提供する通信フレームや、ソフトアップデートを要求する通信フレーム、ハンドル制御を指示する通信フレーム、ブレーキ制御を指示する通信フレーム、車両状態を提供する通信フレーム、シフト変更を要求する通信フレームなど、通信ＩＤを確認することで、通信フレームにどのような情報が格納されているかを判断することができる。

[0073] ＳＯＭＥ／ＩＰ－ＳＤヘッダには、Ｆｌａｇｓと、Ｒｅｓｅｒｖｅｄと、ＬｅｎｇｔｈＯｆＥｎｔｒｉｅｓＡｒｒａｙＩｎＢｙｔｅｓと、ＳＤ－Ｔｙｐｅと、Ｉｎｄｅｘ１ｓｔＯｐｔｉｏｎｓと、Ｉｎｄｅｘ２ｎｄＯｐｔｉｏｎｓと、ＮｕｍｂｅｒＯｆＯｐｔｉｏｎｓと、ＳＤ－ＳｅｒｖｉｃｅＩＤとＩｎｓｔａｎｃｅＩＤと、ＭａｊｏｒＶｅｒｓｉｏｎと、ＴＴＬと、ＭｉｎｏｒＶｅｒｓｉｏｎが記載される。

[0074] Ｆｌａｇｓは、フラグ情報が記載され、Ｒｅｓｅｒｖｅｄは、予約番号が記載され、ＬｅｎｇｔｈＯｆＥｎｔｒｉｅｓＡｒｒａｙＩｎＢｙｔｅｓは、オプションを除く、ＳＯＭＥ／ＩＰ－ＳＤヘッダの最後までの長さが記載され、ＳＤ－Ｔｙｐｅは、ＳＯＭＥ／ＩＰの通信確立フレームにおける通信種別が記載され、Ｉｎｄｅｘ１ｓｔＯｐｔｉｏｎｓとＩｎｄｅｘ２ｎｄＯｐｔｉｏｎｓは、１つ目のオプションヘッダの有無と２つ目のオプションヘッダの有無が記載され、ＮｕｍｂｅｒＯｆＯｐｔｉｏｎｓはオプションヘッダの数が記載され、ＳＤ－ＳｅｒｖｉｃｅＩＤは、ＳＯＭＥ／ＩＰ－ＳＤにおける通信確立フレームの識別番号が記載され、ＩｎｓｔａｎｃｅＩＤは、ＥＣＵを識別する番号が記載され、ＭａｊｏｒＶｅｒｓｉｏｎは、通信確立フェーズのメジャーバージョンが記載され、ＴＴＬは、ＴＴＬが記載され、ＭｉｎｏｒＶｅｒｓｉｏｎは、通信確立フェーズのマイナーバージョンが記載される。

[0075] また、ＳＯＭＥ／ＩＰ－ＳＤヘッダには、オプションとして、ＬｅｎｇｔｈＯｆＯｐｔｉｏｎｓＡｒｒａｙＩｎＢｙｔｅｓと、ＯｐｔｉｏｎＬｅｎｇｔｈと、ＯｐｔｉｏｎＴｙｐｅと、Ｒｅｓｅｒｖｅｄと、ＩＰｖ４－Ａｄｄｒｅｓｓと、Ｌ４－Ｐｒｏｔｏと、ＰｏｒｔＮｕｍｂｅｒが記載される。オプションは、ＩＰアドレスの情報を共有する場合に利用される。

[0076] ＬｅｎｇｔｈＯｆＯｐｔｉｏｎｓＡｒｒａｙＩｎＢｙｔｅｓは、オプションヘッダ全体のデータ長が記載され、ＯｐｔｉｏｎＬｅｎｇｔｈは、１つ目のオプションヘッダの長さが記載され、ＯｐｔｉｏｎＴｙｐｅは、オプションにおける通信種別が記載されと、Ｒｅｓｅｒｖｅｄは、予約番号が記載さ

れ、ＩＰｖ４－Ａｄｄｒｅｓｓは、ＩＰｖ４のアドレス情報が記載され、Ｌ４－Ｐｒｏｔｏは、ＵＤＰやＴＣＰなど、ＩＰｖ４における通信プロトコルの種別が記載され、ＰｏｒｔＮｕｍｂｅｒは、ポート番号が記載される。

[0077] ＳＤ－Ｔｙｐｅは、ＳＤ通信種別とも記載する。具体的には、ＳＤ通信種別は、ＳｅｒｖｉｃｅＯｆｆｅｒ、ＳｅｒｖｉｃｅＳｔｏｐＯｆｆｅｒ、Ｓｕｂｓｃｒｉｂｅ、ＳｅｒｖｉｃｅＳｕｂｓｃｒｉｂｅＡｃｋ、ＳｔｏｐＳｕｂｓｃｒｉｂｅ、ＳｅｒｖｉｃｅＦｉｎｄを識別する番号が記載される。

[0078] ＳｅｒｖｉｃｅＯｆｆｅｒは、サーバーが提供するサービスが提供可能である状態をクライアントへ通知するために利用され、ＳｅｒｖｉｃｅＳｔｏｐＯｆｆｅｒは、サーバーが提供するサービスが提供不能である状態をクライアントへ通知するために利用され、Ｓｕｂｓｃｒｉｂｅは、クライアントがサービスの購読を開始することをサーバーへ通知するために利用され、ＳｔｏｐＳｕｂｓｃｒｉｂｅは、クライアントがサービスの購読を中止することをサーバーへ通知するために利用され、ＳｅｒｖｉｃｅＦｉｎｄは、クライアントが所望のサービスを有するサーバーを探索するために利用される。

[0079] ＳＯＭＥ／ＩＰでは、ＳＯＭＥ／ＩＰ通信を行う前に、サーバーは、ＳＯＭＥ／ＩＰ－ＳＤのヘッダを格納したフレームをブロードキャスト送信することで、所定のＳｅｒｖｉｃｅＩＤと対応するサービスを所望するクライアントを探索し、クライアントは、所望するＳｅｒｖｉｃｅＩＤと対応するサービスを提供するサーバーを探索するとともに、通信相手のＩＰアドレスやポート番号などの情報を取得する。その後、ＳＯＭＥ／ＩＰヘッダに記載されたＳｅｒｖｉｃｅＩＤとＭｅｓｓａｇｅＴｙｐｅとを元に、サービス指向型通信を行う。

[0080] しかしながら、ＳＯＭＥ／ＩＰ単体では、データのなりすまし対策ができておらず、ＳＯＭＥ／ＩＰ－ＳＤのブロードキャスト通信を観測することで、不正なクライアントとして、サーバーと通信確立することや、不正なサーバーとして、クライアントと通信確立することができてしまう課題がある。

[0081] サーバーからブロードキャストで送信されるＳＯＭＥ／ＩＰ－ＳＤのＳｅ

ｒｖｉｃｅＯｆｆｅｒまたはＳｅｒｖｉｃｅＳｕｂｓｃｒｉｂｅＡｃｋを参照することで、特定のサービスＩＤと対応するサービスを提供するサーバーのＩＰアドレス、プロトコル、ポート番号、ＥＣＵの識別番号を取得でき、ＩＰｖ４パケットを参照することで、ＭＡＣアドレスを取得することもできる。

[0082] さらに、サーバーからブロードキャストで送信されるＳＯＭＥ／ＩＰ－ＳＤのＳｔｏｐＳｅｒｖｉｃｅＯｆｆｅｒを参照することで、サービスを提供できない状態であることを取得できる。

[0083] また、クライアントからブロードキャストで送信されるＳＯＭＥ／ＩＰ－ＳＤのＳｅｒｖｉｃｅＦｉｎｄまたはＳｅｒｖｉｃｅＳｕｂｓｃｒｉｂｅを参照することで、特定のサービスＩＤと対応するサービスを提供するクライアントのＩＰアドレス、プロトコル、ポート番号、ＥＣＵの識別番号を取得でき、ＩＰｖ４パケットを参照することで、ＭＡＣアドレスを取得することもできる。

[0084] さらに、クライアントからブロードキャストで送信されるＳＯＭＥ／ＩＰ－ＳＤのＳｔｏｐＳｕｂｓｃｒｉｂｅを参照することで、サービスを受信しない状態であることを取得できる。

[0085] [事前設定検知ルール]

図４は、本開示の実施の形態１における検知ルール記憶部１３０が保持する事前設定検知ルールの一例を示す図である。図４において、事前設定検知ルールは、サービスＩＤとメソッドＩＤからなる通信ＩＤと、サーバー数、クライアント数、車両状態、サービス内容から構成される。

[0086] サービスＩＤは、図３のイーサネット１３におけるＳＯＭＥ／ＩＰのヘッダフォーマットにおけるＳｅｒｖｉｃｅＩＤと対応し、メソッドＩＤは、図３のイーサネット１３におけるＳＯＭＥ／ＩＰのヘッダフォーマットにおけるＭｅｔｈｏｄＩＤと対応する。

[0087] サーバー数は、通信ＩＤと対応するサービスを提供するサーバーの総数を示し、クライアント数は、通信ＩＤと対応するサービスを利用するクライア

ントの総数を示す。

[0088] 車両状態は、通信ＩＤと対応するサービスが、提供または利用される場合の車両状態の条件を示す。具体的には、車両のイグニションがＯＮである状態を示す「イグニションＯＮ状態」、車両のネットワーク接続がＯＮである状態を示す「ネットワークＯＮ状態」、車両のシフト状態がパーキングである状態を示す「パーキングＯＮ状態」、車両の車速が０ｋｍ／ｈである状態を示す「停止状態」、車両の走行モードがオートクルーズモードである状態を示す「オートクルーズモード」、車両の走行モードがオートパーキングモードである状態を示す「オートパーキングモード」、車両のカメラやセンサーが人物を検知している状態を示す「人物検知」などが記載される。

[0089] 車両状態は複数設定することが可能であり、「ｏｒ」はＯＲ条件を表し、「ａｎｄ」はＡＮＤ条件を示す。

[0090] サービス内容は、通信ＩＤと対応するサービスの概要を示す。

[0091] 図４において例えば、２行目に記載される事前設定検知ルールは、サービスＩＤが「０００１」であり、メソッドＩＤが「０００２」であり、通信ＩＤは「０００１０００２」であり、サーバー数は「１」、クライアント数は「５」であり、車両状態は、「ネットワーク接続ＯＮ状態かつパーキング状態かつ停止状態」であり、サービス内容は、「ソフトアップデート要求」である。

