

(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12月12日(12.12.2024)



(10) 国際公開番号

WO 2024/252705 A1

(51) 国際特許分類:
G06F 21/60 (2013.01)

(21) 国際出願番号: PCT/JP2024/000034

(22) 国際出願日: 2024年1月5日(05.01.2024)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2023-095150 2023年6月9日(09.06.2023) JP

(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).

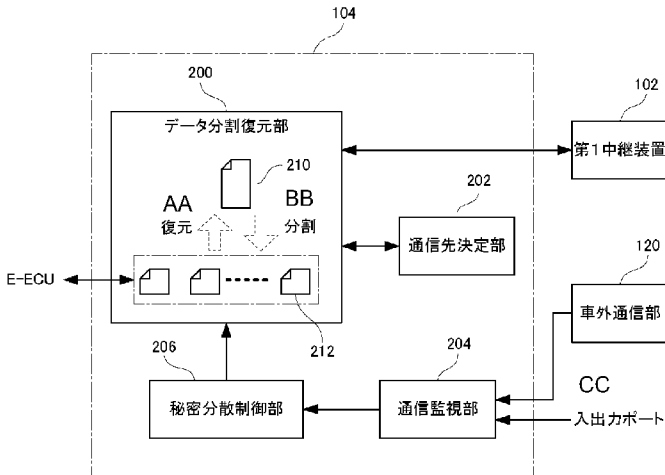
(74) 代理人: 清水 敏, 外 (SHIMIZU, Satoshi et al.); 〒5300002 大阪府大阪市北区曽根崎新地二丁目5番3号 堂島TSSビル4階 堂島特許事務所北新地支所内 Osaka (JP).

(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, 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,

(54) Title: COMMUNICATION PLANNING DEVICE, CONTROL METHOD, AND COMPUTER PROGRAM

(54) 発明の名称: 通信計画装置、制御方法およびコンピュータプログラム

[図2]



102... First relay device
120... Vehicle external communication unit
200... Data splitting/restoration unit
202... Communication destination determination unit
204... Communication monitoring unit
206... Secret sharing control unit
AA ... Restoration
BB ... Splitting
CC ... Input/output port

(57) Abstract: This communication planning device is mounted on a system including a first device, a second device, and a communication device, and includes: a planning unit that plans communication of predetermined information between the first device and the second device; and a detection unit that detects state specification information required for the planning unit to plan communication. The planning unit plans communication of a plurality of pieces of split information between the first device and the second device on the basis of the result of detection by the detection unit, and the split information is information generated by splitting the predetermined information.

LY, MA, MD, MG, MK, MN, MU, MW, MX, MY,
MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL,
PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK,
SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

一 国際調査報告 (条約第21条(3))

(57) 要約：通信計画装置は、第1装置、第2装置および通信装置を含むシステムに搭載される通信計画装置であって、第1装置および第2装置の間における所定情報の通信を計画する計画部と、計画部が通信を計画するために必要となる状態特定情報を検知する検知部とを含み、計画部は、検知部による検知結果に基づいて、第1装置および第2装置の間における複数の断片化情報の通信を計画し、断片化情報は、所定情報が分割されることにより生成される情報である。

明 細 書

発明の名称：

通信計画装置、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、通信計画装置、制御方法およびコンピュータプログラムに関する。本出願は、2023年6月9日出願の日本出願第2023-095150号に基づく優先権を主張し、前記日本出願に記載された全ての記載内容を援用するものである。

背景技術

[0002] 車載システムにおいてセキュリティは重要である。そのために、情報の秘匿化が行われる。秘匿化の方法として暗号化が一般に知られているが、それ以外の方法として秘密分散法がある。秘密分散法は、保護対象データを分散させて管理することにより、情報の秘匿化を実現する。

[0003] 下記特許文献1には、全ノードペア間にフルメッシュのセキュアな通信路が存在するネットワークにおいて、秘密分散法を用いて秘密情報を複数のノード群に分散して保持する分散情報転送システムが開示されている。この分散情報転送システムは、攻撃者が操作するノードが複数存在する場合に、第1のシェアを再度分散して配布することによって、攻撃者が必要十分なシェアを収集することを防ぎ、セキュアな状態を維持する。

先行技術文献

特許文献

[0004] 特許文献1：特開2012-100140号公報

発明の概要

[0005] 本開示のある局面に係る通信計画装置は、第1装置、第2装置および通信装置を含むシステムに搭載される通信計画装置であって、第1装置および第2装置の間における所定情報の通信を計画する計画部と、計画部が通信を計画するために必要となる状態特定情報を検知する検知部とを含み、計画部は

、検知部による検知結果に基づいて、第1装置および第2装置の間における複数の断片化情報の通信を計画し、断片化情報は、所定情報が分割されることにより生成される情報である。

図面の簡単な説明

[0006] [図1]図1は、本開示の実施形態に係る車載システムの構成を示すブロック図である。

[図2]図2は、図1に示した第2中継装置の機能的構成を示すブロック図である。

[図3]図3は、図1に示した第2中継装置により実行される処理を示すフローチャートである。

[図4]図4は、第1変形例に係る第2中継装置の機能的構成を示すブロック図である。

[図5]図5は、セキュリティ強度を決定するために考慮される通信情報をテーブル形式により示す図である。

[図6]図6は、セキュリティ強度を決定するために考慮される空きポートの情報および想定外の通信装置の接続の有無をテーブル形式により示す図である。

[図7]図7は、第1変形例に係る第2中継装置により実行される処理を示すフローチャートである。

[図8]図8は、第1変形例に係る車載システムの構成例を示すブロック図である。

[図9]図9は、第2変形例に係る第2中継装置の機能的構成を示すブロック図である。

[図10]図10は、第2変形例に係る第2中継装置により実行される処理を示すフローチャートである。

発明を実施するための形態

[0007] [本開示が解決しようとする課題]

特許文献1においては、通信経路がセキュアであることを前提としている

が、現実には通信経路がセキュアでない場合が存在する。その場合には、特許文献 1 に開示された技術によっては、通信経路において不正アクセスにより情報漏洩する危険性を回避できない問題がある。

[0008] したがって、本開示は、秘密情報を複数に分割して複数のノードに保存する情報管理において、分割された情報を通信する際に漏洩および改竄の発生を防止できる通信計画装置、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。

[0009] [本開示の効果]

本開示によれば、秘密情報を複数に分割して複数のノードに保存する情報管理において、分割された情報を通信する際に漏洩および改竄の発生を防止できる通信計画装置、制御方法およびコンピュータプログラムを提供できる。

[0010] [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。

[0011] (1) 本開示の第 1 の局面に係る通信計画装置は、第 1 装置、第 2 装置および通信装置を含むシステムに搭載される通信計画装置であって、第 1 装置および第 2 装置の間における所定情報の通信を計画する計画部と、計画部が通信を計画するために必要となる状態特定情報を検知する検知部とを含み、計画部は、検知部による検知結果に基づいて、第 1 装置および第 2 装置の間における複数の断片化情報の通信を計画し、断片化情報は、所定情報が分割されることにより生成される情報である。これにより、所定情報（例えば、秘密にすべき情報（以下、秘密情報という））を複数に分割して複数の装置に保存する情報管理において、分割された情報である断片化情報を通信する際に漏洩および改竄の発生を防止できる。

[0012] (2) 上記 (1) において、状態特定情報は、通信装置によるシステム外との通信である外部通信の通信状態、通信計画装置および第 1 装置の各々が有する入出力ポートの状態、ならびに、システム内の通信経路への想定外の

通信装置の接続の有無のうちの少なくともいずれかの状態を表す情報を含む。これにより、断片化情報を通信する際に漏洩および改竄の発生をより防止できる。

[0013] (3) 上記(1)または(2)において、計画部は、検知結果に基づいて複数の断片化情報の通信を行わないとの計画になる場合においては、第1所定期間が経過すれば、複数の断片化情報を通信するように計画することができる。これにより、複数の断片化情報を通信できない状態がいつまでも持続することを回避できる。

[0014] (4) 上記(3)において、第1所定期間は、複数の断片化情報の通信を必要とする機能のリアルタイム性に基づいて決定されてもよい。これにより、機能に要求されるリアルタイム性が損なわれることを回避できる。

[0015] (5) 上記(1)から(4)のいずれか1つにおいて、通信計画装置は、システムからの情報漏洩に関するセキュリティ強度を評価するセキュリティ強度評価部をさらに含んでもよく、計画部は、検知結果に基づいて複数の断片化情報の通信を行わないとの計画になる場合においては、セキュリティ強度評価部により評価されたセキュリティ強度が所定レベル以上であれば、複数の断片化情報を通信するように計画してもよい。これにより、複数の断片化情報の通信が、必要以上に抑制されることを回避でき、情報漏洩の危険度に応じて、複数の断片化情報の通信を制御できる。

[0016] (6) 上記(5)において、セキュリティ強度評価部は、検知部による検知結果に基づいて、セキュリティ強度を評価してもよい。これにより、セキュリティ強度を適切に評価できる。

[0017] (7) 上記(1)から(6)のいずれか1つにおいて、通信計画装置は、通信装置に、通信装置によるシステム外との通信である外部通信を制限させる通信制御部をさらに含んでもよく、計画部は、外部通信が制限可能であれば、通信制御部に、第2所定期間において外部通信を制限させ、第2所定期間において、複数の断片化情報を通信するように計画してもよい。これにより、複数の断片化情報を通信できない状態がいつまでも持続することを

回避できる。

- [0018] (8) 上記(7)において、計画部は、外部通信が、リアルタイム性が要求される機能のために実行されていなければ、外部通信が制限可能であると判定してもよい。これにより、機能に要求されるリアルタイム性が損なわれることを回避しつつ、複数の断片化情報を通信できる。
- [0019] (9) 上記(7)において、計画部は、外部通信において所定量のデータがバッファに記憶されてから当該データの利用が終了するまでの期間が、複数の断片化情報の通信に要する期間よりも長ければ、外部通信が制限可能であると判定してもよい。これにより、外部通信を実行している機能に影響することなく、複数の断片化情報を通信できる。
- [0020] (10) 上記(1)から(9)のいずれか1つにおいて、通信計画装置は、所定情報を複数の断片化情報に分割する情報処理部をさらに含んでもよく、所定情報は、第1装置から通信計画装置を介して第2装置に送信されてもよく、情報処理部は、秘密分散法により断片化情報を生成してもよい。これにより、情報の漏洩および改竄の発生をより防止できる。
- [0021] (11) 上記(10)において、通信計画装置は、複数の第2装置の中から、複数の断片化情報の個数以下の個数の通信先装置を決定する通信先決定部をさらに含んでもよく、複数の断片化情報は、通信先装置と通信計画装置との間において、計画部による計画に基づいて通信されてもよい。これにより、情報の漏洩および改竄の発生をより一層防止できる。
- [0022] (12) 上記(11)において、通信先決定部は、第1装置から通信計画装置に所定情報の要求が入力されたことを受けて、複数の通信先装置の中から、断片化情報を受信する複数の相手装置を決定してもよく、通信計画装置は、複数の相手装置から受信した断片化情報から、所定情報を生成する復元部をさらに含んでもよい。これにより、複数の第2装置に分散させて記憶している断片化情報から所定情報を生成して第1装置に提供できる。
- [0023] (13) 上記(1)から(12)のいずれか1つにおいて、通信計画装置は、車両に搭載されていてもよい。これにより、車両における所定情報(例

