

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2020年4月23日(23.04.2020)



(10) 国際公開番号

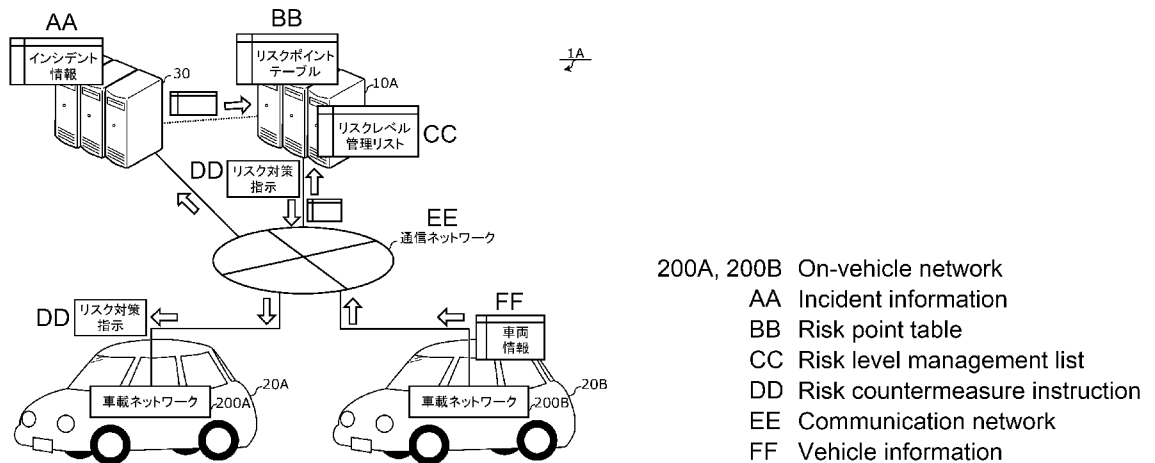
WO 2020/079943 A1

- (51) 国際特許分類:
B60R 25/01 (2013.01) *G06F 21/55* (2013.01)
B60R 25/102 (2013.01) *G08G 1/01* (2006.01)
B60R 25/33 (2013.01)
- (21) 国際出願番号: PCT/JP2019/032336
- (22) 国際出願日: 2019年8月20日(20.08.2019)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
62/746,851 2018年10月17日(17.10.2018) US
特願 2019-098771 2019年5月27日(27.05.2019) JP
- (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 PROPER-
TY CORPORATION OF AMERICA) [US/US];
- 90503 カリフォルニア州トーランス, ス
イト 200, マリナー アベニュー
20000 California (US).
- (72) 発明者: 佐々木 崇光(SASAKI, Takamitsu);
〒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).
高橋 良太(TAKAHASHI, Ryota).
- (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,

(54) Title: INFORMATION PROCESSING DEVICE, INFORMATION PROCESSING METHOD, AND PROGRAM

(54) 発明の名称: 情報処理装置、情報処理方法及びプログラム

[図19]



(57) Abstract: This information processing device for processing information of first and second vehicles is provided with: an incident information acquisition unit (11) that acquires incident information about the actual occurrence of incidents in the vehicles; a vehicle information acquisition unit (12) that acquires second vehicle information about the state of the second vehicle through communication with the second vehicle; a storage unit (13) that stores the incident information and the second vehicle information; a risk determination unit (14) that determines a risk level of a vehicle function of the second vehicle on the basis of the level of matching between the incident information and the second vehicle information; a risk countermeasure instruction generation unit (16) that generates a function limit instruction for a vehicle function of the first vehicle corresponding to the vehicle function of the second vehicle when the risk level is higher than a first standard; and an instruction output unit (17) that outputs the function limit instruction.

HN, HR, HU, ID, IL, IN, IR, IS, JO, KE, KG, KH,
KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,
MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,
NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,
QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

添付公開書類：

- 一 国際調査報告（条約第21条(3)）

(57) 要約：第一車両及び第二車両の情報を処理する情報処理装置は、車両で発生したインシデントの実績に関するインシデント情報を取得するインシデント情報取得部（11）と、第二車両との通信を介して第二車両の状態に関する第二車両情報を取得する車両情報取得部（12）と、インシデント情報及び第二車両情報を蓄積する蓄積部（13）と、インシデント情報と第二車両情報との一致度に基づいて第二車両の車両機能のリスクレベルを判定するリスク判定部（14）と、リスクレベルが第一基準より高い場合、この第二車両の車両機能に対応する第一車両の車両機能に対する機能制限指示を生成するリスク対策指示生成部（16）と、機能制限指示を出力する指示出力部（17）とを備える。

明 細 書

発明の名称： 情報処理装置、情報処理方法及びプログラム

技術分野

[0001] 本発明は、車両で利用される情報を処理する情報処理装置に関する。

背景技術

[0002] 高機能化が進む自動車では、車載ネットワークシステム内で、また、車載ネットワークと外部の情報機器、交通基盤又は他の車両等のシステムとの間で多くの情報がやり取りされる。そして、やり取りされる情報を処理する車載ネットワークシステムの脆弱性を突くサイバー攻撃の脅威が顕在化している。

[0003] 情報処理によって実現される高機能な自動車のセキュリティを向上させる技術が提案されている（例えば特許文献1 参照）。

先行技術文献

特許文献

[0004] 特許文献1：特開2014-146868号公報

発明の概要

発明が解決しようとする課題

[0005] しかしながら、特許文献1に開示される対抗手段は、すでに攻撃者が車載ネットワークに侵入した上で異常メッセージの送信等による発生した攻撃を検知して対応するものである。つまり、この対応が完了するまでの時間、車両は攻撃の影響を受ける。また、攻撃対象である車両単体にとって未知のパターンによる攻撃を受けた場合には、異常の検知又は停止までに時間が掛かったり、さらには被害が深刻化したりするおそれもある。