[0092] また、図４において例えば、６行目に記載される事前設定検知ルールは、サービスＩＤが「０００９」であり、メソッドＩＤが「００１０」であり、通信ＩＤは「０００９００１０」であり、サーバー数は「１」、クライアント数は「１」であり、車両状態は、「―」であり、サービス内容は、「シフト変更要求」である。ここで「―」は車両状態が任意であることを示す。

[0093] 検知ルール生成部１４０は、検知ルール記憶部１３０が有する事前設定検知ルールを参照することで、通信ＩＤに応じて、通信ＩＤと対応するサービスを提供するサーバーの総数、通信ＩＤと対応するサービスを利用するクライアントの総数、通信ＩＤと対応するサービスが通信される際の車両状態の

条件を取得することができる。

[0094] さらに、検知ルール生成部１４０は、特定の通信ＩＤを含むフレームを受信した際に、その通信ＩＤと対応するサービスを提供するサーバーの総数が、観測されたサーバーの総数よりも多い場合、不正なサーバーが接続されているとして異常と判断でき、通信ＩＤと対応するサービスを利用するクライアントの総数が観測されたクライアント数よりも多い場合、不正なクライアントが接続されているとして異常と判断できる。

[0095] さらに、検知ルール生成部１４０は、特定の通信ＩＤを含むフレームを受信した際に、事前設定検知ルールに記載された車両状態と、現在の車両状態が一致しない場合に、不正な車両状態でサービスが提供されているとして異常と判断できる。

[0096] [動的設定検知ルール]

図５は、本開示の実施の形態１における検知ルール生成部１４０が生成し、検知ルール記憶部１３０が記憶し、異常検知部１５０が参照する動的設定検知ルールの一例を示す図である。図５において、サービスＩＤとメソッドＩＤからなる通信ＩＤと、サーバーアドレス、クライアントアドレス、通信確立状態から構成される。

[0097] サービスＩＤは、図３のイーサネット１３におけるＳＯＭＥ／ＩＰのヘッダフォーマットにおけるＳｅｒｖｉｃｅＩＤと対応し、メソッドＩＤは、図３のイーサネット１３におけるＳＯＭＥ／ＩＰのヘッダフォーマットにおけるＭｅｔｈｏｄＩＤと対応する。サーバーアドレスは、通信ＩＤと対応するサービスを提供するサーバーのＩＰアドレスを示し、クライアントアドレスは、通信ＩＤと対応するサービスを利用するクライアントのＩＰアドレスを示す。通信確立状態は、通信ＩＤと対応するサービスが、現在有効であるかどうかを示し、「ＯＮ」であれば許可、「ＯＦＦ」であれば許可されていない状態を示す。

[0098] 図５において例えば、１行目に記載される動的設定検知ルールは、サービスＩＤが「０００１」であり、メソッドＩＤが「０００１」であり、通信Ｉ

Ｄは「０００１０００１」であり、サーバーアドレスは「Ｘ」、クライアントアドレスは「Ｂ」であり、通信確立状態は、「ＯＮ」である。

[0099] また、図５において例えば、９行目に記載される動的設定検知ルールは、サービスＩＤが「０００２」であり、メソッドＩＤが「０００３」であり、通信ＩＤは「０００２０００３」であり、サーバーアドレスは「Ｙ」、クライアントアドレスは「Ｂ」であり、通信確立状態は、「ＯＦＦ」である。

[0100] また、検知ルール記憶部１３０は、車載ネットワークシステム１０の電源がＯＮになる場合に、動的設定検知ルールをすべて消去し、車載ネットワークシステム１０の電源がＯＦＦになる場合に、動的設定検知ルールを旧動的設定検知ルールとして保持する。

[0101] つまり、検知ルール生成部１４０は、図３のイーサネット１３におけるＳＯＭＥ／ＩＰヘッダに含まれるＳｅｒｖｉｃｅＩＤとＭｅｔｈｏｄＩＤを参照して通信ＩＤの項目を生成でき、サーバーから送信される同一の通信ＩＤを含む、ＳＯＭＥ／ＩＰ－ＳＤオプションヘッダに含まれるＩＰアドレスを参照してサーバーアドレスの項目を生成でき、クライアントから送信される同一の通信ＩＤを含む、ＳＯＭＥ／ＩＰ－ＳＤオプションヘッダに含まれるＩＰアドレスを参照してクライアントアドレスの項目を生成でき、サーバーから送信されるオプションヘッダを含むＳＯＭＥ／ＩＰ－ＳＤヘッダに含まれるＳＤ－Ｔｙｐｅを参照して通信確立状態の項目を生成できる。

[0102] 具体的には、通信確立状態の項目として、ＳＤ－Ｔｙｐｅが、ＳｅｒｖｉｃｅＯｆｆｅｒまたはＳｅｒｖｉｃｅＳｕｂｓｃｒｉｂｅＡｃｋであれば、同一の通信ＩＤとサーバーアドレスを含む動的設定検知ルールの通信確立状態を「ＯＮ」に設定でき、ＳＤ－Ｔｙｐｅが、ＳｔｏｐＳｅｒｖｉｃｅＯｆｆｅｒであれば、同一の通信ＩＤとサーバーアドレスを含む動的設定検知ルールの通信確立状態を「ＯＦＦ」に設定でき、ＳＤ－Ｔｙｐｅが、ＳｅｒｖｉｃｅＦｉｎｄまたはＳｅｒｖｉｃｅＳｕｂｓｃｒｉｂｅであれば、同一の通信ＩＤとサーバーアドレスを含む動的設定検知ルールの通信確立状態を「ＯＮ」に設定でき、ＳＤ－Ｔｙｐｅが、ＳｔｏｐＳｕｂｓｃｒｉｂｅであれ

ば、同一の通信ＩＤとサーバーアドレスを含む動的設定検知ルールの通信確立状態を「ＯＦＦ」に設定できる。

[0103] また、異常検知部１５０は、動的設定検知ルールを参照することで、特定の通信ＩＤを含むフレームが、その通信ＩＤとサーバーアドレスおよびクライアントアドレスが動的設定検知ルールに適合しているかどうかを確認でき、適合していない場合、異常検知部１５０は、正規の通信確立フェーズを経ていないとして異常と判断できる。

[0104] さらに異常検知部１５０は、特定の通信ＩＤを含むフレームが、現在有効であるかどうかを確認でき、有効でない場合に、異常検知部１５０は、不正な通信確立状態で送信されたとして、異常と判断できる。

[0105] [処理のシーケンス]

図６と図７は、本開示の実施の形態１におけるＩＤＳＥＣＵ１００が車両ネットワークログを取得し、動的設定検知ルールを生成し、動的設定検知ルールと事前設定検知ルールを参照して、異常なフレームを検知して通知するまでの処理シーケンスを示している。

[0106] （Ｓ６０１）ＩＤＳＥＣＵ１００の通信部１１０は、イーサネット１３に流れるサービス指向通信プロトコルに従うフレームを受信し、転送部１２０へ送信する。

[0107] （Ｓ６０２）転送部１２０は、通信部１１０からフレームを受信し、フレームのＳＯＭＥ／ＩＰ－ＳＤヘッダに車両状態を提供する通信ＩＤが含まれている場合、車両状態抽出部１７０へ送信する。

[0108] （Ｓ６０３）車両状態抽出部１７０は、転送部１２０からフレームを受信し、フレームに含まれる車両状態を抽出する。

[0109] （Ｓ６０４）検知ルール生成部１４０は、車両状態抽出部１７０に対して、車両状態を要求する。

[0110] （Ｓ６０５）車両状態抽出部１７０は、検知ルール生成部１４０からの車両状態の要求を受信する。

[0111] （Ｓ６０６）車両状態抽出部１７０は、車両状態を検知ルール生成部１４

０へ送信する。

[0112] （Ｓ６０７）検知ルール生成部１４０は、車両状態抽出部１７０から車両状態を受信する。

[0113] （Ｓ６０８）転送部１２０は、通信部１１０からフレームを受信し、フレームがＳＯＭＥ／ＩＰ－ＳＤヘッダが含まれている通信確立フレームである場合、検知ルール生成部１４０へ通信確立フレームを送信する。

[0114] （Ｓ６０９）検知ルール生成部１４０は、転送部１２０から通信確立フレームを受信し、動的設定検知ルールを生成し、検知ルール記憶部１３０に記憶する。動的設定検知ルールの生成方法は後述する。

[0115] （Ｓ６１０）検知ルール生成部１４０は、動的設定検知ルールの生成時に、異常であると判定されたフレームを異常フレームとして、異常通知部１６０へ通知する。動的設定検知ルールの生成時に異常と検知する方法は後述する。

[0116] （Ｓ６１１）異常通知部１６０は、Ｓ６０４の異常フレームを受信すると、車両で異常が発生していることを、ドライバーまたは緊急通報先、他の車両、他のシステム、他のＩＰＳ（ＩｎｔｒｕｓｉｏｎＰｒｅｖｅｎｓｉｏｎＳｙｓｔｅｍ）への通知を要求するフレームをＣｅｎｔｒａｌＥＣＵ２００へ送信する。

[0117] （Ｓ７０１）異常検知部１５０は、車両状態抽出部１７０に対して、車両状態を要求する。

[0118] （Ｓ７０２）車両状態抽出部１７０は、異常検知部１５０から車両状態の要求を受信する。

[0119] （Ｓ７０３）車両状態抽出部１７０は、車両状態を異常検知部１５０へ送信する。

[0120] （Ｓ７０４）異常検知部１５０は、車両状態抽出部１７０から車両状態を受信する。

[0121] （Ｓ７０５）転送部１２０は、通信部１１０からフレームを受信し、フレームがＳＯＭＥ／ＩＰ－ＳＤヘッダが含まれていない通信フレームである場

合、異常検知部１５０へ通信フレームを送信する。

[0122] （Ｓ７０６）異常検知部１５０は、転送部１２０からフレームを受信すると、検知ルール記憶部１３０を参照し、事前設定検知ルールと動的設定検知ルールを参照して、受信したフレームが異常であるか否かを判定する。異常判定方法は後述する。

[0123] （Ｓ７０７）異常検知部１５０は、異常と判定した場合、異常フレームを異常通知部１６０へ送信する。

[0124] （Ｓ７０８）異常通知部１６０は、異常検知部１５０から異常フレームを受信すると、車両において異常が発生していることを、ドライバーまたは警察への通知を要求するフレームをＣｅｎｔｒａｌＥＣＵ２００へ送信する。

[0125] [検知ルール生成処理のフローチャート]