例えば秘密情報）を複数に分割して複数の第２装置に保存する情報管理において、断片化情報を通信する際に漏洩および改竄の発生を防止できる。

[0024] （１４）本開示の第２の局面に係る制御方法は、第１装置、第２装置および通信装置を含むシステムにおける第１装置および第２装置間の通信の制御方法であって、制御部が、第１装置および第２装置の間における所定情報の通信を計画する計画ステップと、制御部が、計画ステップにより通信が計画されるために必要となる状態特定情報を検知する検知ステップとを含み、計画ステップは、制御部が、検知ステップによる検知結果に基づいて、第１装置および第２装置の間における複数の断片化情報の通信を計画するステップを含み、断片化情報は、所定情報が分割されることにより生成される情報である。これにより、所定情報（例えば秘密情報）を複数に分割して複数の第２装置に保存する情報管理において、分割された情報である断片化情報を通信する際に漏洩および改竄の発生を防止できる。

[0025] （１５）本開示の第３の局面に係るコンピュータプログラムは、第１装置、第２装置および通信装置を含むシステムに搭載されるコンピュータに、第１装置および第２装置の間における所定情報の通信を計画する計画機能と、計画機能により通信が計画されるために必要となる状態特定情報を検知する検知機能とを実行させ、計画機能は、検知機能による検知結果に基づいて、第１装置および第２装置の間における複数の断片化情報の通信を計画する機能を含み、断片化情報は、所定情報が分割されることにより生成される情報である。これにより、所定情報（例えば秘密情報）を複数に分割して複数の第２装置に保存する情報管理において、分割された情報である断片化情報を通信する際に漏洩および改竄の発生を防止できる。

[0026] [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。

[0027] （全体構成）

図1を参照して、本開示の実施形態に係る車載システム100は、車両に搭載される。車載システム100は、第1中継装置102と、第2中継装置104と、E-ECU(End-Electronic Control Unit)106、E-ECU108およびE-ECU110と、車外通信部120と、バス122とを含む。第1中継装置102は、例えばC-ECU(Central-Electronic Control Unit)である。第2中継装置は、例えば、Z-ECU(Zone-Electronic Control Unit)である。外部装置130は、例えば、サーバコンピュータ(以下、単にサーバという)、路側装置および他車両の車載装置である。車載システム100は、車外通信部120を介して外部装置130と通信し、種々の情報(交通情報および運転者を支援する情報(以下、運転支援情報という))を受信する。車載システム100は、外部装置130から取得した情報と、車載システム100が搭載された車両(以下、自車両という)に搭載されているセンサから得られた情報とを用いて、種々の機能を実現する。例えば、車載システム100は、自車両の運転者に運転支援情報を提示する。自車両が自動運転可能であれば、車載システム100は自動運転を実現する。

[0028] 車外通信部120は、搭載されている車載システム100と、その外部(即ち外部装置130)との双方向通信を行う。例えば、車外通信部120は、広域無線通信(4Gおよび5G等)および近接無線通信(Wi-FiおよびBluetooth(登録商標)等)を行う。

[0029] 第2中継装置104は、制御部140およびメモリ142を含み、通信計画装置として機能する。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。また、第2中継装置104は、複数の入出力

ポートを含む。図1においては、代表的に入出力ポート144および入出力ポート146を示している。入出力ポートは、車載システム100の試験および調整等のための機器が接続され得る。

[0030] 第2中継装置104は、車外通信部120およびE-ECU106、E-ECU108およびE-ECU110等との間のデータ交換を調整する。即ち、第2中継装置104は、外部装置130から車外通信部120を介して受信されたデータを、そのデータを必要とするE-ECUに、バス122を介して伝送する。また、第2中継装置104は、E-ECUのデータ（例えば、車載センサのセンサデータ）を、バス122を介して取得し、車外通信部120を介してそのデータを必要とする外部装置130に送信する。なお、第2中継装置104と、E-ECU106、E-ECU108およびE-ECU110等との間の通信は、バスではなくワイヤーハーネスを介して行われてもよい。

[0031] 車載システム100は、複数のE-ECUを含み、図1においては、代表的にE-ECU106、E-ECU108およびE-ECU110を示す。各E-ECUは、車載システム100の機能（車両走行の制御、車載センサの制御等）を実現するための回路であり、制御部およびメモリを含む。例えば、エンジン制御ECU、ストップスタート制御ECU、トランスミッション制御ECU、エアバッグ制御ECU、パワーステアリング制御ECU、ハイブリッド制御ECU等がある。自動運転可能な車両には、自動運転用ECUも搭載されている。自動運転用ECUは、適宜外部と通信し、必要な情報（交通情報および運転支援情報）の取得を行う。車外通信部120を介して、外部装置130から受信した情報は、例えば、自動運転用ECUにより利用される。車載センサの制御を担うE-ECUにより取得されたセンサデータは、第2中継装置104および車外通信部120を介して、外部装置130（例えばサーバまたは他車両）に送信され、運転支援情報の生成等に利用される。

[0032] 第1中継装置102は、第2中継装置104と同様に、制御部およびメモ

りを含み、車載システム１００の機能を実現するためのプログラムを実行する。また、第１中継装置１０２は、第２中継装置１０４と同様に複数の入出力ポートを備え得る。

[0033] 例えば、外部装置１３０は、車両用電子キー（以下、単に電子キーという）を含み、車外通信部１２０は電子キーを通信する機能を有し、第１中継装置１０２は電子キーを認識する。ユーザは、電子キーを所持して自車両から所定範囲内（車室内を含む）にいれば、ドアの施錠および開錠、車両の電源のオン、ならびにエンジンの始動等が可能になる。また、第１中継装置１０２は、ユーザによる電子キーの操作に応じたコードを、車外通信部１２０を介して受信し、コードに応じて、自車両のドアの施錠および開錠、ならびにスライドドアの自動開閉等を行う。

[0034] 車載システム１００において、秘密情報を管理することがある。例えば、上記した電子キーによる操作を実現するには、自車両用の電子キーを適切に認識することが必要になる。そのために、電子キーと車載システム１００との間において、一意に定められたＩＤ（以下、認証用ＩＤという）が交換される。具体的には、電子キーが、電子キーに記憶されている認証用ＩＤを送信し、車載システム１００は、受信した認証用ＩＤが、車載システム１００が記憶している認証用ＩＤと一致するか否かを判定する。一致すれば、ユーザは、車両に対して上記した操作が可能になる。この認証用ＩＤは秘密情報であり、車載システム１００は、秘密情報を安全に長期間管理する役割を担う。生体情報（例えば、指紋および顔画像）および個人情報（氏名、住所、電話番号および電子メールアドレス等）を車載システム１００に登録することにより、種々の機能を提供する場合、それらの情報も秘密情報であり、安全に管理される必要がある。

[0035] （秘密情報の管理）

秘密情報の管理における第２中継装置１０４の機能に関して説明する。図２を参照して、第２中継装置１０４は、データ分割復元部２００、通信先決定部２０２、通信監視部２０４および秘密分散制御部２０６を含む。各部は

、図1に示した制御部140およびメモリ142により実現される。データ分割復元部200は、第1中継装置102からの要求を受けて、要求に対応する処理を実行する。即ち、データ分割復元部200は、情報の秘匿を要求するコード（以下、秘匿要求という）が入力されると、それと共に入力される対象データ210（秘匿の対象情報であり、例えば秘密情報）を、一点鎖線内に示すように複数の断片化情報212に分割する。その後、データ分割復元部200は、後述する秘密分散制御部206からの指示を受けて、複数の断片化情報212を複数のE-E C U（例えば、E-E C U 108およびE-E C U 110）に送信し、各E-E C Uに記憶させる。複数（例えばn個）の断片化情報212は、通信先決定部202により決定された、断片化情報212の数と同数の複数（n個）のE-E C Uに、1対1に送信される。なお、断片化情報212から対象データ210が復元されるので、対象データ210を元データともいう。対象データ210を断片化情報212に分割するには、任意の方法を用いることができ、例えば、秘密分散法を用いることができる。したがって、「分割」とは、1つの対象データを複数のデータに単に分ける場合に限らず、データの変換および付加を伴い、複数のデータを生成することを意味する。E-E C Uに送信された断片化情報212は、元データと共に、データ分割復元部200（図1のメモリ142）から速やかに消去される。

[0036] また、データ分割復元部200は、第1中継装置102から元データを要求するコード（以下、復元要求という）が入力されると、対応する断片化情報212を記憶しているE-E C Uから断片化情報212を取得する。具体的には、データ分割復元部200は、断片化情報212を記憶しているE-E C Uに、断片化情報212の送信を要求する。データ分割復元部200は、E-E C Uから受信した複数の断片化情報212から元データを復元する。断片化情報212が秘密分散法（例えば（k，n）しきい値法）により生成されていれば、データ分割復元部200は、元データを分割した断片化情報の数（n個）よりも少ない数（k個）の断片化情報をE-E C Uから取得

できれば、元データを復元できる。データ分割復元部 200 は、復元した元データを第 1 中継装置 102 に送信した後、データ分割復元部 200（図 1 のメモリ 142）から速やかに元データおよび断片化情報 212 を消去する。

[0037] 複数の秘密情報を管理する場合、第 1 中継装置 102 は、データ分割復元部 200 に対して、対象データ 210 を特定する情報（以下、元データ特定情報という）を付した秘匿要求を送信すればよい。データ分割復元部 200 は、元データ特定情報と、それに対応する対象データ 210 を分割した断片化情報（秘密分散法におけるシェア）を送信した E-E C U を特定する情報（以下、E-E C U 特定情報という）を対応させたテーブルを記憶しておけば、そのテーブルを参照して、断片化情報を取得する E-E C U を特定できる。

[0038] 通信先決定部 202 は、データ分割復元部 200 からの指示を受けて、複数の断片化情報 212 の各々を 1 対 1 に記憶させる E-E C U を決定する。通信先決定部 202 は、自車両に搭載されており、第 2 中継装置 104 と通信可能である複数の E-E C U の中から、複数の断片化情報 212 と同数の E-E C U を通信先装置として決定する。通信先決定部 202 は、決定した通信先装置（E-E C U）を特定する情報を記憶する。通信先装置の決定方法は任意であり、通信先決定部 202 は、所定の規則に従って通信先装置を決定しても、ランダムに通信先装置を決定してもよい。また、通信先決定部 202 は、各 E-E C U の特性（各 E-E C U の機能に要求されるリアルタイム性およびメモリ容量等）を考慮して通信先装置を決定してもよい。

[0039] 通信監視部 204 は、車外通信部 120 の通信状態、複数の入出力ポートのうちの空きポート（例えば、入出力ポート 144 および入出力ポート 146）の状態、および、想定外の通信装置の接続の有無を監視する。通信監視部 204 は、検知した車外通信部 120 の通信状態、空きポートの状態および想定外の通信装置の有無を表す情報（以下、状態特定情報という）を秘密分散制御部 206 に出力する。通信監視部 204 は、車外通信部 120 の通

信状態、空きポートの状態および想定外の通信装置の有無の検知部といえる。通信監視部204は、最新の状態特定情報を記憶し、秘密分散制御部206からの要求を受けて、状態特定情報を秘密分散制御部206に出力してもよい。車外通信部120の通信状態とは、車外通信部120が外部装置130と通信しているか否かを意味する。空きポートの状態とは、基本的には、機器の接続の有無を意味する。なお、車外通信部120の通信状態には、車外通信部120が通信している場合、通信の種類（例えば、広域無線通信、近接無線通信および有線通信）および通信速度（例えばMbps単位）等が含まれてもよい。空きポートの状態には、機器が接続されている場合、その機器の性質が含まれてもよい。また、車載システム100を構成する各部間（例えば、第1中継装置102および第2中継装置104の間）がワイヤーハーネスにより接続されている場合、そのワイヤーハーネスが加工され、想定外の通信装置が接続される可能性がある。したがって、通信監視部204は、想定外の通信装置の接続の有無、即ち、自車両内の通信経路に、想定外の通信装置が接続されているか否かを監視する。これらは、情報漏洩の可能性に関する情報である。