[0006] 本発明は、車両単体にとっては未知の手法によるものであっても、車載ネットワークへの侵入を抑えてサイバー攻撃の発生及び被害の深刻化を防ぐ情報処理装置等を提供する。

課題を解決するための手段

[0007] 本発明の一態様に係る情報処理装置は、第一車両及び第二車両の情報を処理する情報処理装置であって、車両で発生したサイバー攻撃のインシデントに関するインシデント情報を取得するインシデント情報取得部と、前記第二車両との通信を介して前記第二車両の状態に関する第二車両情報を取得する車両情報取得部と、前記インシデント情報及び前記第二車両情報を蓄積する蓄積部と、前記インシデント情報と前記第二車両情報との一致度に基づいて、前記第二車両が持つ車両機能のリスクレベルを判定するリスク判定部と、前記リスクレベルが第一基準より高い場合、前記第二車両の車両機能に対応する前記第一車両の車両機能に対する機能制限指示を生成するリスク対策指示生成部と、前記機能制限指示を出力する指示出力部とを備える。

[0008] また、本発明の一態様に係る情報処理方法は、第一車両及び第二車両の情報を処理する情報処理装置が車両で発生したサイバー攻撃のインシデントに関するインシデント情報を取得し、前記第二車両との通信を介して前記第二車両の状態に関する第二車両情報を取得し、前記インシデント情報と前記第二車両情報との一致度に基づいて、前記第二車両が持つ車両機能のリスクレベルを判定し、前記リスクレベルが第一基準より高い場合、前記第二車両の車両機能に対応する前記第一車両の車両機能に対する機能制限指示を生成し、前記機能制限指示を出力する。

[0009] また、本発明の一態様に係るプログラムは、プロセッサ及びメモリを備え、第一車両及び第二車両の情報を処理する情報処理装置において、前記メモリを用いて前記プロセッサによって実行されることで、前記プロセッサに、車両で発生したサイバー攻撃のインシデントに関するインシデント情報を取得させ、前記第二車両との通信を介して前記第二車両の状態に関する第二車両情報を取得させ、前記インシデント情報と前記第二車両情報との一致度に基づいて、前記第二車両が持つ車両機能のリスクレベルを判定させ、前記リスクレベルが第一基準より高い場合、前記第二車両の車両機能に対応する前記第一車両の車両機能に対する機能制限指示を生成させ、前記機能制限指示を出力させる。

[0010] なお、これらの包括的または具体的な態様は、システム、集積回路又はコンピュータ読み取り可能なＣＤ－ＲＯＭなどの記録媒体で実現されてもよく、装置、システム、方法、集積回路、コンピュータプログラム又は記録媒体の任意の組み合わせで実現されてもよい。

発明の効果

[0011] 本発明は、車両単体にとっては未知の手法によるものであっても、車載ネットワークへの侵入を抑え、また、サイバー攻撃の発生又は被害の深刻化を防ぐ情報処理装置等を提供する。