図８に、本開示の実施の形態１における検知ルール生成部１４０の検知ルール生成処理のフローチャートを示す。

[0126] （Ｓ８０１）検知ルール生成部１４０は、転送部１２０からＳＯＭＥ／ＩＰ－ＳＤヘッダを含む通信確立フレームを受信し、Ｓ８０２を実施する。

[0127] （Ｓ８０２）検知ルール生成部１４０は、受信した通信確立フレームのＳＯＭＥ／ＩＰ－ＳＤヘッダに含まれるＳＤ通信種別を確認し、ＳＤ通信種別がＳｅｒｖｉｃｅＯｆｆｅｒまたはＳｅｒｖｉｃｅＳｕｂｓｃｒｉｂｅＡｃｋである場合にＳ８０３を実施し、ＳＤ通信種別がＳｅｒｖｉｃｅＦｉｎｄまたはＳｅｒｖｉｃｅＳｕｂｓｃｒｉｂｅである場合にＳ８０４を実施し、ＳＤ通信種別がＳｔｏｐＯｆｆｅｒである場合にＳ８０５を実施し、ＳＤ通信種別がＳｔｏｐＳｅｒｖｉｃｅＳｕｂｓｃｒｉｂｅである場合にＳ８０６を実施し、ＳＤ通信種別がそれ意外の場合、終了する。

[0128] （Ｓ８０３）検知ルール生成部１４０は、受信したフレームのＳＯＭＥ／ＩＰ－ＳＤヘッダに含まれるＳｅｒｖｉｃｅＩＤとＭｅｔｈｏｄＩＤを参照して通信ＩＤを取得し、ＳＯＭＥ／ＩＰ－ＳＤヘッダに含まれるＩＰｖ４Ａｄｄｒｅｓｓを参照してサーバーアドレスを取得し、Ｓ８０７を実施する。ここで、受信するフレームはサーバーから送信されたフレームであるため、

ＩＰｖ４ＡｄｄｒｅｓｓにはサーバーのＩＰアドレスが記載される。

[0129] （Ｓ８０４）検知ルール生成部１４０は、受信したフレームのＳＯＭＥ／ＩＰ－ＳＤヘッダに含まれるＳｅｒｖｉｃｅＩＤとＭｅｔｈｏｄＩＤを参照して通信ＩＤを取得し、ＳＯＭＥ／ＩＰ－ＳＤヘッダに含まれるＩＰｖ４Ａｄｄｒｅｓｓを参照してクライアントアドレスを取得し、Ｓ８０７を実施する。ここで、受信するフレームはクライアントから送信されたフレームであるため、ＩＰｖ４Ａｄｄｒｅｓｓにはクライアントのアドレスが記載される。

[0130] （Ｓ８０５）検知ルール生成部１４０は、受信したフレームのＳＯＭＥ／ＩＰ－ＳＤヘッダに含まれるＳｅｒｖｉｃｅＩＤとＭｅｔｈｏｄＩＤを参照して通信ＩＤを取得し、ＳＯＭＥ／ＩＰ－ＳＤヘッダに含まれるＩＰｖ４Ａｄｄｒｅｓｓを参照してサーバーアドレスを取得し、Ｓ８１６を実施する。ここで、受信するフレームはサーバーから送信されたフレームであるため、ＩＰｖ４Ａｄｄｒｅｓｓにはサーバーのアドレスが記載される。

[0131] （Ｓ８０６）検知ルール生成部１４０は、受信したフレームのＳＯＭＥ／ＩＰ－ＳＤヘッダに含まれるＳｅｒｖｉｃｅＩＤとＭｅｔｈｏｄＩＤを参照して通信ＩＤを取得し、ＳＯＭＥ／ＩＰ－ＳＤヘッダに含まれるＩＰｖ４Ａｄｄｒｅｓｓを参照してクライアントアドレスを取得し、Ｓ８１６を実施する。ここで、受信するフレームはクライアントから送信されたフレームであるため、ＩＰｖ４Ａｄｄｒｅｓｓにはクライアントのアドレスが記載される。

[0132] （Ｓ８０７）検知ルール生成部１４０は、車両状態抽出部１７０から取得した車両状態と、検知ルール記憶部１３０が保持する事前設定検知ルールのうち、Ｓ８０３またはＳ８０４にて取得した通信ＩＤと同一の通信ＩＤの行を参照し、車両状態が一致しない場合、Ｓ８０９を実施し、車両状態が一致する場合、Ｓ８０８を実施する。

[0133] （Ｓ８０８）検知ルール生成部１４０は、Ｓ８０３にて取得した通信ＩＤとサーバーアドレスの組またはＳ８０４にて取得した通信ＩＤとクライアン

トアドレスの組と、検知ルール記憶部１３０が保持する動的設定検知ルールのうち、同一の通信ＩＤの行を参照し、同一の通信ＩＤとサーバーアドレスの組または通信ＩＤとクライアントアドレスが存在する場合、Ｓ８１０を実施し、通信ＩＤとサーバーアドレスの組または通信ＩＤとクライアントアドレスの組が存在しない場合、Ｓ８１１を実施する。

[0134] （Ｓ８０９）検知ルール生成部１４０は、不正な車両状態で通信確立フレームが送信されたとして、異常フレームとして判断し、異常フレームを異常通知部１６０へ送信し、終了する。

[0135] （Ｓ８１０）検知ルール生成部１４０は、Ｓ８０３にて取得した通信ＩＤとサーバーアドレスの組を取得した場合、検知ルール記憶部１３０が保持する動的設定検知ルールのうち、同一の通信ＩＤとサーバーアドレスの組を含む行を参照し、Ｓ８０４にて通信ＩＤとクライアントアドレスの組を取得した場合、同一の通信ＩＤとクライアントアドレスの組を含む行を参照し、通信確立状態がＯＮである場合、終了し、通信確立状態がＯＦＦである場合、Ｓ８０９を実施する。

[0136] （Ｓ８１１）検知ルール生成部１４０は、Ｓ８０３にて取得した通信ＩＤとサーバーアドレスの組を取得した場合、検知ルール記憶部１３０が保持する事前設定検知ルールのうち、同一の通信ＩＤの行を参照してサーバー数を取得し、次に、動的設定検知ルールのうち、同一の通信ＩＤの行を参照してサーバーアドレスの種類数を取得し、サーバーアドレスの種類数がサーバー数よりも小さければ、Ｓ８１２を実施し、サーバーアドレスの種類数がサーバー数以上であれば、Ｓ８１４を実施する。

[0137] また、Ｓ８０４にて取得した通信ＩＤとクライアントアドレスの組を取得した場合、検知ルール記憶部１３０が保持する事前設定検知ルールのうち、同一の通信ＩＤの行を参照してクライアント数を取得し、次に、動的設定検知ルールのうち、同一の通信ＩＤの行を参照してクライアントアドレスの種類数を取得し、クライアントアドレスの種類数がクライアント数よりも小さければ、Ｓ８１２を実施し、クライアントアドレスの種類数がクライアント

数以上であれば、Ｓ８１４を実施する。

[0138] （Ｓ８１２）検知ルール生成部１４０は、Ｓ８０３にて取得した通信ＩＤとサーバーアドレスの組を取得した場合、動的設定検知ルールのうち、同一の通信ＩＤの行のサーバーアドレスの項目が既に記載されている場合は、同一の通信ＩＤの行をすべてコピーし、動的設定検知ルールにコピーした行を追加し、追加したすべての行に対して、サーバーアドレスの項目にＳ８０３にて取得したサーバーアドレスを追加登録し、同一の通信ＩＤの行のサーバーアドレスの項目が記載されていない場合は、同一の通信ＩＤのすべての行に対して、Ｓ８０３にて取得したサーバーアドレスを追加登録する。Ｓ８０４にて取得した通信ＩＤとクライアントアドレスの組を取得した場合、動的設定検知ルールのうち、同一の通信ＩＤの行のクライアントアドレスの項目が既に記載されている場合は、同一の通信ＩＤの行をすべてコピーし、動的設定検知ルールにコピーした行を追加し、追加したすべての行に対して、クライアントアドレスの項目にＳ８０４にて取得したクライアントアドレスを追加登録し、同一の通信ＩＤの行のクライアントアドレスの項目が記載されていない場合は、同一の通信ＩＤのすべての行に対して、Ｓ８０４にて取得したクライアントアドレスを追加登録する。

[0139] （Ｓ８１３）Ｓ８１２にて登録したすべての行に対して、ＳＤ状態の項目をＯＮにし、終了する。

[0140] （Ｓ８１４）検知ルール生成部１４０は、不正なサーバーまたは不正なクライアントが車載ネットワークシステムに追加されているとして、異常と判定し、Ｓ８１５を実施する。

[0141] （Ｓ８１５）検知ルール生成部１４０は、検知ルール記憶部１３０が保持している動的設定検知ルールのうち、Ｓ８１４にて異常と判断した通信ＩＤを含むすべての行を、検知ルール記憶部１３０が保持している前回起動時の旧動的設定検知ルールの通信ＩＤの行と同一になるように上書き登録し、終了する。

[0142] （Ｓ８１６）検知ルール生成部１４０は、車両状態抽出部１７０から取得

した車両状態と、検知ルール記憶部１３０が保持する事前設定検知ルールのうち、Ｓ８０５またはＳ８０６にて取得した通信ＩＤと同一の通信ＩＤの行を参照し、車両状態が一致しない場合、Ｓ８１８を実施し、車両状態が一致する場合、Ｓ８１７を実施する。

[0143] （Ｓ８１７）検知ルール生成部１４０は、Ｓ８０５にて取得した通信ＩＤとサーバーアドレスの組またはＳ８０６にて取得した通信ＩＤとクライアントアドレスの組と、検知ルール記憶部１３０が保持する動的設定検知ルールのうち、同一の通信ＩＤの行を参照し、同一の通信ＩＤとサーバーアドレスの組または通信ＩＤとクライアントアドレスの組が存在する場合、Ｓ８１９を実施し、同一の通信ＩＤとサーバーアドレスの組または通信ＩＤとクライアントアドレスの組が存在しない場合、Ｓ８１８を実施する。

[0144] （Ｓ８１８）検知ルール生成部１４０は、不正な車両状態で通信確立フレームが送信されたとして、異常フレームとして判断し、異常フレームを異常通知部１６０へ送信し、終了する。

[0145] （Ｓ８１９）検知ルール生成部１４０は、Ｓ８０５にて取得した通信ＩＤとサーバーアドレスの組を取得した場合、検知ルール記憶部１３０が保持する動的設定検知ルールのうち、同一の通信ＩＤとサーバーアドレスの組を含む行に対して、通信確立状態をＯＦＦに変更し、Ｓ８０４にて通信ＩＤとクライアントアドレスの組を取得した場合、同一の通信ＩＤとクライアントアドレスの組を含む行に対して、通信確立状態をＯＦＦに変更し、終了する。車両状態をＯＦＦに変更する場合は、例えば１秒など所定時間待機した後、変更する。