[0040] 秘密分散制御部206は、データ分割復元部200が、通信先決定部202により決定された通信先装置（E-ECU）と、断片化情報の通信を行うタイミングを制御する。「断片化情報の通信」には、データ分割復元部200が、断片化情報212を通信先装置に送信する通信と、データ分割復元部200が、通信先装置に記憶されている断片化情報212を受信する通信との両方が含まれる。秘密分散制御部206は、通信監視部204から入力される状態特定情報から、現在の車外通信部120の通信状態、空きポートの接続状態および想定外の通信装置の接続の有無を特定し、それに応じて、断片化情報の通信を行うか否かを決定する（通信を計画）。秘密分散制御部206は、断片化情報を通信すると決定した場合、データ分割復元部200に通信を指示し、データ分割復元部200は、断片化情報の通信を実行する。

[0041] 例えば、車外通信部120が外部通信（外部装置130との通信）を行っ

ておらず、入出力ポートの空きポートに機器の接続がなく、想定外の通信装置の接続が存在しなければ、情報漏洩の危険性はないまたは比較的低い（以下、安全状態という）。したがって、データ分割復元部 200 は、断片化情報の通信を行うと決定する。車外通信部 120 が外部通信（外部装置 130 との通信）中である、入出力ポートの空きポートに機器が接続されている、または、想定外の通信装置の接続が存在する場合、情報漏洩の危険性は比較的高い（以下、危険状態という）。したがって、データ分割復元部 200 は、断片化情報の通信を決定しない。危険状態が続く場合、データ分割復元部 200 が複数の断片化情報を記憶していることは安全ではない。また、第 1 中継装置 102 から元データとして、電子キーの ID を要求されている場合、速やかに、E-ECU から断片化情報を取得して復元し、第 1 中継装置 102 に出力する必要がある。したがって、所定期間待機した後は、危険状態が続いていても、データ分割復元部 200 は、断片化情報の通信を行うと決定してもよい。この所定期間（第 1 所定期間）は、第 1 中継装置 102 が要求する元データを利用する第 1 中継装置 102 の機能の特性（例えばリアルタイム性）に基づいて決定されていけばよい。要求されるリアルタイム性が高い場合には、所定期間を比較的小短く設定する。要求されるリアルタイム性が低い場合には、所定期間を比較的小長く設定できる。

[0042] これにより、第 2 中継装置 104 は、安全状態において、E-ECU と断片化情報を通信でき、断片化情報の通信過程において、断片化情報が車外に漏洩することを抑制できる。また、危険状態であっても、第 1 中継装置 102 が提供する機能のリアルタイム性を損なわないように、E-ECU と断片化情報を通信でき、第 1 中継装置 102 の機能に支障が生じることを回避できる。

[0043] （第 2 中継装置の動作）

図 3 を参照して、第 2 中継装置 104 の動作に関してさらに説明する。図 3 に示した処理は、図 1 に示した第 2 中継装置 104 の制御部 140 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、制御部１４０は、本プログラムと並行して、図２に示した通信監視部２０４の機能を実現するためのプログラムを実行している。即ち、本プログラムは、図２に示したデータ分割復元部２００、通信先決定部２０２および秘密分散制御部２０６の機能を実現するためのものである。断片化情報の生成には秘密分散法が用いられる。

[0044] ステップ３００において、制御部１４０は、第１中継装置１０２からの要求を受信したか否かを判定する。第１中継装置１０２から第２中継装置１０４には、上記したように、秘匿要求または復元要求が出力される。要求を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３２４に移行する。これにより、本プログラムが実行されている間、制御部１４０は、第１中継装置１０２からの要求を待ち受ける。なお、上記したように、第１中継装置１０２は、秘匿要求を出力する場合、秘匿の対象データも出力する。したがって、制御部１４０は、秘匿要求と共に、対象データを受信する。

[0045] ステップ３０２において、制御部１４０は、ステップ３００により受信された要求が秘匿要求であるか否かを判定する。秘匿要求であると判定された場合、制御はステップ３０４に移行する。そうでなければ（即ち、復元要求を受信）、制御はステップ３０８に移行する。

[0046] ステップ３０４において、制御部１４０は、複数のＥ－ＥＣＵの中から、後述のステップにおいて生成されるシェア（断片化情報）を記憶させるＥ－ＥＣＵを、通信先装置として決定する。その後、制御はステップ３０６に移行する。

[0047] ステップ３０６において、制御部１４０は、上記したように、ステップ３００により受信した対象データを複数のシェアに分割する。制御部１４０は、秘密分散法により、対象データから複数のシェアを生成する。その後、制御はステップ３１０に移行する。

[0048] ステップ３００により受信された要求が復元要求であれば、ステップ３０８において、制御部１４０は、複数のＥ－ＥＣＵの中から、要求される元デ

ータを復元するためのシェアを記憶しているE-E C Uを、収集先装置（シェアを取得する相手装置）として決定する。その後、制御はステップ310に移行する。1つの秘密情報を扱う場合、通信先装置と収集先装置とは同じE-E C Uを含む。複数の秘密情報を扱う場合、制御部140は、上記したように、復元要求と共に元データ特定情報を受信し、元データ特定情報とE-E C U特定情報とを対応させたテーブルを参照して、収集先装置を決定できる。秘密分散法（例えば（ k ， n ）しきい値法）によりシェアが生成された場合、シェアの個数は n であるのに対して、収集されるシェアの個数は n 以下の k であればよい。

[0049] ステップ310において、制御部140は、状態特定情報を取得する。その後、制御はステップ312に移行する。状態特定情報は、上記したように、車外通信状態、ポート接続状態および想定外の通信装置の接続の有無を表す情報を含む。状態特定情報は、図2に示した通信監視部204による監視により得られる情報である。通信監視部204の機能は、上記したように、本プログラムと並行して制御部140が実行しているプログラムにより、実現される。状態特定情報は、例えば、メモリ142の所定領域を介して、本プログラムに渡される。

[0050] ステップ312において、制御部140は、ステップ310により取得された状態特定情報により表される車外通信状態、空きポートの状態および想定外の通信装置の接続の有無が、上記した安全状態であるか否かを判定する。安全状態であると判定された場合、制御はステップ316に移行する。そうでなければ、制御はステップ314に移行する。

[0051] ステップ314において、制御部140は、所定期間が経過したか否かを判定する。経過したと判定された場合、制御はステップ316に移行する。そうでなければ、制御はステップ310に戻り、ステップ310およびステップ312が繰返される。所定期間は、上記したように、第1中継装置102が要求する元データを利用する第1中継装置102の機能の特性（例えばリアルタイム性）に基づいて決定されていけばよい。

- [0052] ステップ316において、制御部140は、ステップ302と同様の処理を実行する。秘匿要求であると判定された場合、制御はステップ318に移行する。そうでなければ（即ち、復元要求を受信）、制御はステップ320に移行する。
- [0053] ステップ318において、制御部140は、ステップ306により生成された複数のシェアを、ステップ304により決定された通信先装置（E-E C U）に送信する。このとき、1つの通信先装置には、1つのシェアが送信されても複数のシェアが送信されてもよい。但し、1つのシェアが複数の通信先装置に重複して送信されないようにする。また、1つの通信先装置に複数のシェアを送信する場合、1つの通信先装置に送信した複数のシェアにより元データが復元されないように、1つの通信先装置に送信するシェアの個数を制限することが必要である。例えば、 (k, n) しきい値法を用いてシェアを生成する場合、1つの通信先装置には k 未満の個数のシェアを送信する。送信完了後、制御部140は、全てのシェアを消去する。その後、制御はステップ324に移行する。
- [0054] ステップ316の判定結果がNO（復元要求を受信）であれば、ステップ320において、制御部140は、ステップ308により決定された収集先装置（E-E C U）からシェアを取得し、元データを復元する。その後、制御はステップ322に移行する。
- [0055] ステップ322において、制御部140は、ステップ320により復元された元データを、第1中継装置102に送信する。その後、制御はステップ324に移行する。これにより、第1中継装置102は、第2中継装置104に要求したデータを取得でき、そのデータを必要とするアプリケーションソフトウェア（以下、単にアプリケーションという）に引き渡す。
- [0056] ステップ324において、制御部140は、終了の指示を受けたか否かを判定する。終了の指示を受けたと判定された場合、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、上記の処理が繰返される。終了の指示は、例えば、車載システム100が搭載されている車両のスタ

ートボタン等がオフされることにより成される。

[0057] 以上により、第2中継装置104は、所定情報（例えば秘密情報）を複数に分割して複数のE-E C Uに保存する情報管理において、安全状態において複数の断片化情報（シェア）を通信するので、通信の際に漏洩および改竄の発生を防止できる。

[0058] また、第2中継装置104は、危険状態が持続している場合、第1中継装置102が提供する機能のリアルタイム性を損なわないように、所定期間が経過すれば、E-E C Uと断片化情報を通信するので、複数の断片化情報を通信できない状態がいつまでも持続することを回避できる。したがって、第1中継装置102の機能に支障が生じることを回避できる。

[0059] また、所定期間を、断片化情報により復元される元データを必要とする第1中継装置102の機能の特性（例えばリアルタイム性）に基づいて設定することにより、第1中継装置102の機能に要求されるリアルタイム性が損なわれることを回避できる。

[0060] また、上記したように、対象データを複数の断片化情報に分割するデータ分割復元部200を含み、対象データは第1中継装置102から第2中継装置104に入力され、データ分割復元部200は、秘密分散法により断片化情報を生成する。これにより、情報の漏洩および改竄の発生をより防止できる。

[0061] また、上記したように、第2中継装置104は、複数のE-E C Uの中から、複数の断片化情報の個数以下の個数のE-E C Uを通信先装置として決定する通信先決定部202を含み、複数の断片化情報の各々は、通信先装置と第2中継装置104との間において、秘密分散制御部206による計画に基づいて通信される。これにより、情報の漏洩および改竄の発生をより一層防止できる。

[0062] また、通信先決定部202は、第1中継装置102から第2中継装置104に所定情報の要求（復元要求）が入力されたことを受けて、複数の通信先装置（E-E C U）の中から、断片化情報を取得する複数の相手装置（E-E

E C U) を決定し、データ分割復元部 2 0 0 は、複数の相手装置から受信した断片化情報から、所定情報を生成する復元機能を有する。これにより、複数の E - E C U に分散させて記憶している断片化情報から元データを生成して第 1 中継装置 1 0 2 に提供できる。

[0063] 上記したように、第 2 中継装置 1 0 4 は、車両に搭載されている。これにより、車両における所定情報（例えば秘密情報）を複数の分割して複数の E - E C U に保存する情報管理において、断片化情報を通信する際に漏洩および改竄の発生を防止できる。

[0064] (適用例)

上記した、電子キーにより車両のドアの施錠および開錠等を行う場合、第三者に認証用 I D を知られると、ユーザ不在時に第三者により不正にドアが開錠される危険性がある。その対策として、例えば、車両の出荷時に、上記した電子キーの認証用 I D (秘密情報) を分割して複数の断片化情報を生成し、複数の断片化情報の各々を車載システム 1 0 0 の複数の E - E C U に記憶させることができる。ユーザが車両を操作（開錠および施錠等）する際には、例えば車載システム 1 0 0 の第 1 中継装置 1 0 2 は、事前にユーザが所持した電子キーの認証処理を実行する。認証過程において、車載システム 1 0 0 の第 2 中継装置 1 0 4 は、第 1 中継装置 1 0 2 からの復元要求を受信し、断片化情報を記憶している E - E C U から断片化情報を取得して車載側の認証用 I D を複合し、第 1 中継装置 1 0 2 に出力する。第 1 中継装置 1 0 2 は、電子キーから受信した認証用 I D が、復元された認証 I D と一致するかどうかを判定する。このとき、第 2 中継装置 1 0 4 は、安全状態において、断片化情報を記憶している E - E C U から断片化情報を通信により取得するので、断片化情報を通信する過程において、第三者により断片化情報が取得され、認証用 I D を第三者に知られてしまうリスクを回避できる。