図面の簡単な説明

[0012] [図1]図１は、実施の形態１に係る情報処理装置を含むセキュリティリスク対策システムの構成例の概要を示す図である。

[図2]図２は、実施の形態１におけるインシデント情報のデータ構成例を示す図である。

[図3]図３は、上記のセキュリティリスク対策システムによるセキュリティリスク対策の適用対象である車両が備える車載ネットワークの構成例を示す図である。

[図4]図４は、上記のセキュリティリスク対策システムに含まれるセキュリティリスク対策サーバの構成例を示す図である。

[図5]図５は、上記のセキュリティリスク対策サーバで実行されるセキュリティリスク対策の処理の手順例を示すフロー図である。

[図6]図６は、上記のセキュリティリスク対策の処理における、インシデント情報収集サーバとセキュリティリスク対策サーバとの連携を含む手順を示すシーケンス図である。

[図7A]図７Ａは、上記のセキュリティリスク対策の処理で用いられるリスクポイントテーブルの一例である。

[図7B]図７Ｂは、上記のセキュリティリスク対策の処理で用いられるリスクポイントテーブルの一例である。

[図7C]図７Ｃは、上記のセキュリティリスク対策の処理で用いられるリスク

ポイントテーブルの一例である。

[図7D]図7Dは、上記のセキュリティリスク対策の処理で用いられるリスクポイントテーブルの一例である。

[図7E]図7Eは、上記のセキュリティリスク対策の処理で用いられるリスクポイントテーブルの一例である。

[図7F]図7Fは、上記のセキュリティリスク対策の処理で用いられるリスクポイントテーブルの一例である。

[図7G]図7Gは、上記のセキュリティリスク対策の処理で用いられるリスクポイントテーブルの一例である。

[図8]図8は、上記のリスクポイントテーブルの更新処理の手順例を示すフロー図である。

[図9]図9は、上記のセキュリティリスク対策の処理における、第一車両とセキュリティリスク対策サーバとの連携を含む手順を示すシーケンス図である。

[図10]図10は、実施の形態1における車両情報のデータ構成例を示す図である。

[図11]図11は、実施の形態1における車両情報のデータ構成例を示す図である。

[図12]図12は、実施の形態1におけるリスクレベル管理リストのデータ構成例を示す図である。

[図13]図13は、上記のリスクレベル管理リストに含まれるリスクスコアの算出処理の手順例を示すフロー図である。

[図14A]図14Aは、上記のセキュリティリスク対策の処理における、第一車両の車載機器のリスクポイントの算出処理の手順例を示すフロー図である。

[図14B]図14Bは、上記のセキュリティリスク対策の処理における、第一車両の走行位置のリスクポイントの算出処理の手順例を示すフロー図である。

[図14C]図14Cは、上記のセキュリティリスク対策の処理における、第一車両の車種のリスクポイントの算出処理の手順例を示すフロー図である。

[図14D]図14Dは、上記のセキュリティリスク対策の処理における、第一車両の通信プロトコルのリスクポイントの算出処理の手順例を示すフロー図である。

[図14E]図14Eは、上記のセキュリティリスク対策の処理における、第一車両の搭載機能のリスクポイントの算出処理の手順例を示すフロー図である。

[図14F]図14Fは、上記のセキュリティリスク対策の処理における、第一車両の走行状態のリスクポイントの算出処理の手順例を示すフロー図である。

[図15]図15は、上記のリスクレベル管理リストに含まれるリスクスコアを用いたリスク制御処理の手順例を示すフロー図である。

[図16A]図16Aは、上記のセキュリティリスク対策の処理における、第一車両とセキュリティリスク対策サーバとの連携を含む手順を示すシーケンス図である。

[図16B]図16Bは、上記のセキュリティリスク対策の処理における、第一車両とセキュリティリスク対策サーバとの連携を含む手順を示すシーケンス図である。

[図17]図17は、上記のリスクレベル管理リストに含まれるリスクスコアを用いたリスク制御処理の手順例を示すフロー図である。

[図18A]図18Aは、上記のリスクレベル管理リストに含まれるリスクスコアを用いたリスク制御処理の手順例を示すフロー図である。

[図18B]図18Bは、上記のリスクレベル管理リストに含まれるリスクスコアを用いたリスク制御処理の手順例を示すフロー図である。

[図18C]図18Cは、上記のリスクレベル管理リストに含まれるリスクスコアを用いたリスク制御処理の手順例を示すフロー図である。

[図19]図19は、実施の形態2に係る情報処理装置を含むセキュリティリスク対策システムの構成例の概要を示す図である。

[図20]図20は、実施の形態2に係る情報処理装置で実現されるセキュリティリスク対策サーバで実行されるセキュリティリスク対策の処理の手順例を示すフロー図である。

[図21]図 2 1 は、上記のセキュリティリスク対策の処理における、第二車両とセキュリティリスク対策サーバとの連携及び第一車両とセキュリティリスク対策サーバとの連携を含む手順を示すシーケンス図である。

[図22]図 2 2 は、第二車両のリスクスコアを用いた第一車両のリスク制御処理の手順例を示すフロー図である。

[図23]図 2 3 は、第二車両のリスクスコアを用いた第一車両のリスク制御処理の手順例を示すフロー図である。

[図24A]図 2 4 A は、第一車両と第二車両と間の距離を用いた第一車両のリスク制御処理の手順例を示すフロー図である。

[図24B]図 2 4 B は、第一車両と第二車両と間の距離を用いた第一車両のリスク制御処理の手順例を示すフロー図である。

[図25]図 2 5 は、第二車両のインシデント履歴に応じたセキュリティ対策の処理の手順例を示すフロー図である。

[図26]図 2 6 は、実施の形態におけるセキュリティリスク対策を実行する車載の情報処理装置の構成例を示す図である。

発明を実施するための形態

[0013] (本発明の基礎となった知見)

本発明者は、「背景技術」の欄において記載したサイバー攻撃への対抗手法に関し、異常の検知後の対応であることによる上述のような問題が生じることを見出した。

[0014] I T (Information Technology) の分野では、新たな手法によるサイバー攻撃に対してもコストを抑えながら速やかな対応を可能にするために、蓄積される脅威情報を共有する仕組みの構築が始まっている。情報化が進んだ自動車についても、セキュリティ対策として同様の仕組みを導入することは一案である。しかしながら、自動車では車両間で状態に差があり、各車両の状態も一定ではない。そのため、脅威に対するリスクレベル及び必要な対処は車両によって差があり、各車両でも変化し得る。したがって、単純に各車両からの情報の収集及び各車両へのセキュリティに関する情報の提供が可能な

仕組みを構築するだけでは、自動車の情報セキュリティと情報の利用による利便性との両立に支障が出る可能性もある。

[0015] このような問題を解決するために、本発明の一態様に係る情報処理装置は、第一車両及び第二車両の情報を処理する情報処理装置であって、車両で発生したサイバー攻撃のインシデントに関するインシデント情報を取得するインシデント情報取得部と、前記第二車両との通信を介して前記第二車両の状態に関する第二車両情報を取得する車両情報取得部と、前記インシデント情報及び前記第二車両情報を蓄積する蓄積部と、前記インシデント情報と前記第二車両情報との一致度に基づいて、前記第二車両が持つ車両機能のリスクレベルを判定するリスク判定部と、前記リスクレベルが第一基準より高い場合、前記第二車両の車両機能に対応する前記第一車両の車両機能に対する機能制限指示を生成するリスク対策指示生成部と、前記機能制限指示を出力する指示出力部とを備える。

[0016] これにより、多数の車両でのサイバー攻撃のインシデントに関する情報に基づいて、状態に応じた第二車両のリスクレベルが判定される。そして、この判定の結果得られたリスクレベルが所定の基準を超えて高い場合、第一車両の機能を制限することで攻撃の発生、又は攻撃による悪影響の拡大を抑えることができる。

[0017] 例えば、前記リスク対策指示生成部は、前記リスクレベルが前記第一基準より上の第二基準よりも高い場合、前記機能制限指示として前記第二車両の車両機能に対応する前記第一車両の車両機能に対する機能無効化指示を生成してもよい。また例えば、前記第二車両の車両機能のリスクレベルが前記第一基準より低い場合、前記第二車両の車両機能に対応する前記第一車両の車両機能に対する機能制限解除指示を生成する機能制限解除指示生成部を備え、前記指示出力部は、前記機能制限解除指示を出力してもよい。