[0146] [異常検知処理のフローチャート]

図９に、本開示の実施の形態１における異常検知部１５０の異常検知処理のフローチャートを示す。

[0147] （Ｓ９０１）異常検知部１５０は、転送部１２０からＳＯＭＥ／ＩＰヘッダを含む通信確立フレームを受信し、Ｓ９０２を実施する。

[0148] （Ｓ９０２）異常検知部１５０は、受信したフレームを参照し、通信ＩＤ

と、サーバーアドレスと、クライアントアドレスを取得する。通信ＩＤは、ＳＯＭＥ／ＩＤヘッダに記載されるＭｅｓｓａｇｅＩＤをもとに取得され、サーバーアドレスとクライアントアドレスはＩＰｖ４ヘッダに記載される送信元ＩＰｖ４アドレスおよび送信先ＩＰｖ４アドレスをもとに取得される。

[0149] （Ｓ９０３）異常検知部１５０は、車両状態抽出部１７０から取得した車両状態と、検知ルール記憶部１３０が保持する事前設定検知ルールのうち、Ｓ９０２にて取得した通信ＩＤと同一の通信ＩＤの行を参照し、車両状態が一致しない場合、Ｓ９０５を実施し、車両状態が一致する場合、Ｓ９０４を実施する。

[0150] （Ｓ９０４）異常検知部１５０は、Ｓ９０２にて通信ＩＤとサーバーアドレスとクライアントアドレスの組と、検知ルール記憶部１３０が保持する動的設定検知ルールのうち、同一の通信ＩＤの行を参照し、同一の通信ＩＤとサーバーアドレスとクライアントアドレスの組が存在する場合、Ｓ９０６を実施し、同一の通信ＩＤとサーバーアドレスとクライアントアドレスの組が存在しない場合、Ｓ９０５を実施する。

[0151] （Ｓ９０５）異常検知部１５０は、不正な車両状態で通信確立フレームが送信されたとして、異常フレームとして判断し、異常フレームを異常通知部１６０へ送信し、終了する。

[0152] （Ｓ９０６）異常検知部１５０は、検知ルール記憶部１３０が保持する動的設定検知ルールのうち、Ｓ９０２にて取得した通信ＩＤとサーバーアドレスとクライアントアドレスの組を含む行を参照し、通信確立状態がＯＮである場合、終了し、通信確立状態がＯＦＦである場合、Ｓ９０５を実施する。

[0153] （他の実施の形態）

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

[0154] （１）上記実施の形態では、自動車に対するセキュリティ対策として説明

したが、適用範囲はこれに限られない。自動車に限らず、建機、農機、船舶、鉄道、飛行機などのモビリティにも適用してもよい。

[0155] （２）上記の実施の形態では、検知ルール生成部１４０が生成し、検知ルール記憶部１３０が記憶する動的設定検知ルールにおいて、サーバーアドレスとクライアントアドレスがＩＰｖ４アドレスとして説明したが、サーバーアドレスとクライアントアドレスはＩＰｖ６アドレスでもよいし、ＭＡＣアドレスでもよいし、ポート番号でもよいし、ＥＣＵの識別番号でもよいし、通信プロトコルの種別でもよいし、またはこれらの組み合わせでも良い。

[0156] また、ＣＡＮやＣＡＮ－ＦＤにおいて交換されるフレームに用いられるＣＡＮＩＤを含めてもよい。この場合、ＣＡＮＩＤは、ＳＯＭＥ／ＩＰの通信フレーム内に格納されて通信される。

[0157] （３）上記の実施の形態では、ＩＤＳＥＣＵ１００は、イーサネット１３に接続されるとして説明したが、具体的には、イーサネットスイッチまたは、イーサネットハブ、ゲートウェイ、ルーターにソフトウェアまたはハードウェアとして搭載されてもよいし、それらとイーサネットケーブルで接続されるＥＣＵやＺｏｎｅＥＣＵにソフトウェアまたはハードウェアとして搭載されてもよい。

[0158] ＩＤＳＥＣＵ１００がイーサネットスイッチまたは、イーサネットハブ、ゲートウェイ、ルーターに搭載される場合、異常検知部１５０が異常フレームを検出した後、異常フレームを遮断してもよい。

[0159] ＩＤＳＥＣＵ１００がＥＣＵやＺｏｎｅＥＣＵに搭載される場合、ユニキャストパケットを含むイーサネット１３上のすべてのパケットをＩＤＳＥＣＵ１００が受信するために、イーサネットスイッチ、イーサネットハブ、ゲートウェイ、ルーターは、すべてのパケットをＩＤＳＥＣＵ１００に転送してもよい。

[0160] （４）上記の実施の形態では、イーサネット１３は、ＳＯＭＥ／ＩＰプロトコルに従うフレームによってＥＣＵ間の情報が交換されると記載したが、ＳＯＭＥ／ＩＰプロトコルでなくとも、他のサービス指向型通信プロトコル

やデータ指向型通信プロトコルであってもよい。例えば、他のデータ指向通信プロトコルとしてＤＤＳ（Ｄａｔａ　Ｄｉｓｔｒｉｂｕｔｉｏｎ　Ｓｅｒｖｉｃｅ）がある。また、ＲＥＳＴ通信や、ＨＴＴＰ通信であっても、事前設定検知ルールおよび動的設定検知ルールに含めてもよい。この場合、サービス単位ではなく、データ単位で検知ルールを生成する。

[0161] （５）上記の実施の形態では、異常通知部１６０は、異常をドライバーや警察へ通知するとして説明したが、通知先は、車両と接続されるサーバーでもよいし、交通省でもよいし、近接する車両でもよいし、交通システムでもよいし、脆弱性情報等の共有機関でもよい。

[0162] （６）上記実施の形態における各装置を構成する構成要素の一部または全部は、１個のシステムＬＳＩ（Ｌａｒｇｅ　Ｓｃａｌｅ　Ｉｎｔｅｇｒａｔｉｏｎ：大規模集積回路）から構成されているとしても良い。システムＬＳＩは、複数の構成部を１個のチップ上に集積して製造された超多機能ＬＳＩであり、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ等を含んで構成されるコンピュータシステムである。ＲＡＭには、コンピュータプログラムが記録されている。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、システムＬＳＩは、その機能を達成する。また、上記各装置を構成する構成要素の各部は、個別に１チップ化されていても良いし、一部または全部を含むように１チップ化されても良い。また、ここでは、システムＬＳＩとしたが、集積度の違いにより、ＩＣ、ＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩと呼称されることもある。また、集積回路化の手法はＬＳＩに限るものではなく、専用回路または汎用プロセッサで実現しても良い。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Ｆｉｅｌｄ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用しても良い。更には、半導体技術の進歩または派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行っても良い。バイオ技術の適用等が可能性としてあ

り得る。

[0163] （７）上記各装置を構成する構成要素の一部または全部は、各装置に脱着可能なＩＣカードまたは単体のモジュールから構成されているとしても良い。ＩＣカードまたはモジュールは、マイクロプロセッサ、ＲＯＭ、ＲＡＭ等から構成されるコンピュータシステムである。ＩＣカードまたはモジュールは、上記の超多機能ＬＳＩを含むとしても良い。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、ＩＣカードまたはモジュールは、その機能を達成する。このＩＣカードまたはこのモジュールは、耐タンパ性を有するとしてもよい。

[0164] （８）本開示の一態様としては、異常検知の方法をコンピュータにより実現するプログラム（コンピュータプログラム）であるとしても良いし、コンピュータプログラムからなるデジタル信号であるとしても良い。また、本開示の一態様としては、コンピュータプログラムまたはデジタル信号をコンピュータで読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕｅ－ｒａｙ（登録商標） Ｄｉｓｃ）、半導体メモリ等に記録したものとしても良い。また、これらの記録媒体に記録されているデジタル信号であるとしても良い。また、本開示の一態様としては、コンピュータプログラムまたはデジタル信号を、電気通信回線、無線または有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしても良い。また、本開示の一態様としては、マイクロプロセッサとメモリを備えたコンピュータシステムであって、メモリは、上記コンピュータプログラムを記録しており、マイクロプロセッサは、コンピュータプログラムに従って動作するとしても良い。また、プログラム若しくはデジタル信号を記録媒体に記録して移送することにより、または、プログラム若しくはデジタル信号を、ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

[0165] （９）上記実施の形態および上記変形例で示した各構成要素および機能を

任意に組み合わせることで実現される形態も本開示の範囲に含まれる。

産業上の利用可能性

[0166] 本開示の車載ネットワークにおける異常検知装置によれば、ＳＯＭＥ／ＩＰ－ＳＤの通信フレームを監視して検知ルールを動的生成することで、送信先ＩＰアドレスと送信元ＩＰアドレスの事前設定を不要とし、動的生成した検知ルールを用いてＳＯＭＥ／ＩＰの通信フレームを監視して異常なフレームとして検知する方法を取ることで、サービス指向型通信の可搬性を失わずに、安全な自動運転や先進運転支援システムを提供することを目的とする。

符号の説明

[0167] １０　車載ネットワークシステム

１１、１２、１３　イーサネット

１４　ＣＡＮ

１５　ＣＡＮ－ＦＤ

１００　ＩＤＳＥＣＵ

１１０　通信部

１２０　転送部

１３０　検知ルール記憶部

１４０　検知ルール生成部

１５０　異常検知部

１６０　異常通知部

１７０　車両状態抽出部

２００　ＣｅｎｔｒａｌＥＣＵ

３００ａ、３００ｂ、３００ｃ、３００ｄ　ＺｏｎｅＥＣＵ

４００ａ　カメラＥＣＵ

４００ｂ　カーナビＥＣＵ

４００ｃ　ステアリングＥＣＵ

４００ｄ　ブレーキＥＣＵ

請求の範囲

[請求項1] イーサネット（登録商標）で構成される車載ネットワークシステムにおける異常検知装置であって、前記異常検知装置は、

サービス指向型通信の通信確立フェーズにおける通信確立フレームを監視し、前記通信確立フレームに記載される通信ＩＤごとに、前記通信確立フレームに記載されるサーバーアドレスまたはクライアントアドレスを含む検知ルールを生成する検知ルール生成部と、