[0065] なお、認証過程において、上記したように、安全状態でなければ、認証用 I D を復元するための断片化情報の通信を所定期間行わない。電子キーの認証は速やかに実行される必要があり、比較的高いリアルタイム制が要求され

る。したがって、所定期間は比較的短く設定される。

[0066] (第1変形例)

上記においては、危険状態であれば断片化情報を通信しない（即ち、所定期間待機する）場合を説明したが、これに限定されない。第1変形例においては、危険状態の程度に応じて、断片化情報の通信を実行する。

[0067] 第1変形例に係る車載システムは、図1に示した車載システム100と同じ構成を有し、第1変形例に係る第2中継装置の構成は、図2と異なる。図4を参照して、第1変形例に係る第2中継装置104Aは、データ分割復元部200、通信先決定部202、通信監視部204、秘密分散制御部206およびセキュリティ強度評価部220を含み、通信計画装置として機能する。各部は、図1に示した制御部140およびメモリ142により実現される。図4に示した第2中継装置104Aは、図2に示した第2中継装置104に、セキュリティ強度評価部220が追加されたものである。図4において、図2と同じ符号を付した構成は、図2と同じ機能を有する。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。また、図1において第2中継装置104を第2中継装置104Aと読み替えて、適宜図1に示した符号を参照する。

[0068] セキュリティ強度評価部220は、通信監視部204から入力される状態特定情報に基づいて、セキュリティ強度を評価し、評価結果を秘密分散制御部206に出力する。上記したように、状態特定情報は、通信監視部204による検知結果である、車外通信部120の通信状態、入出力ポート144および入出力ポート146等の空きポートの状態、ならびに、想定外の通信装置の接続の有無を表す情報である。セキュリティ強度評価部220は、車外通信部120の通信状態、空きポートの状態、ならびに、想定外の通信装置の接続の有無から、セキュリティ強度を決定するために、例えば図5および図6に示すような評価テーブルを記憶している。

[0069] 図5を参照して、車外通信部120の通信状態は、通信種別および通信速度の組合せにより表される。通信種別および通信速度の組合せに対するセキ

セキュリティ強度を、「高」、「中」および「低」の3つのレベルにより表している。図5においては、通信種別として物理的通信（有線通信）、近接無線通信および広域無線通信を示している。通信速度は、 a （Mbps）未満、 a （Mbps）以上 b （Mbps）未満、および、 b （Mbps）以上の3つの範囲に区分されている。 a および b は、 $0 < a < b$ を満たす実数である。各レベルの設定に関して、例えば、通信速度が高い場合、不正アクセスによる情報漏洩の危険度が高くなるので、セキュリティ強度を相対的に低く設定する。通信種別に関しては、広域無線通信時には、不正アクセスが比較的容易になるので、セキュリティ強度は相対的に低く設定される。

[0070] 図6に、空きポートの状態と想定外の通信装置の接続の有無との組合せに対して、セキュリティ強度を設定する例を示す。図6を参照して、空きポートの状態は、機器の接続の有無と、機器が接続されている場合においてその機器が想定内の機器であるか否かにより表される。なお、想定内の機器とは、安全であることが既知である機器を意味し、想定外の機器とは、安全であることが既知でない機器を意味する。想定外の通信装置の接続の有無に関しては、接続あり、および接続なしにより表される。図6においては、図5に示した3つのレベルよりも低いレベルを表すために、「最低」を用いている。空きポートに機器が接続されているか否かにかかわらず、想定外の通信装置が接続されていれば、セキュリティ強度は「最低」に設定される。空きポートに機器が接続されておらず、想定外の通信装置の接続もない場合に関して、「－」が示されている。そのような場合には、セキュリティ強度を算出しなくても秘密分散が可能であるので、考慮されないこと、即ち、セキュリティ強度が算出されないことを表すために「－」が示されている。なお、空きポートに接続されている機器が想定内の機器であるか否かは、予め想定内とする機器（安全であることが既知の機器）の情報を記憶しておくことにより、判定できる。

[0071] セキュリティ強度評価部220は、上記したように、通信監視部204から受信した状態特定情報に基づいて、車外通信部120の通信状態、空きポ

ートの状態および想定外の通信装置の接続の有無を特定し、評価テーブル（図5および図6参照）を参照して、車外通信部120の通信状態および空きポートの状態の各々のレベルを特定する。2つのレベルが特定されるので、セキュリティ強度評価部220は、2つのレベルのうちより低いレベルをセキュリティ強度として決定する。

[0072] 秘密分散制御部206は、通信監視部204の検知結果が危険状態であり、各E-ECUとの断片化情報の通信を行うことにより、通信過程における情報漏洩の危険性がある場合、セキュリティ強度評価部220から入力されるセキュリティ強度に応じて、各E-ECUとの断片化情報の通信を行うか否かを判定する。通信監視部204の検知結果が危険状態であっても、秘密分散制御部206は、セキュリティ強度が所定レベル以上であれば、各E-ECUとの断片化情報の通信を行うように決定する。これにより、複数の断片化情報の通信が、必要以上に抑制されることを回避でき、情報漏洩の危険性に応じて、複数の断片化情報の通信を制御できる。

[0073] 上記においては、車外通信部120の通信状態、空きポートの状態および想定外の通信装置の接続の有無により、セキュリティ強度を評価する場合を説明したが、これに限定されない。車外通信部120の通信状態、空きポートの状態および想定外の通信装置の接続の有無のうちの少なくともいずれかに応じて、セキュリティ強度を評価してもよい。これにより、セキュリティ強度を適切に評価できる。

[0074] 上記においては、セキュリティ強度を、車外通信部120の通信状態、空きポートの接続状態、および想定外の通信装置の接続の有無に基づいて決定する場合を説明したが、これに限定されない。例えば、秘匿化の対象データの性質に応じて、セキュリティ強度を決定してもよい。例えば、対象データの機密性または重要性が高い場合、情報漏洩した場合の影響に鑑み、セキュリティ強度を低く設定する。

[0075] （第2中継装置の動作）

図7を参照して、第2中継装置104Aの動作に関してさらに説明する。

断片化情報の生成には秘密分散法を用いる。図7に示した処理は、図1に示した第2中継装置104と同様に、制御部140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、制御部140は、本プログラムと並行して、図2に示した通信監視部204の機能を実現するためのプログラムを実行している。即ち、本プログラムは、図4に示したデータ分割復元部200、通信先決定部202、秘密分散制御部206およびセキュリティ強度評価部220の機能を実現するためのものである。図7のフローチャートは、図3に示したフローチャートにおいて、ステップ340およびステップ342が追加されたものである。図7において、図3と同じ符号を付したステップは、図3と同じ処理を実行する。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。

[0076] ステップ310が実行された後、ステップ340において、制御部140は、セキュリティ強度Sを評価する。その後、制御はステップ312に移行する。これは、上記したセキュリティ強度評価部220の機能に対応する。制御部140は、上記したように評価テーブルを参照して、セキュリティ強度を決定する。セキュリティ強度は、例えば、上記したように「高」、「中」、「低」および「最低」の4つのレベルにより表される。

[0077] ステップ312において、制御部140は、上記したように、車外通信状態、空きポートの状態および想定外の通信装置の接続の有無が安全状態であるか否かを判定する。安全状態であれば、制御はステップ316に移行し、そうでなければ、制御はステップ342に移行する。

[0078] ステップ342において、制御部140は、ステップ340により決定されたセキュリティ強度が所定のしきい値 T_h 以上であるか否かを判定する。 $S \geq T_h$ （セキュリティ強度が所定のしきい値 T_h 以上）であると判定された場合、制御はステップ316に移行する。そうでなければ、制御はステップ314に移行する。上記したように、セキュリティ強度は「高」、「中」、「低」および「最低」の4つのレベルにより表されるので、しきい値 T_h に

は、「高」、「中」、「低」および「最低」のいずれかが設定される。例えば、しきい値 T_h に「中」が設定されていれば、セキュリティ強度 S が「高」または「中」であれば、 $S \geq T_h$ と判定される。

[0079] 以上により、第2中継装置104Aは、第2中継装置104と同様に、所定情報（例えば秘密情報）を複数に分割して複数のE-ECUに保存する情報管理において、安全状態において複数の断片化情報（シェア）を通信するので、通信の際に漏洩および改竄の発生を防止できる。

[0080] また、第2中継装置104Aは、車外通信状態、空きポートの状態および想定外の通信装置の接続の有無が安全状態でなく、各E-ECUとの断片化情報の通信を行うことにより、通信過程における情報漏洩の危険性がある場合、セキュリティ強度に応じて、各E-ECUとの断片化情報の通信を行うか否かを判定する（ステップ342参照）。安全状態でなくても、第2中継装置104Aは、セキュリティ強度が所定レベル以上であれば、各E-ECUとの断片化情報の通信を行うように決定する（ステップ342の判定結果がYES）。これにより、複数の断片化情報の通信が、必要以上に抑制されることを回避でき、情報漏洩の危険性に応じて、複数の断片化情報の通信を制御できる。

[0081] （セキュリティ強度の具体例）

セキュリティ強度の設定に関する具体例を示す。例えば、図8を参照して、図1に示した車載システム100にカメラ160が追加されて構成された車載システム100Aにおいて、第1中継装置102は、車両内を監視するアプリケーションを実行する。カメラ160は、例えばデジタルビデオカメラである。例えば、第1中継装置102は、カメラ160により撮像された大容量の車内監視用の映像データを、断片化情報に分割して、第2中継装置104Aから複数のE-ECUに記憶させる。このとき、車外通信部120による外部装置130との通信速度が比較的低速であれば、第2中継装置104AとE-ECUとの間において大容量の断片化情報を通信しても、通信過程において、不正アクセスにより断片化情報が車外に漏洩する可能性は低

い。したがって、セキュリティ強度は比較的高く設定できる。

[0082] また、第2中継装置104Aまたは第1中継装置102の空きポート等に、ドライブレコーダが接続される場合、ディーラが提供するドライブレコーダであれば、想定内の機器に含まれるので、セキュリティ強度を比較的高く設定できる。ディーラとは、例えば、自動車メーカーまたはその系列の販売会社と契約を結んだ信頼できる販売会社を意味する。ディーラが提供するドライブレコーダを特定するための情報は、予め第2中継装置104Aのメモリに記憶しておけばよい。第2中継装置104Aは、接続された機器にアクセスしてその機器の情報を取得し（通信監視部204の機能）、ディーラのドライブレコーダであるか否かを判定できる。セキュリティ強度評価部220は、通信監視部204の判定結果を受けて、上記した評価テーブルを参照し、セキュリティ強度を決定できる。

[0083] 上記においては、セキュリティ強度が、「高」、「中」、「低」および「最低」の4つのレベルにより表される場合を説明したが、これに限定されない。セキュリティ強度は、複数レベルであればよく、3つ以下のレベルにより表されても、5つ以上のレベルにより表されてもよい。また、セキュリティ強度は、数値（正の整数等）により表されてもよい。その場合、各レベルを所定の数値範囲として設定しておけばよい。

[0084] （第2変形例）

上記においては、危険状態であれば断片化情報を通信しない（即ち、所定期間待機する）場合、および、危険状態の程度（セキュリティ強度）に応じて、断片化情報の通信を実行する場合を説明したが、これらに限定されない。第2変形例においては、危険状態において、通信を切断可能であれば、一時的に通信を切断して断片化情報の通信を実行する。

[0085] 第2変形例に係る車載システムは、図1に示した車載システム100と同じ構成を有し、第2変形例に係る第2中継装置の構成は、図2と異なる。図9を参照して、第2変形例に係る第2中継装置104Bは、データ分割復元部200、通信先決定部202、通信監視部204、秘密分散制御部206