[0018] このように、リスクの高さに応じて機能の制限の程度を変えることで、車両による情報利用における安全と利便性との両立を図ることができる。

[0019] 例えば、前記第二車両情報が示す前記第二車両の走行状態が変化した場合

、前記リスク判定部は、前記第二車両の車両機能のリスクレベルを再判定してもよい。具体的な例としては、前記第二車両の走行状態が走行中状態から停止状態に変化した場合、前記機能制限解除指示生成部は、前記第一車両の車両機能のうち通信関連機能に対する機能制限を解除する前記機能制限解除指示を生成してもよい。

[0020] これにより、車両の走行状態によって変わるリスクレベルの高さ又は必要な対処に応じて適切な機能制限が適用される。

[0021] 例えば、前記蓄積部に蓄積されている前記インシデント情報に前記第二車両で発生したインシデント情報が含まれている場合、前記第二車両の車両機能のリスクレベルを前記第一基準より高くしてもよい。

[0022] サイバー攻撃のインシデントが発生した実績のある車両には、攻撃を許した何らかの脆弱性、又はその攻撃の影響が残る可能性があるため、リスクレベルが高いとの判定が妥当である。そして第一車両では、そのような第二車両のリスクの高さに応じて適切な機能制限が適用される。

[0023] 例えば、前記第二車両の車両機能のリスクレベルが第三基準より高く、かつ前記第一車両の走行位置と前記第二車両の走行位置との距離が所定距離以下の場合、前記リスク対策指示生成部は、前記第一車両の車両機能のうち走行系機能に対する機能制限指示を生成してもよい。

[0024] 例えば自車両の近くを走行する車両がサイバー攻撃に対するリスクが高いため脅威となり得る場合、この近くを走行する車両が攻撃により不正走行を行うと、自車両と衝突する可能性がある。また、この近くを走行する車両と情報の授受をする自車両のサイバー攻撃に対するリスクも上がる。例えば不正な虚偽の情報が提供されたり、不正なコードが埋め込まれたメッセージが送信されたりし得る。上記の構成により、近くを走行する車両の変化するリスクレベルの高さ又は必要な対処に応じて適切なレベルの機能制限が自車両に適用される。また、この場合に走行系（加減速の制御系）の機能に対する機能制限をすることで、攻撃が防ぎきれなかった場合の事故の発生の可能性が抑えられる。なお、車両間の距離は、例えば、各車両のGPS（Global

Positioning System) から得られる位置情報から計算してもよいし、車両間通信の遅延時間、レーダー等により測定した距離など、いずれの方法で計算してもよい。また、第三基準は、第一車両のリスクレベルと比較される第一基準又は第二基準と同じものであってもよいし別のものであってもよい。

[0025] 例えば、前記第一車両の走行位置と前記第二車両の走行位置との距離が所定距離より遠い場合、前記機能制限解除指示生成部は、前記第一車両の前記走行系機能に対する前記機能制限解除指示を生成してもよい。

[0026] つまり、車両は移動体であり、一時は近くにあつてサイバー攻撃に対するリスクの高い、通信相手であれば脅威となり得る車両であっても、通信相手となり得ない距離まで離れば脅威ではなくなる。したがって、この相手と情報の授受がなくなった車両のリスクは低下するため、厳しい機能制限は不要となる。上記の構成により、第一車両では、変化するリスクの高さ又は必要な対処に応じて適切なレベルの機能制限が適用される。

[0027] また、本発明の一態様に係る情報処理方法は、第一車両及び第二車両の情報を処理する情報処理装置が車両で発生したサイバー攻撃のインシデントに関するインシデント情報を取得し、前記第二車両との通信を介して前記第二車両の状態に関する第二車両情報を取得し、前記インシデント情報と前記第二車両情報との一致度に基づいて、前記第二車両が持つ車両機能のリスクレベルを判定し、前記リスクレベルが第一基準より高い場合、前記第二車両の車両機能に対応する前記第一車両の車両機能に対する機能制限指示を生成し、前記機能制限指示を出力する。また、本発明の一態様に係るプログラムは、プロセッサ及びメモリを備え、第一車両及び第二車両の情報を処理する情報処理装置において、前記メモリを用いて前記プロセッサによって実行されることで、前記プロセッサに、車両で発生したサイバー攻撃のインシデントに関するインシデント情報を取得させ、前記第二車両との通信を介して前記第二車両の状態に関する第二車両情報を取得させ、前記インシデント情報と前記第二車両情報との一致度に基づいて、前記第二車両が持つ車両機能のリスクレベルを判定させ、前記リスクレベルが第一基準より高い場合、前記第

二車両の車両機能に対応する前記第一車両の車両機能に対する機能制限指示を生成させ、前記機能制限指示を出力させる。

[0028] これらの方法又はプログラムにより、多数の車両でのサイバー攻撃のインシデントに関する情報に基づいて、車両の状態に応じた第一車両のリスクが判定される。また、判定の結果得られたリスクが所定の基準を超えて高い場合、第一車両の機能を制限することで攻撃の発生、又は攻撃による悪影響の拡大を抑えることができる。

[0029] なお、これらの包括的または具体的な態様は、システム、集積回路、又はコンピュータ読み取り可能なＣＤ－ＲＯＭ等の記録媒体で実現されてもよく、装置、システム、方法、集積回路、コンピュータプログラム又は記録媒体の任意な組み合わせで実現されてもよい。

[0030] 以下、実施の形態について、図面を参照しながら具体的に説明する。

[0031] なお、以下で説明する実施の形態は、いずれも包括的または具体的な例を示すものである。以下の実施の形態で示される数値、形状、材料、構成要素、構成要素の配置位置及び接続形態、ステップ、ステップの順序、及び機能的な構成要素間の機能分担等は一例であり、本発明を限定する趣旨ではない。また、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、任意の構成要素として説明される。