サービス指向型通信の通信フェーズにおける通信フレームを監視し、前記通信フレームに含まれる通信ＩＤと対応する前記検知ルールを参照し、前記通信フレームに記載されたサーバーアドレスまたはクライアントアドレスが、前記検知ルールに記載されたサーバーアドレスまたはクライアントアドレスと異なる場合に、前記通信フレームを異常フレームとして検知する異常検知部と、

前記異常フレームを検知した場合に、異常を通知する異常通知部を備える、

異常検知装置。

[請求項2] 前記検知ルール生成部は、前記通信確立フレームに記載される通信ＩＤごとに、前記通信確立フレームに記載される１以上のサーバーアドレスまたは１以上のクライアントアドレスを含む１以上の検知ルールを生成し、

前記異常検知部は、前記通信フレームに記載された通信ＩＤと対応する前記１以上の検知ルールを参照し、前記通信フレームに記載されたサーバーアドレスまたはクライアントアドレスが、前記１以上の検知ルールに記載されたサーバーアドレスまたはクライアントアドレスとすべて異なる場合に、前記通信フレームを異常フレームとして検知する、

請求項１記載の異常検知装置。

[請求項3] 前記検知ルール生成部は、前記通信確立フレームに記載される通信

種別を確認し、前記通信種別がサービス提供またはサービス購読応答、サービス探索、サービス購読であれば、前記通信確立フレームに含まれる通信ＩＤとサーバーアドレスの組もしくは、前記通信ＩＤとクライアントアドレスの組と対応する検知ルールの通信確立状態をＯＮに変更し、前記通信種別がサービス提供停止またはサービス購読停止であれば、前記通信ＩＤと対応する検知ルールの通信確立状態をＯＦＦに変更し、

前記異常検知部は、前記通信フレームに記載された通信ＩＤと対応する検知ルールを参照し、前記通信フレームに記載されたサーバーアドレスとクライアントアドレスが、前記検知ルールに記載されたサーバーアドレスとクライアントアドレスと一致する場合に、前記検知ルールの通信確立状態がＯＦＦであれば、前記通信フレームを異常フレームとして検知する、

請求項１または２に記載の異常検知装置。

[請求項4] 前記検知ルール生成部は、前記通信種別がサービス提供停止またはサービス購読停止であれば、所定時間待機した後、前記通信ＩＤと対応する前記検知ルールの通信確立状態をＯＦＦに変更する、

請求項３記載の異常検知装置。

[請求項5] 前記検知ルール生成部は、前記通信確立フレームの通信種別を確認し、前記通信種別がサービス提供停止であれば、前記通信ＩＤとサーバーアドレスと対応する検知ルールを確認し、前記検知ルールが存在しない場合に異常と判定し、前記通信種別がサービス購読停止であれば、前記通信ＩＤとクライアントアドレスと対応する検知ルールを確認し、前記検知ルールが存在しない場合に異常と判定する、

請求項３または４記載の異常検知装置。

[請求項6] 前記検知ルール生成部は、通信ＩＤごとに利用するサーバー数を表す通信ＩＤ別サーバー数と通信ＩＤごとに利用するクライアント数を表す通信ＩＤ別クライアント数のうち少なくとも１つを事前に記憶し

、前記通信確立フレームに記載された通信ＩＤとサーバーアドレスの組または、前記通信ＩＤとクライアントアドレスの組と、前記通信ＩＤと対応する検知ルールを確認し、前記通信ＩＤと前記アドレスの組が一致しない場合に、通信ＩＤ別サーバー数または通信ＩＤ別クライアント数を確認し、現在検知ルールに登録されているサーバーの種類数よりも通信ＩＤ別サーバー数の方が大きければ、異常として検知し、または、現在検知ルールに登録されているクライアントの種類数よりも通信ＩＤ別クライアント数の方が大きければ、異常として検知する、

請求項１から５のいずれか１項に記載の異常検知装置。

[請求項7] 前記検知ルール生成部は、前回生成した前回検知ルールを記憶し、前記検知ルールの生成時に、異常として検知した場合に、前記通信ＩＤとサーバーアドレスの組または通信ＩＤとクライアントアドレスの組と一致する前回検知ルールを参照し、前記通信ＩＤとサーバーアドレスの組または通信ＩＤとクライアントアドレスの組と対応する検知ルール記載の内容を前回検知ルール記載の内容に書き換える、

請求項６記載の異常検知装置。

[請求項8] 前記検知ルール生成部は、通信ＩＤごとに通信許可される車両状態を事前に記憶し、前記通信確立フレームを受信すると、車両状態を取得し、通信ＩＤごとに通信許可される車両状態でない場合に、異常と検知し、

前記異常検知部は、前記通信フレームを受信すると、車両状態を取得し、通信ＩＤごとに通信許可される車両状態でない場合に、異常と検知する、

請求項１から７のいずれか１項に記載の異常検知装置。

[請求項9] 前記車両状態は、イグニションの状態、ネットワーク接続状態、シフト状態、運転支援モードの状態、自動運転の状態、人物または物体検知の状態のうち少なくとも１つを含む、

請求項８記載の異常検知装置。

[請求項10] 前記サービス指向型通信における通信フェーズはＳＯＭＥ／ＩＰであり、通信確立フェーズはＳＯＭＥ／ＩＰ－ＳＤであり、通信ＩＤは、Ｓｅｒｖｉｃｅ　ＩＤおよびＭｅｔｈｏｄ　ＩＤであり、通信種別におけるサービス提供、サービス購読、サービス探索、サービス購読応答、サービス提供停止、サービス購読停止は、それぞれＳｅｒｖｉｃｅ　Ｏｆｆｅｒ、Ｓｅｒｖｉｃｅ　Ｓｕｂｓｃｒｉｂｅ、Ｓｅｒｖｉｃｅ　Ｆｉｎｄ、Ｓｅｒｖｉｃｅ　ＳｕｂｓｃｒｉｂｅＡｃｋ、Ｓｔｏｐ　Ｏｆｆｅｒ、Ｓｔｏｐ　Ｓｕｂｓｃｒｉｂｅである、

請求項１から９のいずれか１項に記載の異常検知装置。

[請求項11] イーサネットで構成される車載ネットワークシステムにおける異常検知方法であって、前記異常検知方法は、

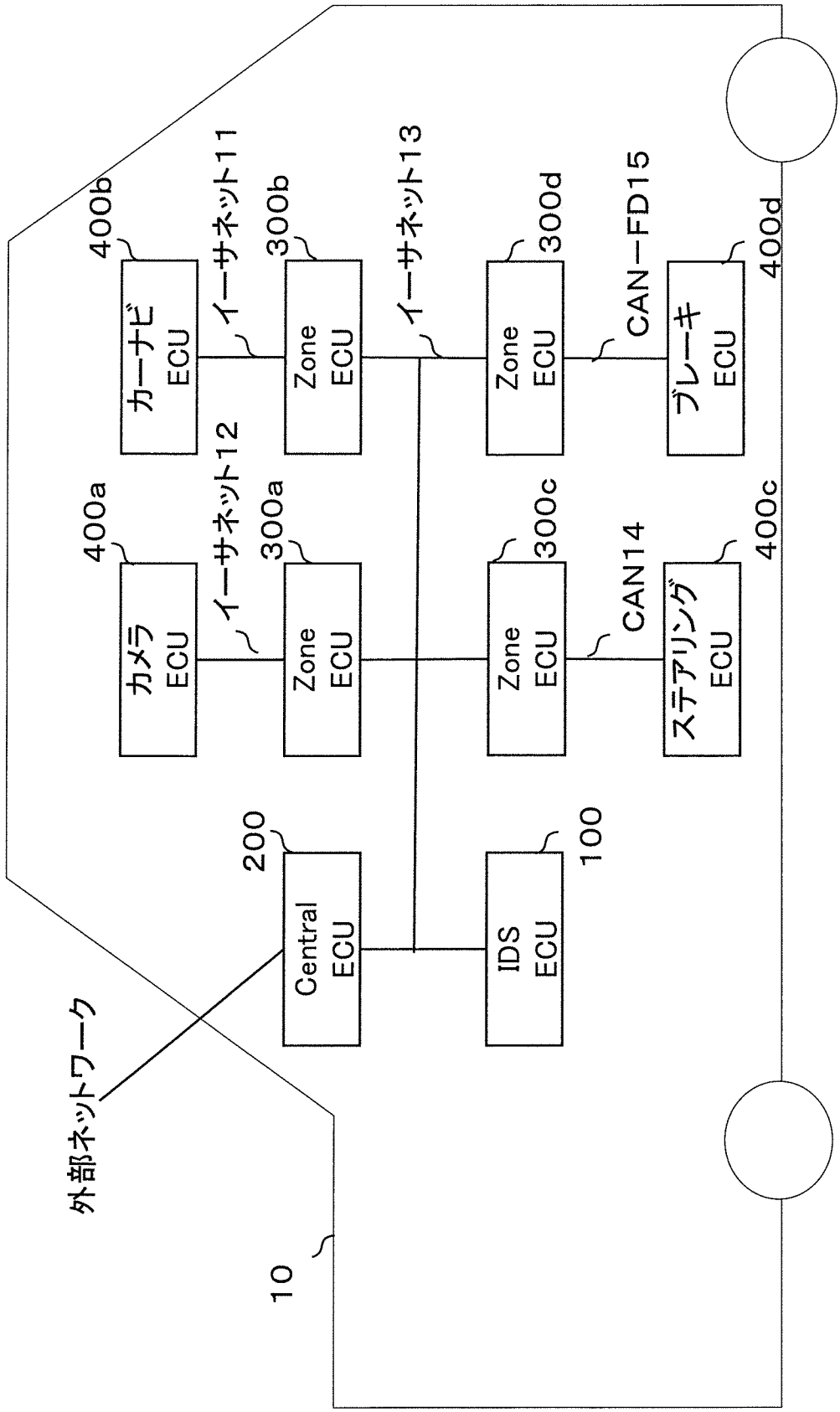
サービス指向型通信の通信確立フェーズにおける通信確立フレームを監視し、前記通信確立フレームに記載される通信ＩＤごとに、前記通信確立フレームに記載されるサーバーアドレスまたはクライアントアドレスを含む検知ルールを生成する検知ルール生成ステップと、

サービス指向型通信の通信フェーズにおける通信フレームを監視し、前記通信フレームに含まれる通信ＩＤと対応する前記検知ルールを参照し、前記通信フレームに記載されたサーバーアドレスまたはクライアントアドレスが、前記検知ルールに記載されたサーバーアドレスまたはクライアントアドレスと異なる場合に、前記通信フレームを異常フレームとして検知する異常検知ステップと、