および通信制御部 230 を含み、通信計画装置として機能する。各部は、図 1 に示した制御部 140 およびメモリ 142 により実現される。図 9 に示した第 2 中継装置 104 B は、図 2 に示した第 2 中継装置 104 に、通信制御部 230 が追加されたものである。図 9 において、図 2 と同じ符号を付した構成は、図 2 と同じ機能を有する。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。また、図 1 において第 2 中継装置 104 を第 2 中継装置 104 B と読み替えて、適宜図 1 に示した符号を参照する。

[0086] 通信制御部 230 は、車外通信部 120 による通信を一時的に切断可能かを判定する。通信制御部 230 は、判定結果を秘密分散制御部 206 に出力する。秘密分散制御部 206 は、通信監視部 204 の検知結果が危険状態であり、各 E-E C U との断片化情報の通信を行うことにより、通信過程における情報漏洩の危険性がある場合、通信制御部 230 から入力される判定結果に応じて、各 E-E C U との断片化情報の通信を行うか否かを判定する。入力される通信制御部 230 の判定結果が切断可能を表していれば、秘密分散制御部 206 は、通信制御部 230 に車外通信部 120 の通信切断を指示し、各 E-E C U との断片化情報の通信を行うように決定する。通信切断の指示を受けて通信制御部 230 は、車外通信部 120 に、通信を切断させ、所定期間（第 2 所定期間）切断状態を維持させる。所定期間が経過すれば、通信制御部 230 は、車外通信部 120 に通信を再開させる。

[0087] 車外通信部 120 の通信を切断する所定期間は、第 2 中継装置 104 および E-E C U の間における断片化情報の通信を完了できる期間以上の期間に設定される。そのように設定しておけば、断片化情報の通信中において、車外通信部 120 による通信は切断された状態に維持される。

[0088] 通信制御部 230 は、例えば、車載システム 100 が実行している機能（例えば、第 1 中継装置 102 が実行しているアプリケーション）に、車外通信部 120 の通信状態が関係している場合、車外通信部 120 による通信を一時的に切断できるか否かを判定する。例えば、自車両が車外装置と通信す

るサービスを使用中であり、通信を切断すると走行不能になる場合、通信制御部 230 は、車外通信部 120 の通信を切断できないと判定する。例えば、遠隔制御および死角情報共有等の機能が実行されていれば、通信制御部 230 は、車外通信部 120 の通信を切断できないと判定する。自車両が自律走行中であれば、通信制御部 230 は、車外通信部 120 の通信を切断できると判定する。自律走行機能に限らず、車外通信部 120 の通信が、リアルタイム性が要求される機能に関係している場合には、通信制御部 230 は、車外通信部 120 の通信を切断できないと判定する。

[0089] また、例えば、第 1 中継装置 102 が、外部装置 130（例えばサーバ）から音楽データまたは映像データ等をダウンロードしつつ再生するアプリケーションを実行している場合、所定量のデータがバッファに保持されていれば、通信制御部 230 は、車外通信部 120 の通信を切断できると判定してもよい。例えば、データがバッファに記憶されてからそのデータの利用（再生）が終了するまでの期間（以下、バッファ期間という）に、第 2 中継装置 104 が各 E-ECU との断片化情報の通信を完了できる場合、通信制御部 230 は、車外通信部 120 の通信を切断できると判定する。また、まとまった音楽データまたは映像データを一括ダウンロードした後、再生できる場合にも、通信制御部 230 は、車外通信部 120 の通信を切断できると判定してもよい。

[0090] このように、通信監視部 204 の検知結果が危険状態であっても、秘密分散制御部 206 は、車外通信部 120 の通信を切断して、各 E-ECU との断片化情報の通信を行うように決定する。これにより、断片化情報を通信できない状態がいつまでも持続することを回避できる。なお、上記においては、車外通信部 120 の通信を切断する場合を説明したが、これに限定されない。車外通信部 120 の通信を制限できればよい。車外通信部 120 の通信を制限すれば、断片化情報の通信過程における、断片化情報の漏洩を抑制できる。

[0091] 上記したように、車外通信部 120 による通信が、リアルタイム性が要求

される機能のために実行されていなければ、通信制御部 230 は、車外通信部 120 の通信を遮断可能であると判定してもよい。これにより、機能に要求されるリアルタイム性が損なわれることを回避しつつ、複数の断片化情報を通信できる。

[0092] 上記したように、車外通信部 120 による通信において所定量のデータのバッファ期間が、複数の断片化情報の通信に要する期間よりも長ければ、車外通信部 120 の通信が制限可能であると判定してもよい。これにより、外部通信を実行している機能に影響することなく、複数の断片化情報を通信できる。

[0093] (第2中継装置の動作)

図 10 を参照して、第2中継装置 104 B の動作に関してさらに説明する。断片化情報の生成には秘密分散法を用いる。図 10 に示した処理は、図 1 に示した第2中継装置 104 と同様に、制御部 140 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、制御部 140 は、本プログラムと並行して、図 2 に示した通信監視部 204 の機能を実現するためのプログラムを実行している。即ち、本プログラムは、図 9 に示したデータ分割復元部 200、通信先決定部 202、秘密分散制御部 206 および通信制御部 230 の機能を実現するためのものである。図 10 のフローチャートは、図 3 に示したフローチャートにおいて、ステップ 314 がステップ 350 により代替され、ステップ 352 およびステップ 354 が追加されたものである。図 10 において、図 3 と同じ符号を付したステップは、図 3 と同じ処理を実行する。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。

[0094] ステップ 312 において、制御部 140 は、上記したように、車外通信部 120 の通信状態、空きポートの状態および想定外の通信装置の接続の有無が安全状態であるか否かを判定する。安全状態であると判定された場合、制御はステップ 316 に移行する。そうでなければ、制御はステップ 350 に移行する。

- [0095] ステップ350において、制御部140は、車外通信部120の通信を切断可能か否かを判定する。切断可能と判定された場合、制御はステップ352に移行する。そうでなければ、制御はステップ310に戻り、ステップ310およびステップ312が実行される。これにより、安全状態でなければ（ステップ312の判定結果がNO）、車外通信部120が切断可能になるまで、待機状態が維持され、シェアの通信は行われない。
- [0096] ステップ352において、制御部140は、車外通信部120の通信を一時的に切断させる。その後、制御はステップ316に移行する。ステップ350およびステップ352は、上記した通信制御部230の機能に対応する。
- [0097] ステップ316に移行すれば、上記したように、第1中継装置102からの要求に応じた処理が実行される。即ち、シェアのE-ECUへの送信（ステップ318）、または、E-ECUからシェアの収集および元データの復元（ステップ320およびステップ322）が実行される。その後、制御はステップ354に移行する。
- [0098] ステップ354において、制御部140は、車外通信部120に、ステップ352により切断していた通信を再開させる。その後、制御はステップ324に移行する。
- [0099] 以上により、第2中継装置104Bは、通信監視部204の検知結果が危険状態であっても、車外通信部120の通信を切断して、各E-ECUとの断片化情報（シェア）の通信を行うように決定する。これにより、断片化情報を通信できない状態がいつまでも持続することを回避できる。
- [0100] 上記において、通信計画装置が、車両に搭載された第2中継装置104、第2中継装置104Aおよび第2中継装置104Bである場合を説明したが、これに限定されない。通信計画装置は、装置外部と通信する機能を有する装置またはシステムに搭載されていればよい。その装置またはシステムの内部に秘密情報を、断片化情報として分散させて記憶する必要がある場合に、通信計画装置は上記した動作を実行する。これにより、その装置またはシス

テムの内部における断片化情報の通信過程において、情報漏洩を抑制できる。

[0101] なお、上述の実施形態および変形例の各処理（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合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。なお物理的に分離した上記複数のプロセッサが互いに協働して上記各処理を実行してもよい。例えば物理的に分離した複数のコンピュータのそれぞれに搭載された上記プロセッサがLAN（Local Area Network）、WAN（Wide Area Network）およびインターネット等のネットワークを介して互いに協働して上記各処理を実行してもよい。

[0102] 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における全ての変更を含む。

符号の説明

[0103] 100、100A 車載システム

102 第1中継装置

104、104A、104B 第2中継装置

106、108、110 E-ECU

120 車外通信部

122 バス

130 外部装置

140 制御部

142 メモリ

144、146 入出力ポート

160 カメラ

200 データ分割復元部

202 通信先決定部

204 通信監視部

206 秘密分散制御部

210 対象データ

212 断片化情報

220 セキュリティ強度評価部

230 通信制御部

300、302、304、306、308、310、312、314、31

6、318、320、322、324、340、342、350、352、

354 ステップ

請求の範囲

- [請求項1] 第1装置、第2装置および通信装置を含むシステムに搭載される通信計画装置であって、
- 前記第1装置および前記第2装置の間における所定情報の通信を計画する計画部と、
- 前記計画部が前記通信を計画するために必要となる状態特定情報を検知する検知部とを含み、
- 前記計画部は、前記検知部による検知結果に基づいて、前記第1装置および前記第2装置の間における複数の断片化情報の通信を計画し、
- 前記断片化情報は、前記所定情報が分割されることにより生成される情報である、通信計画装置。
- [請求項2] 前記状態特定情報は、前記通信装置による前記システム外との通信である外部通信の通信状態、前記通信計画装置および前記第1装置の各々が有する入出力ポートの状態、ならびに、前記システム内の通信経路への想定外の通信装置の接続の有無のうちの少なくともいずれかの状態を表す情報を含む、請求項1に記載の通信計画装置。
- [請求項3] 前記計画部は、前記検知結果に基づいて前記複数の断片化情報の通信を行わないとの計画になる場合においては、第1所定期間が経過すれば、前記複数の断片化情報を通信するように計画する、請求項1または請求項2に記載の通信計画装置。
- [請求項4] 前記第1所定期間は、前記複数の断片化情報の通信を必要とする機能のリアルタイム性に基づいて決定される、請求項3に記載の通信計画装置。
- [請求項5] 前記システムからの情報漏洩に関するセキュリティ強度を評価するセキュリティ強度評価部をさらに含み、
- 前記計画部は、前記検知結果に基づいて前記複数の断片化情報の通信を行わないとの計画になる場合においては、前記セキュリティ強度

評価部により評価された前記セキュリティ強度が所定レベル以上であれば、前記複数の断片化情報を通信するように計画する、請求項1から請求項4のいずれか1項に記載の通信計画装置。

[請求項6] 前記セキュリティ強度評価部は、前記検知結果に基づいて、前記セキュリティ強度を評価する、請求項5に記載の通信計画装置。

[請求項7] 前記通信装置に、前記通信装置による前記システム外との通信である外部通信を制限させる通信制御部をさらに含み、
前記計画部は、

前記外部通信が制限可能であれば、前記通信制御部に、第2所定期間において前記外部通信を制限させ、

前記第2所定期間において、前記複数の断片化情報を通信するように計画する、請求項1から請求項6のいずれか1項に記載の通信計画装置。

[請求項8] 前記計画部は、前記外部通信が、リアルタイム性が要求される機能のために実行されていなければ、前記外部通信が制限可能であると判定する、請求項7に記載の通信計画装置。

[請求項9] 前記計画部は、前記外部通信において所定量のデータがバッファに記憶されてから当該データの利用が終了するまでの期間が、前記複数の断片化情報の通信に要する期間よりも長ければ、前記外部通信が制限可能であると判定する、請求項7に記載の通信計画装置。