[0032] (実施の形態１)

実施の形態１に係る情報処理装置を含むセキュリティリスク対策システムでは、多数の車両を対象に集められたサイバー攻撃のインシデントに関する情報（以下、インシデント情報ともいう）と、車両の現在の状態に関する情報（以下、車両情報ともいう）とを用いて、この車両が持つ機能（以下、車両機能ともいう）のサイバー攻撃を受ける可能性（リスクレベル）が判定される。本実施の形態における車両機能は、通信関連機能と、走行関連機能とに分類される。通信関連機能は、例えば、ＣＡＮ通信、Ｗｉ－Ｆｉ（登録商標）通信、Ｂｌｕｅｔｏｏｔｈ（登録商標）通信、ＬＴＥ通信の機能である。通信関連機能によって、これらの通信関連機能によって、車両が備える各

種の機器間、車両と乗員が持つ機器との間、又は車両と車両の外部にある機器との間で情報がやり取りされる。走行関連機能は、例えば、自動運転、各種の運転支援の機能である。このような機能を備える車両にとって、サイバー攻撃は異常な動作を招く脅威である。この脅威に対する対策としてセキュリティリスク対策システム 1 では、車両機能のリスクレベルが所定の基準より高い場合に、この車両機能を制限する。車両機能を制限することで、例えばサイバー攻撃による不正なデータの車載ネットワークへの侵入の抑制が図られる。また、不正なデータが車載ネットワークに流されたとしても、このデータによる異常な動作の発生の抑制が図られる。

[0033] [1. 構成]

図 1 は、本実施の形態に係る情報処理装置を含むセキュリティリスク対策システム 1 の構成例の概要を示す図である。

[0034] 図 1 に示される構成例では、セキュリティリスク対策サーバ 10 と、車両 20 と、インシデント情報収集サーバ 30 とがインターネット等の通信ネットワークを介して接続されて相互に情報の授受が可能である。

[0035] [1. 1 インシデント情報サーバ]

インシデント情報収集サーバ 30 は、例えば車両メーカーが設ける SOC (Security Operation Center) のサーバであり、プロセッサ及びメモリを含む 1 台又は複数台の情報処理装置で構成される。インシデント情報収集サーバ 30 には、各車両で実際に発生したサイバー攻撃に関するインシデントの履歴がインシデント情報として蓄積されている。図 2 は、本実施の形態 1 におけるインシデント情報のデータ構成例を示す図である。図 2 に示すデータ構成例では、インシデント情報に含まれる項目は下記のとおりである。

[0036] インシデント ID : インシデント識別用の文字列

発生日時 : インシデントの発生日時

発生地域 : インシデントが発生した場所を含む地域

車種 : インシデントが発生した車両の車種

リスク部品 : インシデントにおいて攻撃の標的となった部品。この例では

部品が型番で特定されている。

リスク機能：インシデントにおいて影響を受けた車両機能

侵入経路：車載ネットワークへの不正アクセスに利用された、又は不正な機器が設置された車載ネットワーク上の場所

脅威度：インシデントの影響の大きさについての安全に関する所定の基準に依る評価。例えば、侵入のみで車内の機器の動作に影響がないものは低。加減速、操舵、又はドライバー若しくはセンサーによる周辺状況の認識に影響するものは高。その他のものは中。

[0037] 上に挙げた項目は例であり、これらの項目すべてが本発明において必須ではなく、また、インシデント情報には上記以外の情報に関する項目が含まれてもよい。例えばリスク部品の製造者又はソフトウェアバージョン、インシデントが発生したときの車両の走行状態（走行中または停止）、インシデントが発生した車両を識別するための情報等が含まれてもよい。

[0038] このようなインシデント情報は多数の車両を対象として集められたものであり、大規模なデータ資産とも言える。そしてインシデント情報の少なくとも一部は必要に応じてセキュリティリスク対策サーバ10に提供される。インシデント情報収集サーバ30からセキュリティリスク対策サーバ10へのインシデント情報の提供は、例えば仮想専用線（図1の点線）を通じて行われるが、これに限定されない。

[0039] なお、インシデント情報収集サーバ30は複数でもよく、例えば車両メーカー各社のSOCのインシデント情報収集サーバからセキュリティリスク対策サーバ10にインシデント情報が提供されてもよい。インシデント情報は、このような複数の主体による共有を容易にするために、例えば脅威情報に関する国際標準であるSTIX（Structured Threat Information Expression）に準拠する形式で記述されていてもよい。

[0040] [1. 2 車両]

車両20は、セキュリティリスク対策システム1による目下のセキュリティリスク対策の実行対象の車両である。本開示では、目下のセキュリティ

スク対策の実行対象の車両を、車両全般又は特定の他の車両と区別して指すために、第一車両ともいう。

[0041] 車両20は車載ネットワーク200を備える。図3は、車載ネットワーク200の構成例を示す図である。

[0042] 車載ネットワーク200には、多数のECUが接続されている。図3に示される車載ネットワーク200にはCAN (Controller Area Network)、Ethernet (登録商標)、FlexRay (登録商標)といった異なる通信プロトコルによる複数のサブネットワークが含まれ、ECUはこれらのサブネットワークのいずれかに接続されている。これらのECUの中には、例えば図示しないセンサと接続されて車両内又は車両周辺の状況を示すデータを収集するもの、又はアクチュエータと接続され、制御信号を送出して車両上の装置を動作させるものが含まれる。また別の例として、ネットワークを流れるデータを監視する等、セキュリティに関する情報処理を行うECUも含まれ得る。上記の車両機能は、これらのECUのいずれかによって、又は複数のECU間のデータのやり取りを伴う連携によって実現される。通信プロトコルが異なるサブネットワーク同士は、ゲートウェイ220を介して接続されている。ゲートウェイ220は、サブネットワーク間でやり取りされるデータの通信プロトコル間での変換を行う。