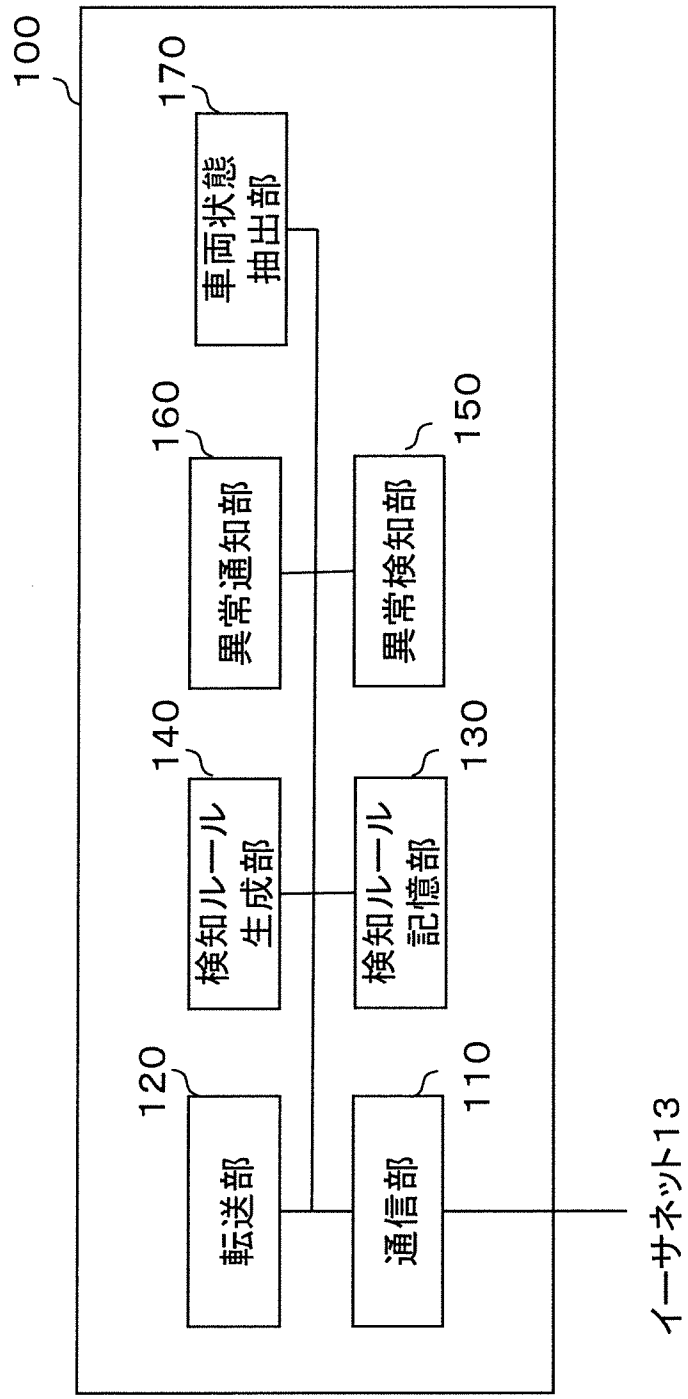
前記異常フレームを検知した場合に、異常を通知する異常通知ステップを備える、

異常検知方法。

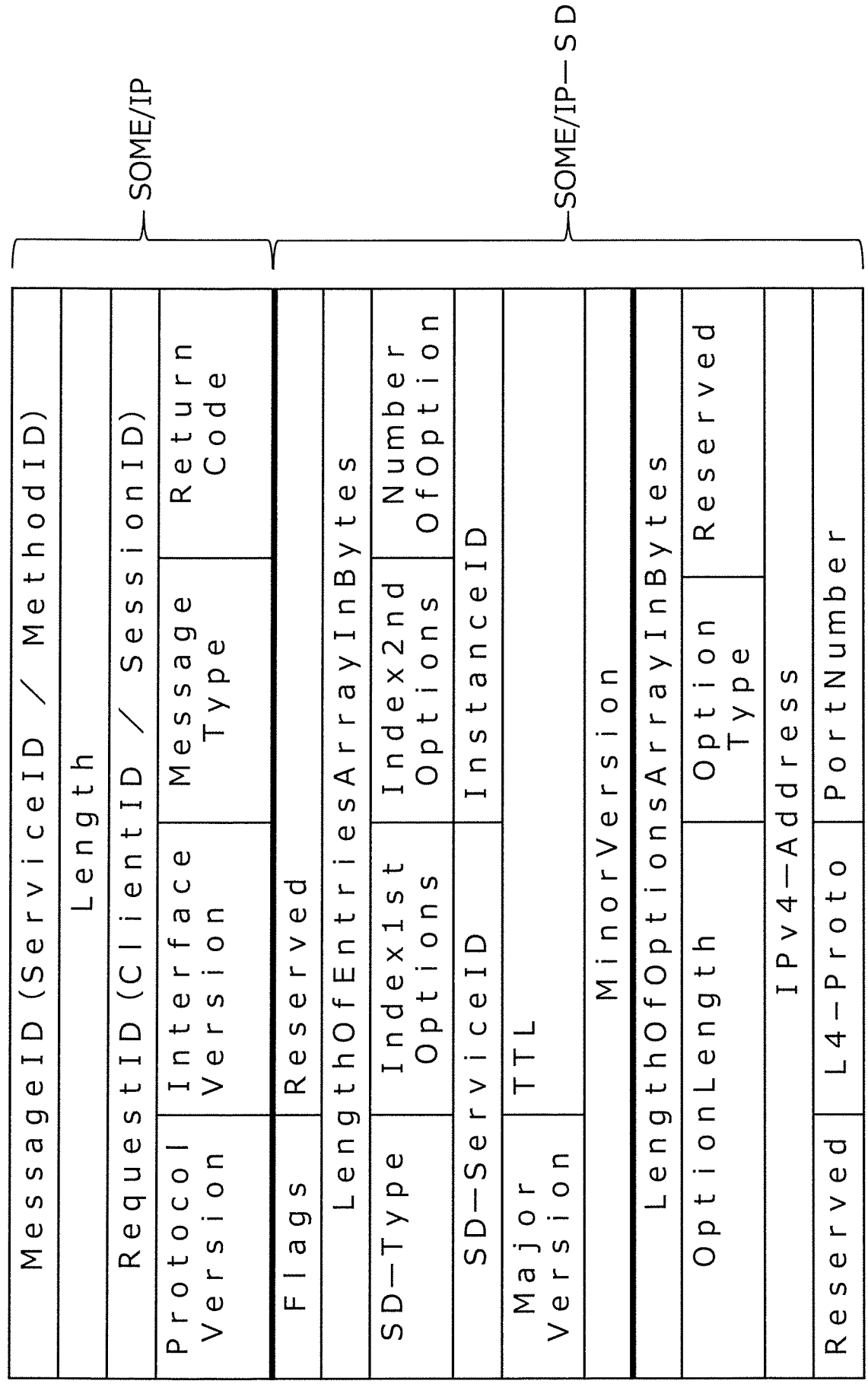
[図1]


400b
カーナビ ECU
イーサネット11
300b
Zone ECU
イーサネット13
300d
Zone ECU
CAN−FD15
ブレーキ ECU
400d
400a
カメラ ECU
イーサネット12
300a
Zone ECU
300c
Zone ECU
CAN14
ステアリング ECU
400c
200
Central ECU
100
IDS ECU
外部ネットワーク
10

[図2]


100
170
車両状態
抽出部
160
異常通知部
150
異常検知部
140
検知ルール
生成部
130
検知ルール
記憶部
120
転送部
110
通信部
イーサネット13

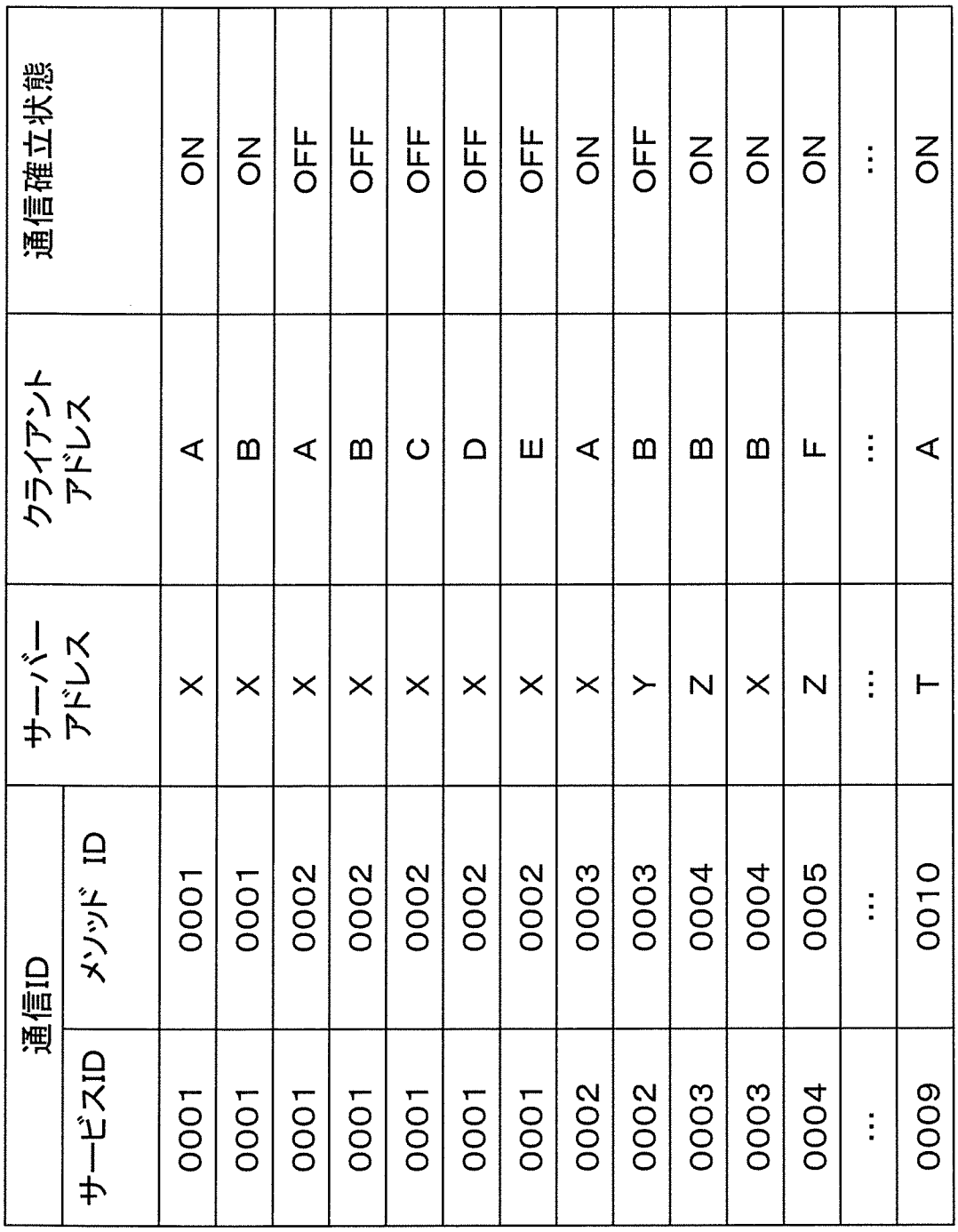
[図3]