[請求項10] 前記所定情報を前記複数の断片化情報に分割する情報処理部をさらに含み、

前記所定情報は、前記第1装置から前記通信計画装置を介して前記第2装置に送信され、

前記情報処理部は、秘密分散法により前記断片化情報を生成する、請求項1から請求項9のいずれか1項に記載の通信計画装置。

[請求項11] 複数の前記第2装置の中から、前記複数の断片化情報の個数以下の個数の通信先装置を決定する通信先決定部をさらに含み、

前記複数の断片化情報は、前記通信先装置と前記通信計画装置との間において、前記計画部による計画に基づいて通信される、請求項 10 に記載の通信計画装置。

[請求項12] 前記通信先決定部は、前記第 1 装置から前記通信計画装置に前記所定情報の要求が入力されたことを受けて、複数の前記通信先装置の中から、前記断片化情報を受信する複数の相手装置を決定し、

複数の前記相手装置から受信した前記断片化情報から、前記所定情報を生成する復元部をさらに含む、請求項 11 に記載の通信計画装置。

[請求項13] 車両に搭載される、請求項 1 から請求項 12 のいずれか 1 項に記載の通信計画装置。

[請求項14] 第 1 装置、第 2 装置および通信装置を含むシステムにおける前記第 1 装置および前記第 2 装置間の通信の制御方法であって、

制御部が、前記第 1 装置および前記第 2 装置の間における所定情報の通信を計画する計画ステップと、

前記制御部が、前記計画ステップにより前記通信が計画されるために必要となる状態特定情報を検知する検知ステップとを含み、

前記計画ステップは、前記制御部が、前記検知ステップによる検知結果に基づいて、前記第 1 装置および前記第 2 装置の間における複数の断片化情報の通信を計画するステップを含み、

前記断片化情報は、前記所定情報が分割されることにより生成される情報である、制御方法。

[請求項15] 第 1 装置、第 2 装置および通信装置を含むシステムに搭載されるコンピュータに、

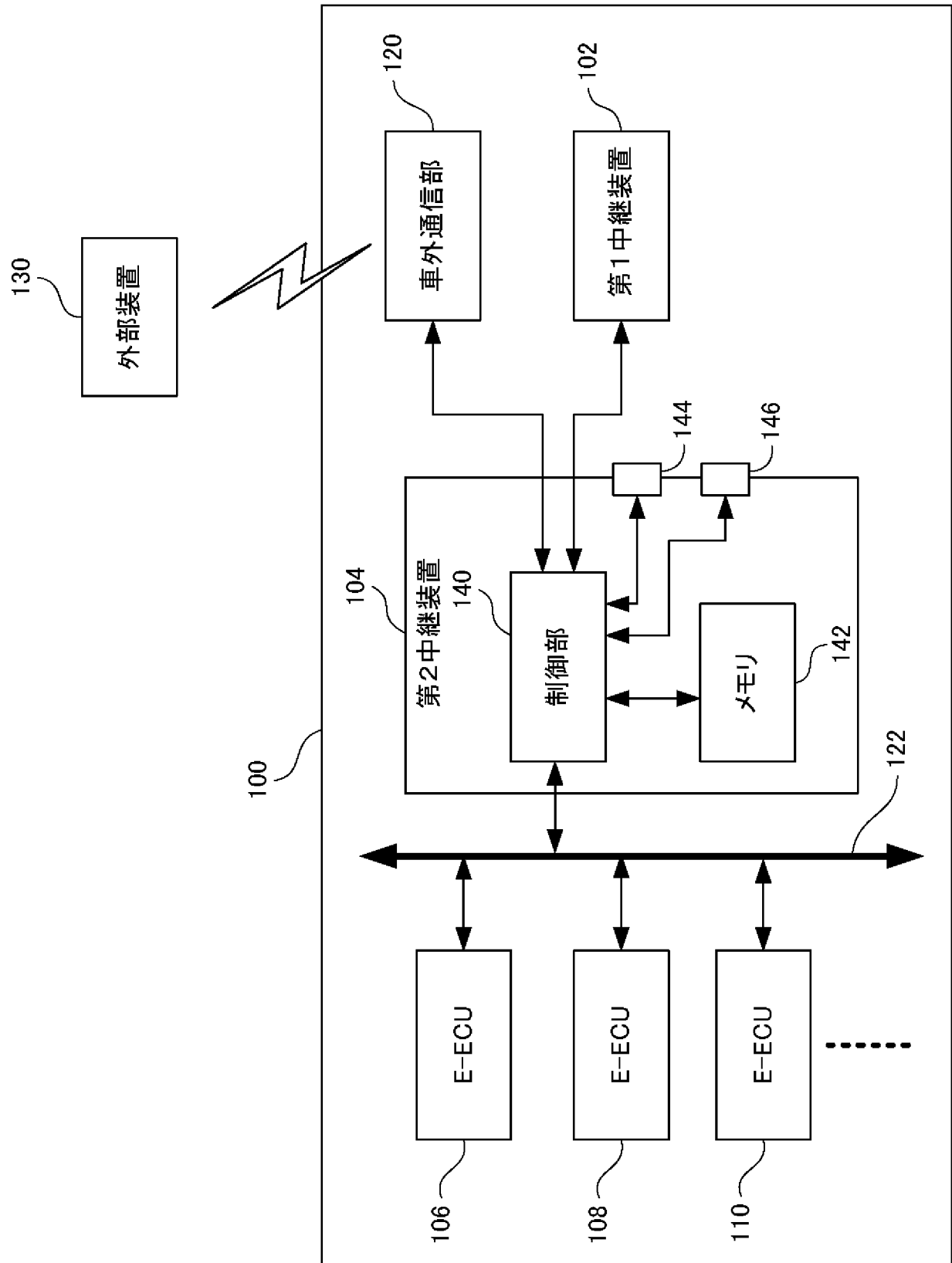
前記第 1 装置および前記第 2 装置の間における所定情報の通信を計画する計画機能と、

前記計画機能により前記通信が計画されるために必要となる状態特定情報を検知する検知機能とを実行させ、

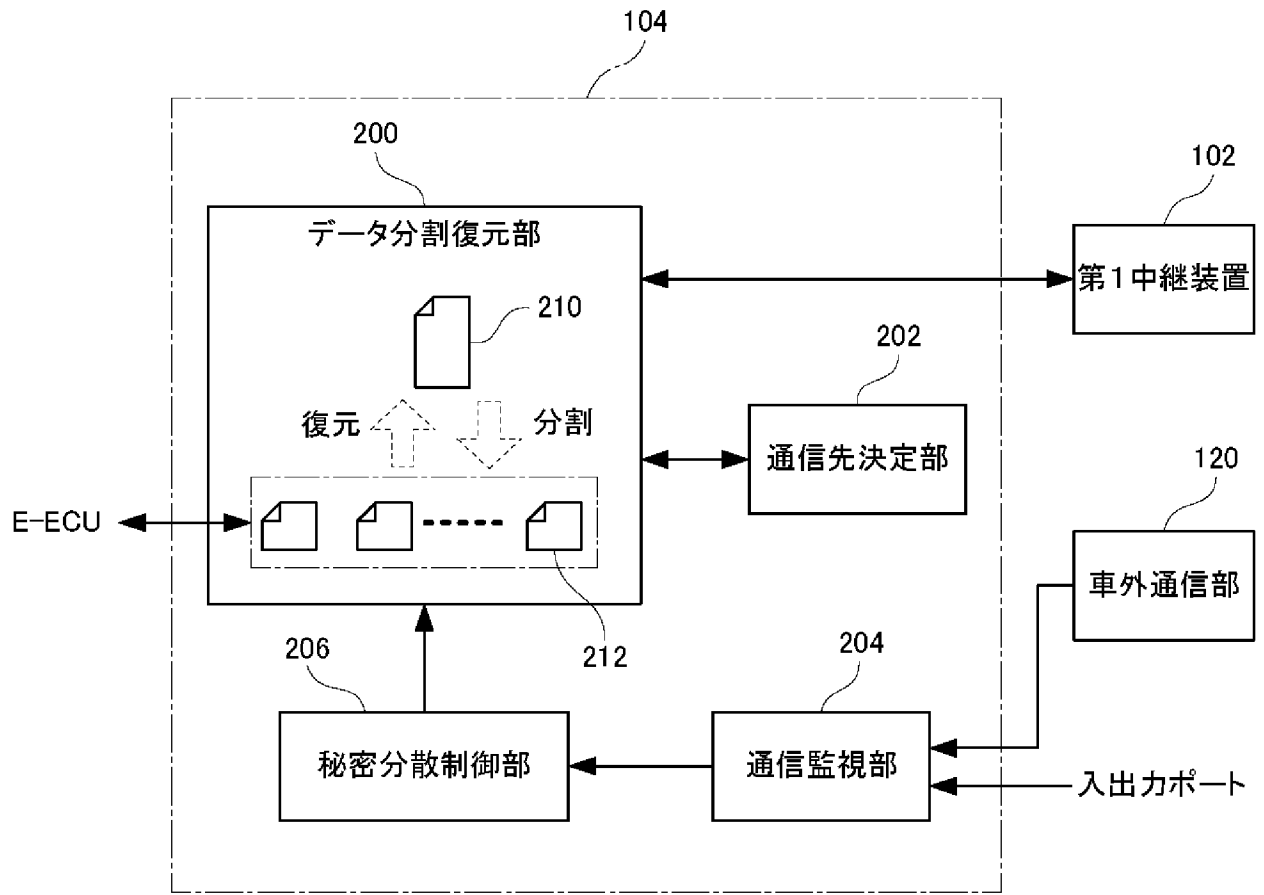
前記計画機能は、前記検知機能による検知結果に基づいて、前記第 1 装置および前記第 2 装置の間における複数の断片化情報の通信を計画する機能を含み、

前記断片化情報は、前記所定情報が分割されることにより生成される情報である、コンピュータプログラム。

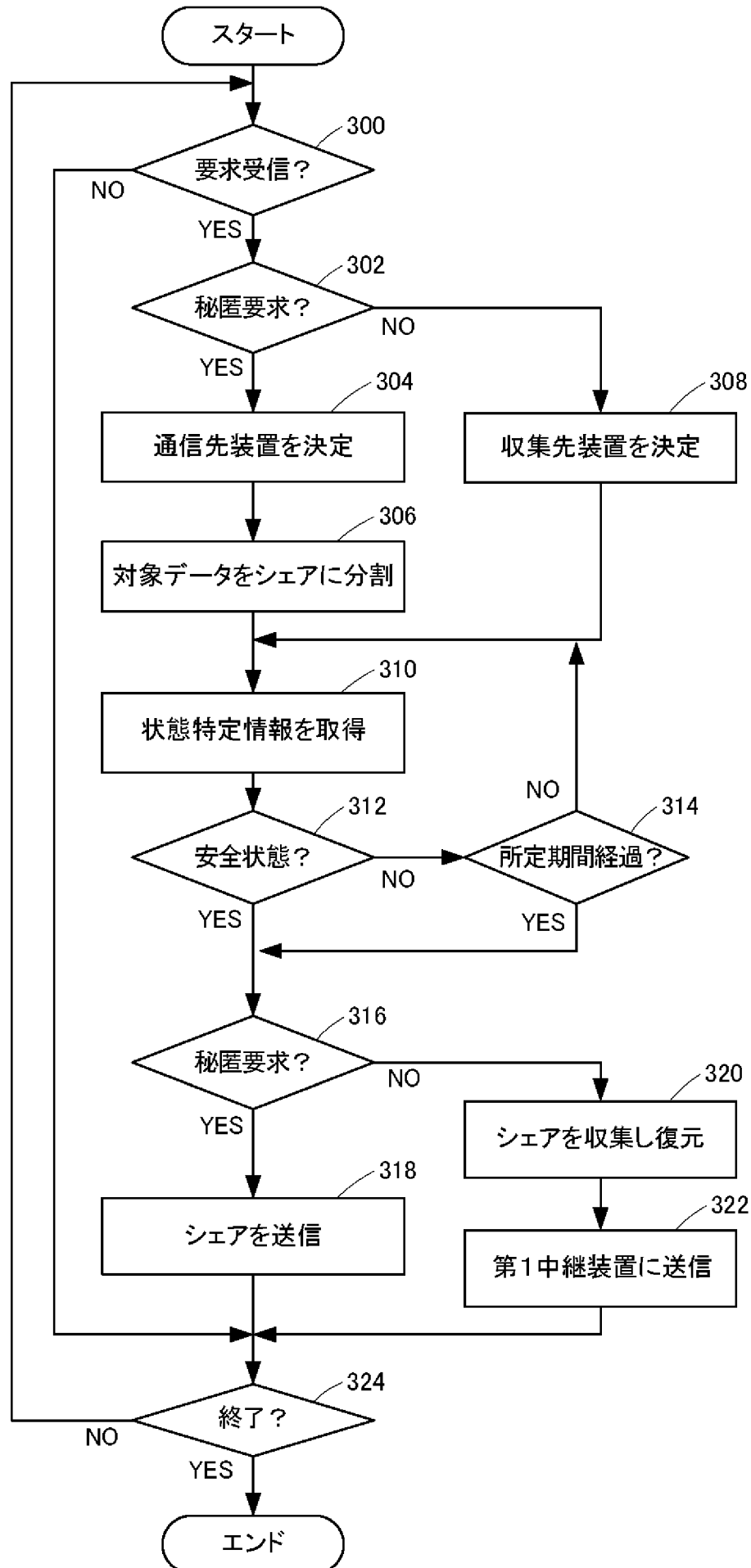
[図1]