[0043] また、この構成例では、車載ネットワーク200にIVI (In-Vehicle Infotainment) システム230が接続されている。

[0044] 各ECU及びIVIシステム230は、ゲートウェイ220と、通信モジュールとしての機能を有する外部通信装置240とを介して外部の通信ネットワークと接続する。上述のSOCに提供されるインシデントの発生に関する情報、及びセキュリティリスク対策サーバ10に提供される車両情報も、これらのECUのいずれかからこの経路で送信される。車両情報については、具体例を挙げて後述する。

[0045] [1. 3 セキュリティリスク対策サーバ]

セキュリティリスク対策サーバ10は、インシデント情報収集サーバ30

から取得するインシデント情報と、車両 20 から取得した車両情報とを用いて、車両 20 が持つ車両機能のサイバー攻撃に関するリスクレベルを判定する。また、セキュリティリスク対策サーバ 10 は、判定したリスクレベルが所定の基準より高い場合には、車両 20 の車両機能を制限する指示（以下、機能制限指示ともいう）を発行し、この指示を、通信ネットワークを介して車両 20 に送信する。セキュリティリスク対策サーバ 10 は、プロセッサ及びメモリを含む 1 台又は複数台の情報処理装置で構成される。

[0046] 図 4 は、セキュリティリスク対策サーバ 10 の構成例を示す図である。

[0047] セキュリティリスク対策サーバ 10 の構成要素には、インシデント情報取得部 11、車両情報取得部 12、蓄積部 13、リスク判定部 14、リスクポイント管理部 15、リスク対策指示生成部 16、指示出力部 17、及び機能制限解除指示生成部 18 が含まれる。

[0048] インシデント情報取得部 11 は、インシデント情報収集サーバ 30 からインシデント情報を受信して取得する。

[0049] 車両情報取得部 12 は、車両 20 の状態に関する情報である車両情報を受信して取得する。

[0050] 蓄積部 13 は、上記のインシデント情報、車両情報、及び後述のリスクレベルの判定に用いられるその他の情報が蓄積される。図 1 に記載のリスクレベル管理リスト及びリスクポイントテーブルも蓄積部 13 に蓄積されるその他の情報に含まれ、これらについては例を用いて後述する。

[0051] リスク判定部 14 は、上記のインシデント情報と車両 20 の車両情報との一致度に基づいて、車両 20 が持つ各種の車両機能のリスクレベルを判定する。

[0052] リスクポイント管理部 15 は、リスク判定部 14 による上記のリスクレベルの判定に用いられる情報の一種であるリスクポイント情報の管理を、インシデント情報に基づいて行う。

[0053] リスク対策指示生成部 16 は、リスク判定部 14 が判定したリスクレベルに応じて、リスク対策としての車両機能に対する制限（無効化の場合を含む

）に関する指示（以下、リスク対策指示ともいう）を生成する。

[0054] 機能制限解除指示生成部 18 は、リスク判定部 14 が判定したリスクレベルに応じて、車両機能に対する制限を解除する指示（以下、機能制限解除指示ともいう）を生成する。

[0055] 指示出力部 17 は、機能制限指示及び機能制限解除指示を車両 20 に送信する。

[0056] セキュリティリスク対策サーバ 10 のこれらの構成要素は、セキュリティリスク対策サーバ 10 を構成する情報処理装置において、例えばメモリに記憶される 1 個又は複数個のプログラムをプロセッサが実行することで実現される機能的な構成要素であってよい。セキュリティリスク対策システム 1 で実行されるセキュリティリスク対策のための処理は、セキュリティリスク対策サーバ 10 のこれらの構成要素が上記の機能を発揮しながら連携することで実行される。

[0057] なお、インシデント情報収集サーバ 30 とセキュリティリスク対策サーバ 10 とは個別に確立される存在でなくてもよい。例えば、インシデント情報収集サーバ 30 とセキュリティリスク対策サーバ 10 とは一体的に統合されたシステムであってもよい。また、インシデント情報収集サーバ 30 がセキュリティリスク対策サーバ 10 の一部であってもよく、例えばインシデント情報収集サーバ 30 が蓄積部 13 として機能してもよい。この場合のインシデント情報取得部 11 の機能は、処理に用いる範囲のインシデント情報を蓄積部 13 から取得することであってもよい。

[0058] [2. 動作]

次に、セキュリティリスク対策システム 1 で実行されるセキュリティリスク対策の処理の動作について説明する。

[0059] 図 5 は、セキュリティリスク対策サーバ 10 で実行されるこの処理の手順例を示すフロー図である。以下では、説明の便宜上、この手順を大きく二つの段階に分けて説明する。

[0060] ひとつは、多数の車両でのサイバー攻撃のインシデントに関するインシデ

ント情報を収集し、このインシデント情報に基づいて車両の様々な状態についてのリスクの高さを評価し、リスクポイントとして管理する（ステップS 1 及びステップS 2）の第一段階である。

[0061] もうひとつは、セキュリティリスク対策の実行対象である第一車両の状態を示す車両情報を取得し、この車両情報が示す第一車両の状態と、インシデント情報に表れる車両の状態との一致度に基づいて、リスクポイントから第一車両の各車両機能のリスクレベルを算出し、算出したリスクレベルに基づいて、車両機能の制限又は制限の解除を実行するか否かについて判定し、必要に応じて第一車両のリスク対策指示を出力するまで（ステップS 3 からステップS 7）の第二段階である。

[0062] [2. 1 第一段階]