SOME/IP
SOME/IP—SD
MessageID(ServiceID / MethodID)
Length
RequestID(ClientID / SessionID)
Protocol Version
Interface Version
Message Type
Return Code
Flags
Reserved
LengthOfEntriesArrayInBytes
SD—Type
Index1st Options
Index2nd Options
NumberOfOption
SD—ServiceID
InstanceID
Major Version
TTL
MinorVersion
LengthOfOptionsArrayInBytes
OptionLength
Option Type
Reserved
IPv4—Address
Reserved
L4—Proto
PortNumber

[図4]

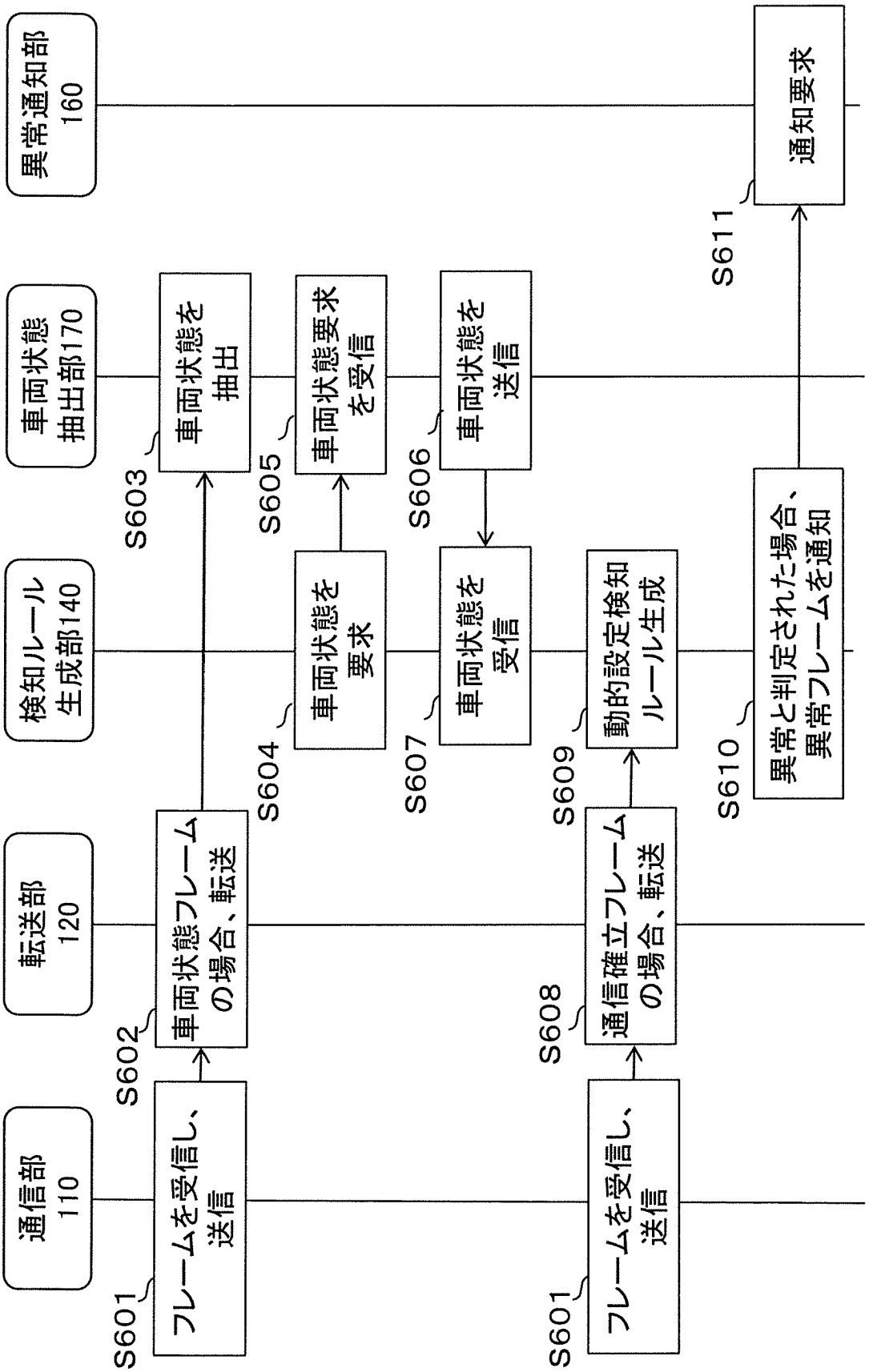
通信ID		サーバー数	クライアント数	車両状態	サービス内容
サービスID	メソッドID				
0001	0001	1	2	イグニションON状態	カメラ映像要求
0001	0002	1	5	ネットワーク接続ON状態 and パーキング状態 and 停止状態	ソフトアップデート要求
0002	0003	1	2	オートクルーズモード or オートパーキングモード	ハンドル制御指示
0003	0004	2	1	オートクルーズモード or オートパーキングモード or 人物検知	ブレーキ制御指示
0004	0005	1	1	-	車両状態
0009	0010	1	1	-	シフト変更要求
…	…	…	…	…	…

[図5]

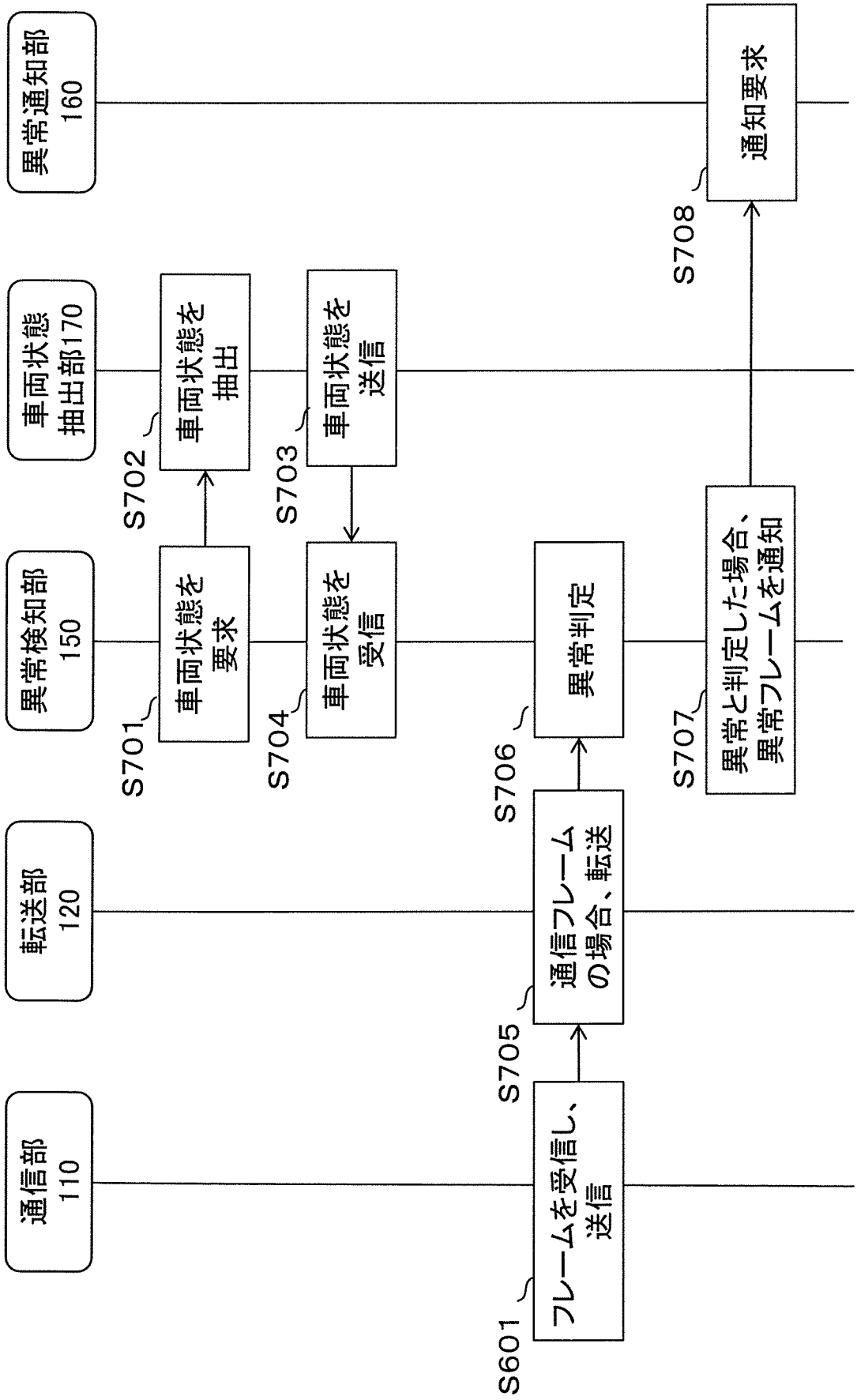


通信ID		サーバーアドレス	クライアントアドレス	通信確立状態
サービスID	メソッド ID			
0001	0001	X	A	ON
0001	0001	X	B	ON
0001	0002	X	A	OFF
0001	0002	X	B	OFF
0001	0002	X	C	OFF
0001	0002	X	D	OFF
0001	0002	X	E	OFF
0002	0003	X	A	ON
0002	0003	Y	B	OFF
0003	0004	Z	B	ON
0003	0004	X	B	ON
0004	0005	Z	F	ON
…	…	…	…	…
0009	0010	T	A	ON