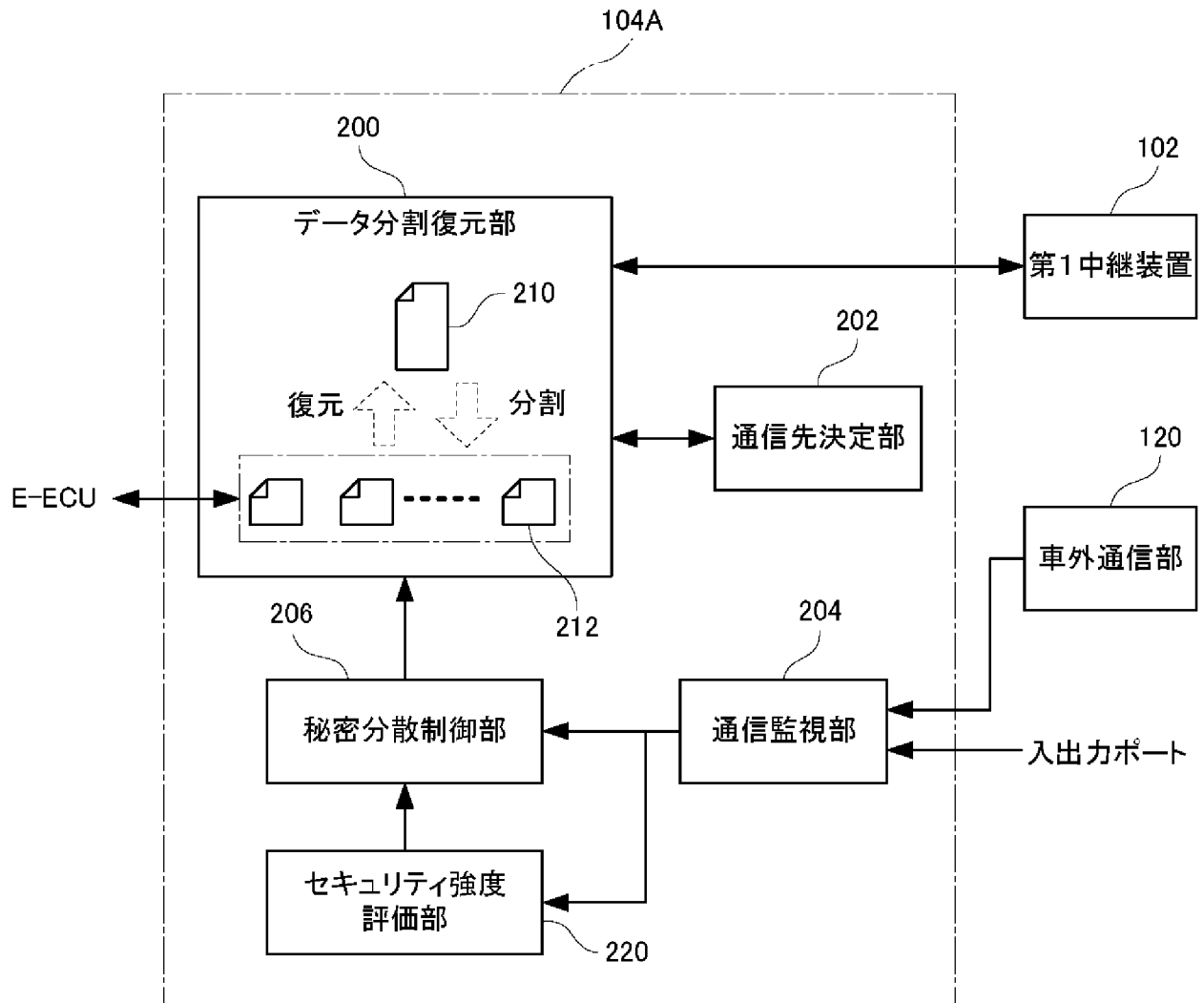
[図2]



[図3]



[図4]



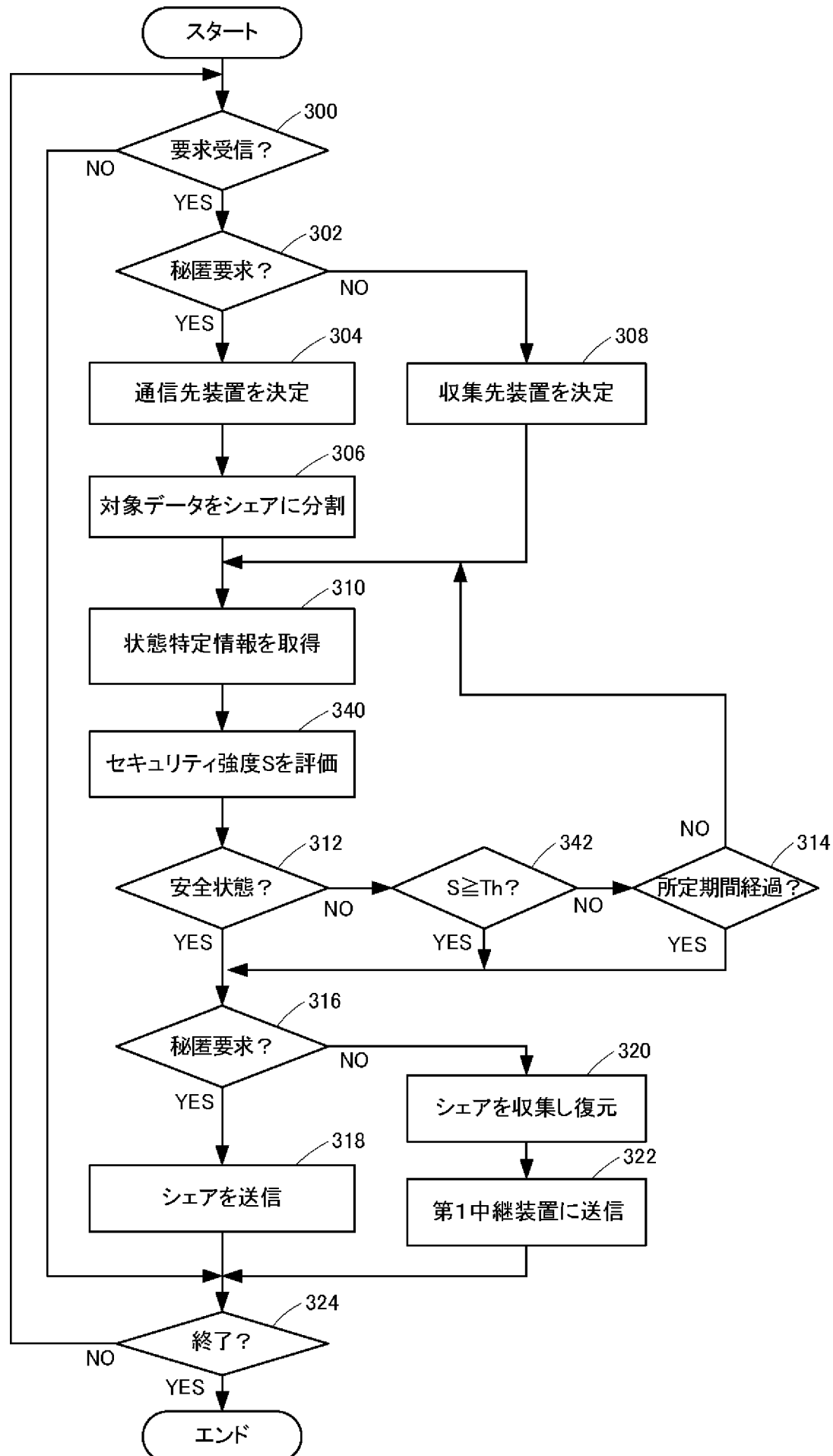
[図5]

通信速度 [Mbps]	a未満	a以上 b未満	b以上
通信種別			
物理的(有線)	高	高	中
近接(無線)	高	中	低
広域(無線)	中	低	低

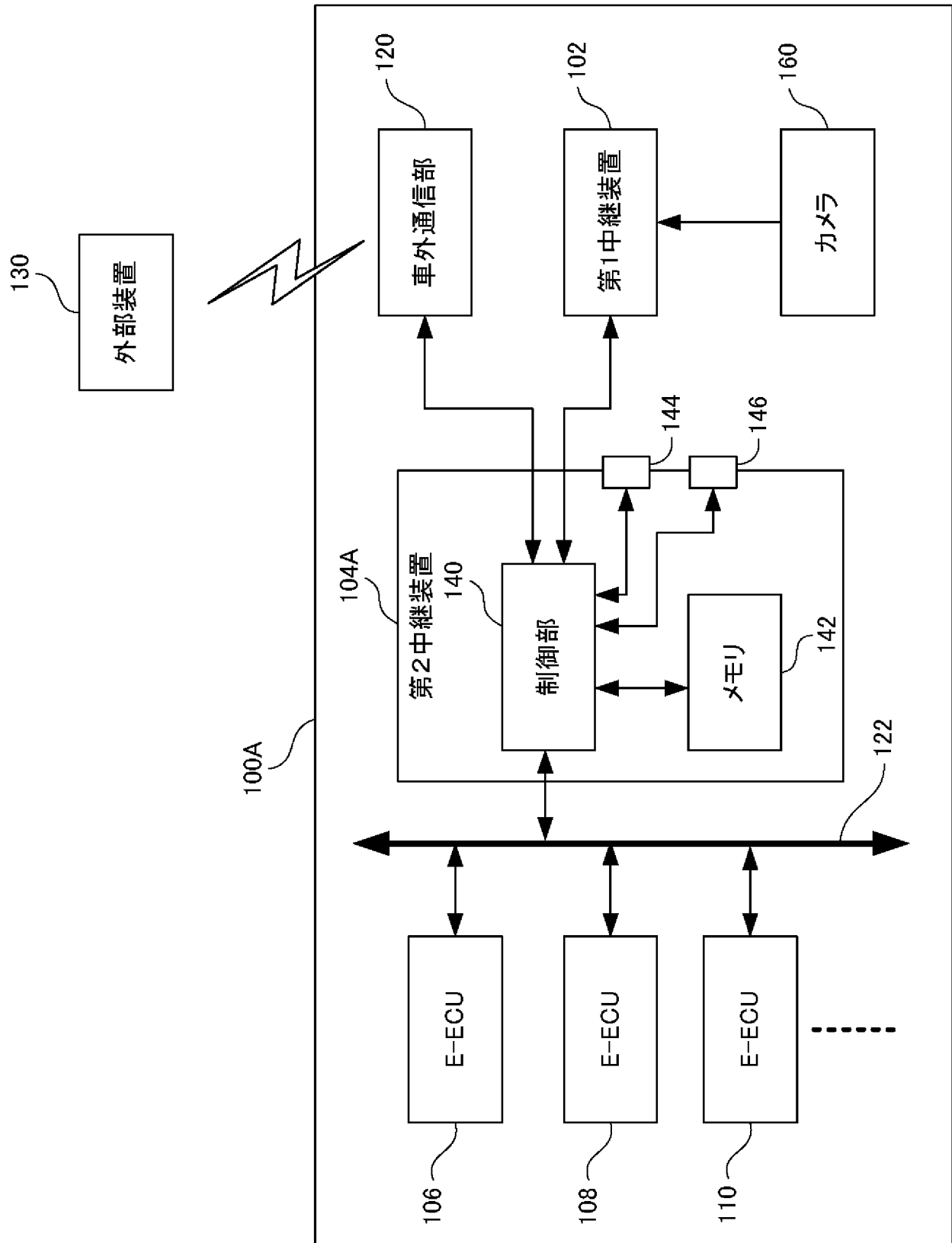
[図6]