図6は、インシデント情報収集サーバ30とセキュリティリスク対策サーバ10との連携を含む手順を示すシーケンス図であり、図5に示される処理手順例の第一段階に関する。

[0063] 第一段階では、まずインシデント情報収集サーバ30からセキュリティリスク対策サーバ10へとインシデント情報が送信される（ステップS 3010）。インシデント情報は図2にデータ構成例が示されるものであり、再度の説明は省略する。インシデント情報の送信は一定の時間間隔で行われてもよいし、所定数のレコード又は脅威度の高いインシデントのレコードが追加されたとき等の、所定のイベントの発生をトリガに行われてもよい。また、セキュリティリスク対策サーバ10からの要求に応じて送信されてもよい。

[0064] セキュリティリスク対策サーバ10では、インシデント情報取得部11によって受信されたインシデント情報がいったん蓄積部13に保存される（ステップS 10）。ここまでの図5のフロー図のステップS 1に相当する。次いでセキュリティリスク対策サーバ10では、リスクポイント管理部15によって、このインシデント情報に基づいてリスクポイントテーブルが更新される（ステップS 20）。ステップS 20は、図5のフロー図のステップS 2に相当する。

[0065] リスクポイントテーブルとは、車両の様々な状態のサイバー攻撃に対するリスクの評価値（リスクポイント）をまとめたテーブルであり、蓄積部13に保持される。リスクポイントはインシデント情報が示すインシデントの実績に基づいて決定され、新たなインシデント情報が取得されると更新される。リスクポイントの更新処理については、例を用いて後述する。

[0066] 図7Aから図7Gは、本実施の形態におけるリスクポイントテーブルの例である。

[0067] 図7Aに示すリスクポイントテーブルは、車両の状態としての車両が搭載する機器、この例ではECU及びIVIシステムの、型番及びソフトウェアのバージョン別のリスクポイントに関する。図7Bに示すリスクポイントテーブルは、車両の状態としての車両が搭載する機器の製造者（メーカー）別のリスクポイントに関する。図7Cに示すリスクポイントテーブルは、車両の状態としての車両が走行している地域別のリスクポイントに関する。図7Dに示すリスクポイントテーブルは、車両の状態としての車両の車種別のリスクポイントに関する。図7Eに示すリスクポイントテーブルは、車両の状態としての車両が搭載する車載ネットワークで使用されている通信プロトコル別のリスクポイントに関する。図7Fに示すリスクポイントテーブルは、車両の状態としての搭載する車両機能別のリスクポイントに関する。図7Gに示すリスクポイントテーブルは、車両の状態としての車両で有効な車両機能ごとの走行状態別のリスクポイントに関する。走行状態は、この例では2つの走行速度帯及び停止の計3つの状態に分類される。

[0068] インシデント情報に基づいてリスクポイントが決定されることで、例えばこれらの状態別のサイバー攻撃に対する脆弱性又は攻撃者からの狙われやすさの現実の傾向が反映される。このようなリスクポイントの決定を含むリスクポイントテーブルの更新（又は作成）処理の手順について、フロー図を用いて次に説明する。

[0069] 図8は、リスクポイント管理部15による上記の各リスクポイントテーブルの更新処理の手順例を示すフロー図である。この処理は、図5のフロー図

のステップS 2 及び図6のシーケンス図のステップS 2 0に相当する。以下の説明は、図7 Aから図7 Gに示されるリスクポイントテーブルのいずれか及び図2に示されるインシデント情報を適宜参照して理解されたい。

[0070] リスクポイント管理部1 5は、リスクポイントテーブル内のポイントをいったん初期化してから（ステップS 2 1 0）、リスクポイントテーブルに含まれる状態の種類を示す項目に対して順次、以下に説明するステップS 2 1 1からステップS 2 1 8までを実行する（図8中、テーブル項目ループ）。状態の種類を示す項目とは、本実施の形態の例では各リスクポイントテーブルの太い縦罫線の左に配置され、図7 Aの搭載機器に関するリスクポイントテーブルでは、「E C U - a」及び「1 . 0 . 1」等である。図7 Dの車種に関するリスクポイントテーブルでは、「X」、「Y」等などである。

[0071] ステップS 2 1 1では、リスクポイント管理部1 5は、インシデント情報の一レコードに、上記の状態の種類を示す項目に対応する情報が含まれるか否か判定する。当該レコードが対応する情報を含む場合（ステップS 2 1 1でY e s）、当該レコードにある脅威度に応じた所定値を、この項目のリスクポイントとして加算する（ステップS 2 1 2）。脅威度に応じた所定値としては、より高い脅威度により大きな値が定められている。これにより、車両の安全な走行により深刻な影響を与えたインシデントに関与した項目には、大きな値のリスクポイントが付与される。このような脅威度に応じた所定値は、例えば蓄積部1 3に保持される図示しないテーブルで管理されていてもよい。

[0072] 次にリスクポイント管理部1 5は、当該レコードに含まれる発生日時から所定の時間が既に経過しているか否か判定する（ステップS 2 1 3）。所定の時間が既に経過している場合（ステップS 2 1 3でY e s）、ステップS 2 1 2での加算後のリスクポイントから所定値を減算する（ステップS 2 1 4）。これは、ある程度以上古い脅威は、例えば車両、E C U、又は通信機器等のメーカーによって対策が実施された結果、発生当時に比べて脅威度が下がっている可能性が高いことに基づくリスクポイントの調整である。