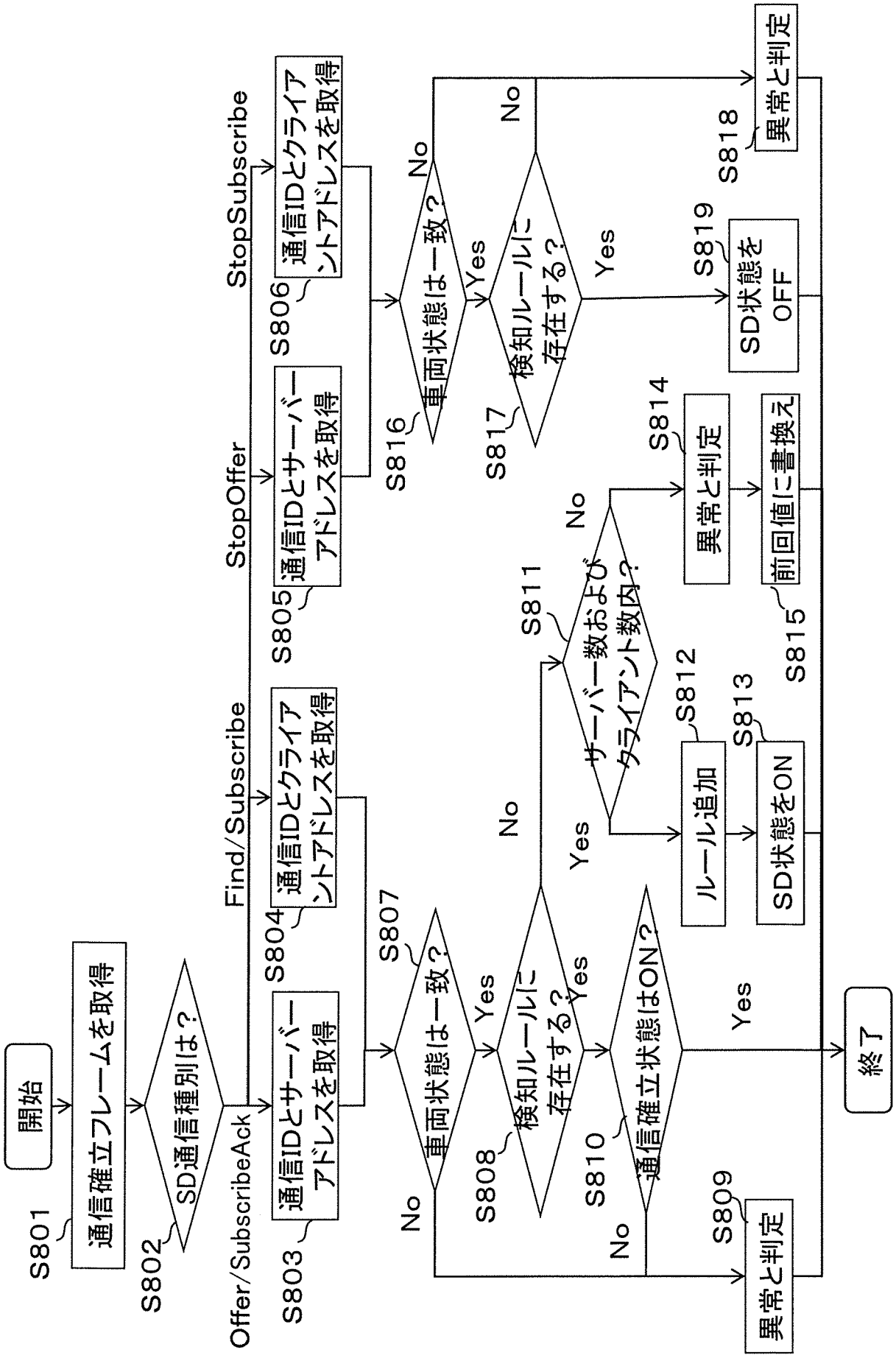
[図6]


通信部 110
転送部 120
検知ルール生成部140
車両状態抽出部170
異常通知部 160
S601
フレームを受信し、送信
S602
車両状態フレームの場合、転送
S603
車両状態を抽出
S604
車両状態を要求
S605
車両状態要求を受信
S606
車両状態を送信
S607
車両状態を受信
S608
通信確立フレームの場合、転送
S609
動的設定検知ルール生成
S610
異常と判定された場合、異常フレームを通知
S611
通知要求

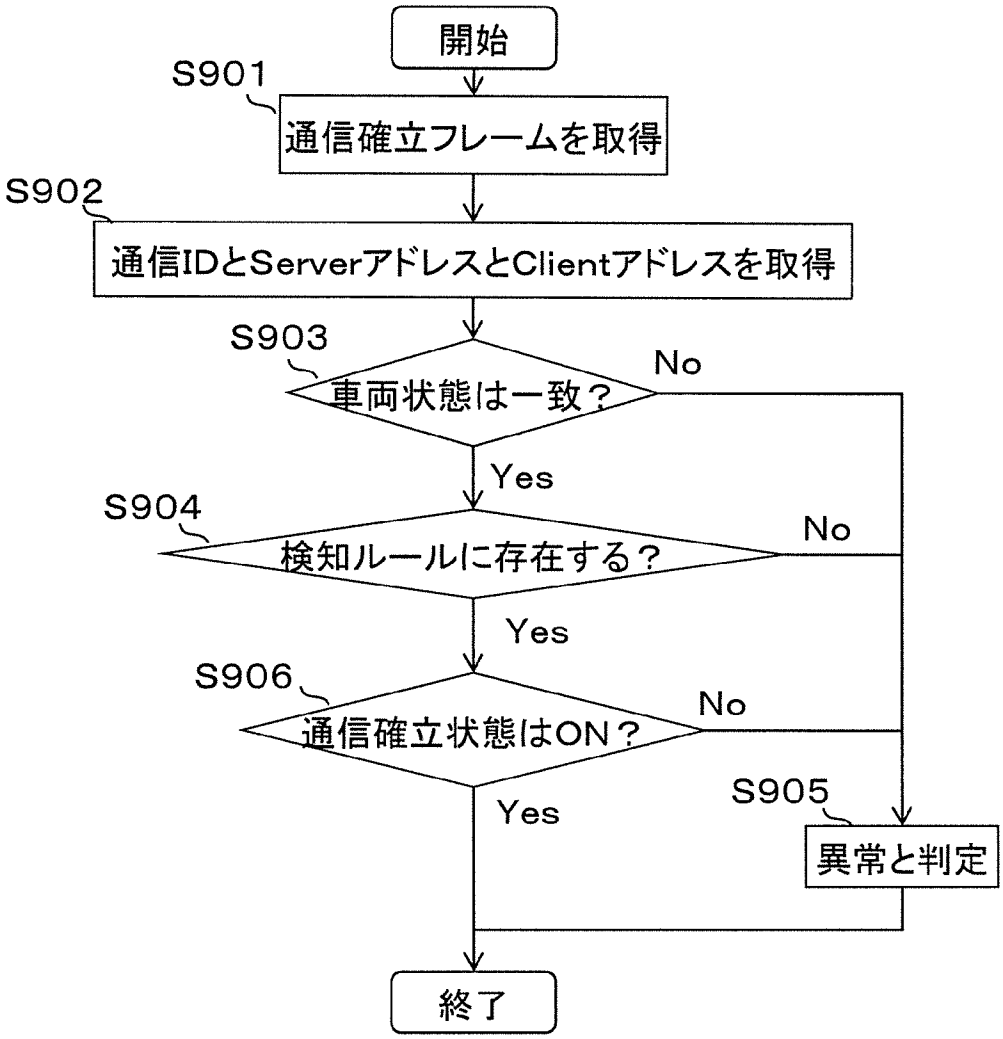
[図7]


異常通知部
160
車両状態
抽出部170
異常検知部
150
転送部
120
通信部
110
車両状態を
抽出
車両状態を
送信
車両状態を
要求
車両状態を
受信
異常判定
通信フレーム
の場合、転送
フレームを受信し、
送信
通知要求
異常と判定した場合、
異常フレームを通知
S601
S701
S702
S703
S704
S705
S706
S707
S708

[図8]


開始
S801
通信確立フレームを取得
S802
SD通信種別は？
Offer/SubscribeAck
S803
通信IDとサーバーアドレスを取得
S807
車両状態は一致？
No
S808
検知ルールに存在する？
No
S810
通信確立状態はON？
No
S809
異常と判定
Yes
終了
Find/Subscribe
S804
通信IDとクライアントアドレスを取得
S811
サーバー数およびクライアント数内？
No
S814
異常と判定
Yes
S812
ルール追加
S813
SD状態をON
S815
前回値に書換え
StopOffer
S805
通信IDとサーバーアドレスを取得
S816
車両状態は一致？
No
S817
検知ルールに存在する？
No
S818
異常と判定
Yes
StopSubscribe
S806
通信IDとクライアントアドレスを取得
S819
SD状態をOFF
Yes

[図9]


開始
S901
通信確立フレームを取得
S902
通信IDとServerアドレスとClientアドレスを取得
S903
車両状態は一致？
No
Yes
S904
検知ルールに存在する？
No
Yes
S906
通信確立状態はON？
No
Yes
S905
異常と判定
終了

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/026722

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. G06F21/31(2013.01)i, G06F21/62(2013.01)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. G06F21/31, G06F21/62

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)
IEEE Xplore

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2019/021402 A1 (PANASONIC INTELLECTUAL PROPERTY CORPORATION OF AMERICA) 31 January 2019 & WO 2019/021995 A1	1-11
A	JP 2018-190465 A (PANASONIC INTELLECTUAL PROPERTY CORPORATION OF AMERICA) 29 November 2018 & JP 2017-111796 A & US 2018/0295147 A1 & WO 2017/104112 A1 & EP 3393086 A1 & CN 107925600 A	1-11

☒ 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
30.07.2019	13.08.2019

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/026722

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2016/0142303 A1 (HYUNDAI MOTOR COMPANY) 19 May 2016 & DE 102015207483 A1 & CN 106209758 A & KR 10-1612819 B1	1-11

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１９／０２６７２２

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/31(2013.01)i, G06F21/62(2013.01)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.　G06F21/31, G06F21/62

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）

IEEE Xplore

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	WO 2019/021402 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）2019.01.31, & WO 2019/021995 A1	1-11
A	JP 2018-190465 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）2018.11.29, & JP 2017-111796 A & US 2018/0295147 A1 & WO 2017/104112 A1 & EP 3393086 A1 & CN 107925600 A	1-11

☑　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	国際調査報告の発送日
３０．０７．２０１９	１３．０８．２０１９

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
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）　５Ｓ　５３８０
和平　悠希
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	US 2016/0142303 A1 (HYUNDAI MOTOR COMPANY) 2016.05.19, & DE 102015207483 A1 & CN 106209758 A & KR 10-1612819 B1	1-11