空き ポート 想定外通信 装置	接続なし	接続あり
	接続なし	接続あり
接続なし	—	最低
接続あり (想定内)	高	最低
接続あり (想定外)	低	最低

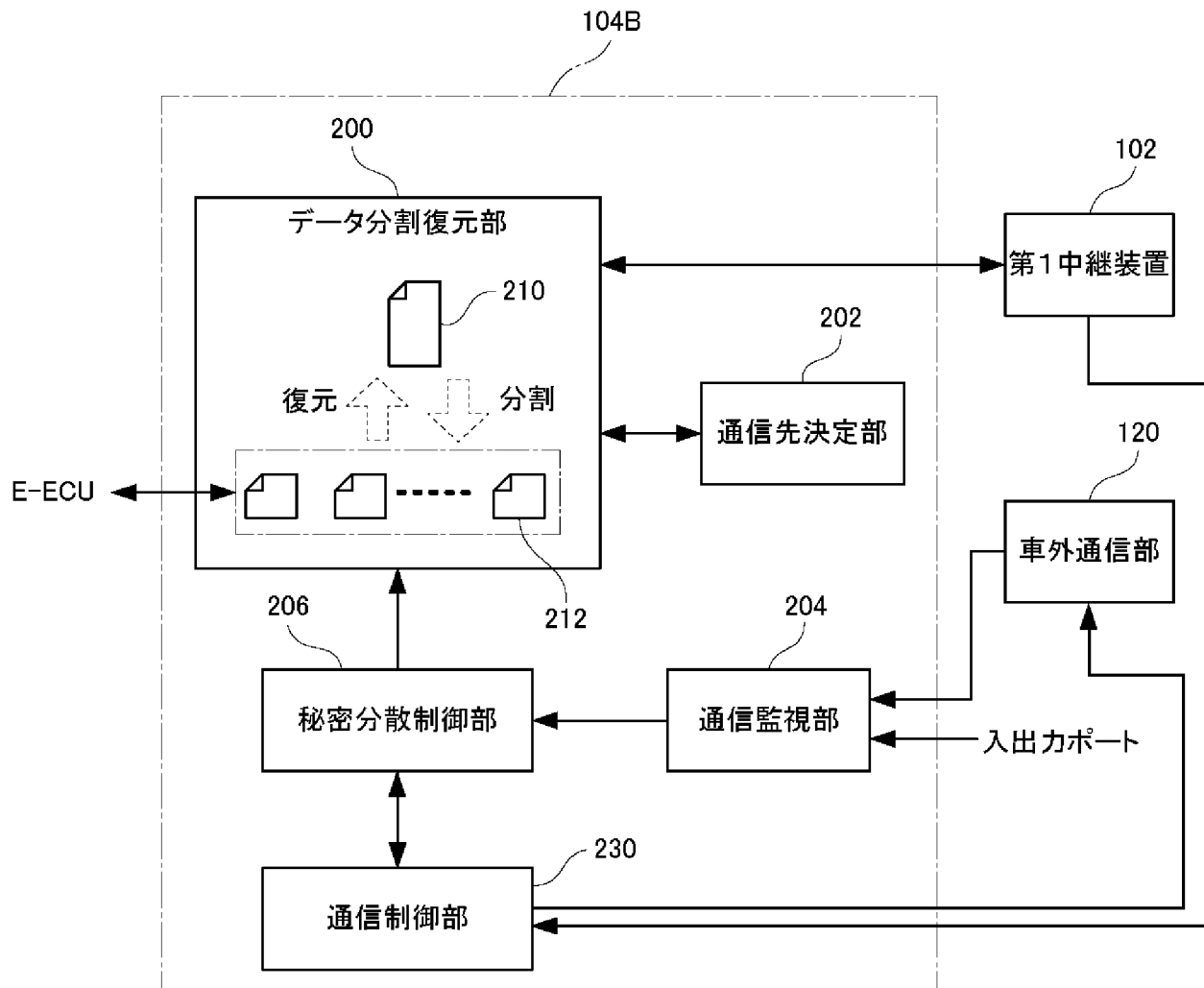
[図7]



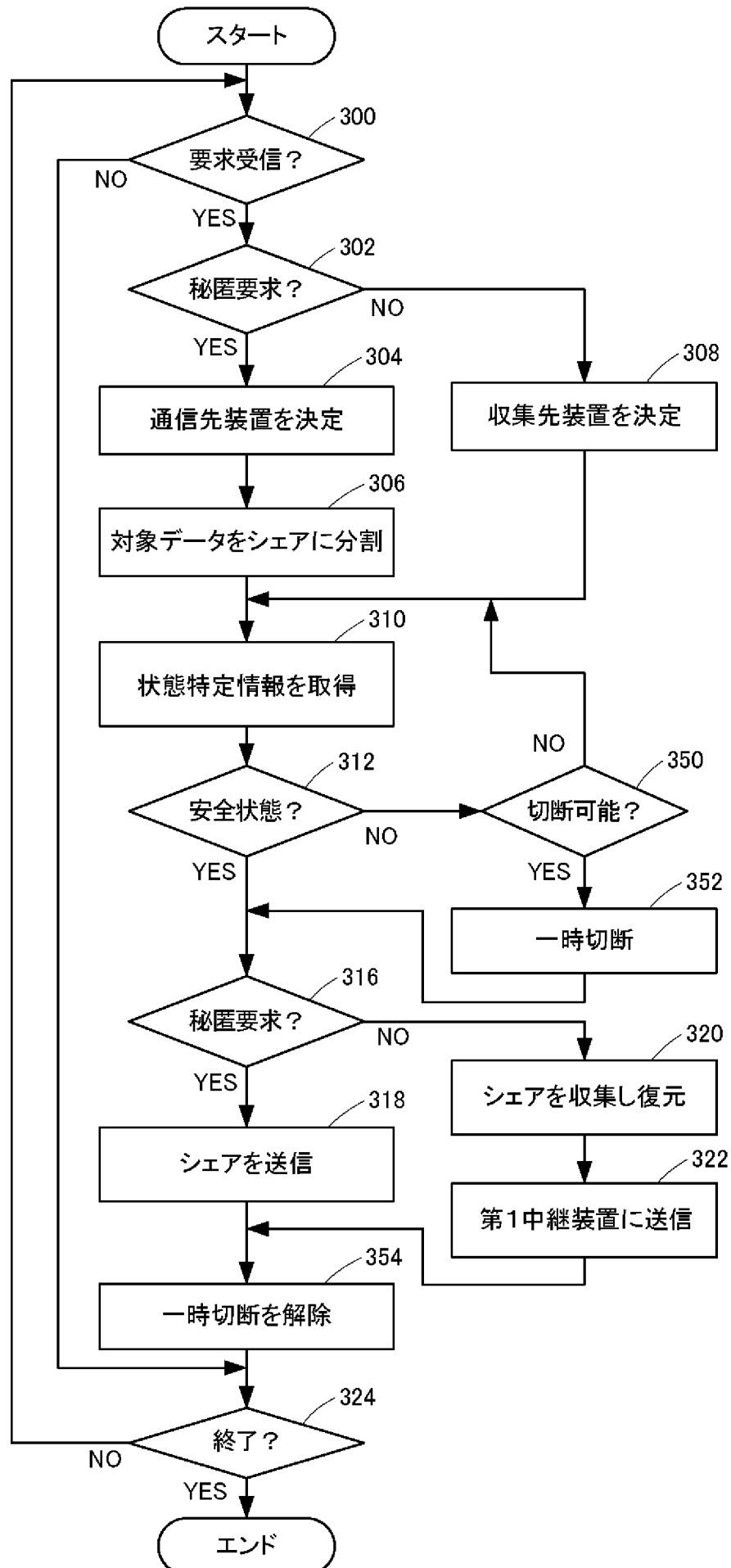
[図8]



[図9]



[図10]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2024/000034

A. CLASSIFICATION OF SUBJECT MATTER G06F 21/60 (2013.01)i FI: G06F21/60 360 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) G06F21/60 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 1971-2024 Registered utility model specifications of Japan 1996-2024 Published registered utility model applications of Japan 1994-2024 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 2018-205809 A (HITACHI SYSTEMS ENG SERVICES LTD.) 27 December 2018 (2018-12-27) paragraphs [0029]-[0045]	1, 10, 14-15
A	paragraphs [0029]-[0045]	2-9, 11-13
A	JP 2005-171538 A (OKI ELECTRIC INDUSTRY CO., LTD.) 30 June 2005 (2005-06-30) paragraphs [0063]-[0102]	1-15
A	JP 2019-114916 A (DENSO CORPORATION) 11 July 2019 (2019-07-11) claim 1	1-15
☐ 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 “D” document cited by the applicant in the international application “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 07 March 2024		Date of mailing of the international search report 19 March 2024
Name and mailing address of the ISA/JP Japan Patent Office (ISA/JP) 3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915 Japan		Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2024/000034

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP	2018-205809	A	27 December 2018	(Family: none)	
JP	2005-171538	A	30 June 2005	(Family: none)	
JP	2019-114916	A	11 July 2019	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC））

G06F 21/60(2013.01)i

FI: G06F21/60 360

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））

G06F21/60

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 - 2024年

日本国実用新案登録公報

1996 - 2024年

日本国登録実用新案公報

1994 - 2024年

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

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
X	JP 2018-205809 A（株式会社日立システムズエンジニアリングサービス） 27.12.2018 (2018 - 12 - 27)	1,10,14-15
A	段落[0029]-[0045]	2-9,11-13
A	JP 2005-171538 A（沖電気工業株式会社） 30.06.2005（2005 - 06 - 30） 段落[0063]-[0102]	1-15
A	JP 2019-114916 A（株式会社デンソー） 11.07.2019（2019 - 07 - 11） 請求項1	1-15

☐ 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、一般的技术水準を示すもの

“D” 国際出願で出願人が先行技術文献として記載した文献

“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

07.03.2024

国際調査報告の発送日

19.03.2024

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）

宮司 卓佳 5S 9555

電話番号 03-3581-1101 内線 3546

様式 PCT/ISA/210（第2ページ）（2022年7月）

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/JP2024/000034

引用文献			公表日	パテントファミリー文献	公表日
JP	2018-205809	A	27.12.2018	(ファミリーなし)	
JP	2005-171538	A	30.06.2005	(ファミリーなし)	
JP	2019-114916	A	11.07.2019	(ファミリーなし)	