- [0073] なお、テーブル項目ループの中でステップS 2 1 1からステップS 2 1 4までは、インシデント情報に含まれるレコードに対して順次実行される（図8中、インシデント情報ループ）。つまり、例えば状態の種類を示す車種の項目「X」について、車種のフィールドに「X」を含む全レコードの脅威度に応じたリスクポイントが加算され、そのレコードのうちある程度以上古いレコードの件数に応じて、リスクポイントから所定値が減算される。なお、ステップS 2 1 1でN oであったレコードについてはステップS 2 1 2からS 2 1 4まで、ステップS 2 1 3でN oであったレコードについてはステップS 2 1 4が省略される。
- [0074] 次にリスクポイント管理部15は、項目に対応する情報を含むレコードの件数が所定の基準値n以上か否か判定する（ステップS 2 1 5）。このレコードの件数が基準値n以上である場合（ステップS 2 1 5でY e s）、リスクポイント管理部15は、この項目のリスクポイントに所定値を加算する（ステップS 2 1 6）。これは、多くのインシデントに関与した状態には、脆弱性等の何らかのインシデント発生の要因がある可能性が高いことに基づくリスクポイントの調整である。
- [0075] 次にリスクポイント管理部15は、現在から遡る所定期間における、項目に対応する情報を含むレコードの件数が所定の基準値m以上か否か判定する（ステップS 2 1 7）。このレコードの件数が基準値m以上である場合（ステップS 2 1 7でY e s）、リスクポイント管理部15は、この項目のリスクポイントに所定値を加算する（ステップS 2 1 8）。これは、例えばこの項目に関する未知の脆弱性が攻撃者によって標的にされ始めている等の、インシデントの何らかの傾向がある可能性が高いことに基づくリスクポイントの調整である。
- [0076] ここまでのステップをリスクポイントテーブルに含まれる状態の種類を示す項目すべてについて実行することで、当該リスクポイントテーブルの更新が完了する。このようにして算出されたリスクポイントの大きさは、サイバー攻撃に対する車両の種々の状態の、セキュリティリスク対策サーバ10が

取得した最新のインシデント情報に基づくリスクの高さを反映する。

[0077] このように更新されたリスクポイントテーブルが、次の第二段階で実行される第一車両20のリスクレベルの判定に用いられる。

[0078] [2.2 第二段階]

[2.2.1 第一車両のリスクレベル判定]

図9は、第一車両20とセキュリティリスク対策サーバ10との連携を含む手順を示すシーケンス図である。また、このシーケンス図は図5に示される処理手順例の、第二段階に関する。

[0079] 第一車両20からセキュリティリスク対策サーバ10へと車両情報が送信される（ステップS3020）。車両情報は、第一車両20の状態に関する情報であり、以下、第一車両情報ともいう。図10及び図11は、それぞれこの車両情報のデータ構成の一例を示す図である。

[0080] 図10の車両情報は、第一車両20が備える機器、特に情報処理又は通信に関する機器に関する情報を含み、以下では機器リストともいう。このような内容の変更の頻度が低い車両情報は、例えば第一車両20の各日の最初の始動時等の日次処理で、又は車載ネットワーク200上で機器構成の変更が発生した時等の特定のイベントをトリガにセキュリティリスク対策サーバ10へ送信されてもよい。ここでの機器構成の変更とは、例えば機器の追加又は削除のみならず、ソフトウェアの更新も含む。また、ここでの関連機能とは、各機器によって送受信又はその他の処理がなされる情報が、第一車両20で利用される車両機能である。別の表現をすると、各機器が故障したりサイバー攻撃を受けたりした場合に悪影響を受ける可能性がある車両機能である。

[0081] 図11のデータ構成例は、第一車両20の直近の様々な状態に関する車両情報の例である。図11の車両情報には、走行位置及び走行状態といった変更の頻度が高い情報が含まれているため、例えば数分以下の頻度で定期的に、又は第一車両20の状態に変化が生じる度にセキュリティリスク対策サーバ10へ随時送信されてもよい。

[0082] なお、図 10 及び図 11 に示した車両情報の例にそれぞれ含めた情報の項目は一例であり、これに限定されない。例えば、図 10 及び図 11 に示した全項目を含む種類の車両情報として送信されてもよい。また、図 11 に示される項目のうち、車種、通信プロトコル、搭載機能等の変更の頻度が比較的低い項目は、その他の変更の頻度が高い項目と別のスケジュールで第一車両 20 からセキュリティリスク対策サーバ 10 へ送信されてもよい。また、いずれの例でも、すべての項目の情報が毎回送信されるのではなくてもよい。例えば、セキュリティリスク対策サーバ 10 で第一車両 20 を識別するための車両 ID と、前回の送信時から変更のあった項目の情報とが送信されてもよい。また、これらの項目の全てが必須ではなく、又は他の項目も含まれてもよい。また、各項目により詳細な情報が含まれてもよい。例えば走行位置の項目は、図 11 での市町村のような地域で表現される情報に限定されず、第一車両 20 が備える GPS 受信機で取得される経緯度の情報が含まれてもよい。

[0083] セキュリティリスク対策サーバ 10 では、車両情報取得部 12 によって受信された車両情報がいったん蓄積部 13 に保存される（ステップ S30）。ここまでの図 5 のフロー図のステップ S3 に相当する。

[0084] 次にセキュリティリスク対策サーバ 10 では、リスク判定部 14 が、リスクポイントテーブル及び車両情報を用いてリスクレベルを判定し、リスクレベル管理リストを作成（更新の場合を含む）する（ステップ S40）。ステップ S40 は図 5 のフロー図のステップ S4 に相当する。続く第二段階については後述する。

[0085] リスクレベル管理リストとは、第一車両 20 が持つ車両機能ごとに判定された、サイバー攻撃に対するリスクレベル（リスクの高さ）のリストであり、蓄積部 13 に保持される。図 12 に示される例では、リスクレベルは、上述のインシデント情報に基づくリスクポイントテーブルと車両情報とを用いて算出されるリスクスコアで表されている。以下では、このリスクレベル管理リスト及びリスクレベルの算出処理について例を用いて説明する。

[0086] 図12は、本実施の形態におけるリスクレベル管理リストのデータ構成例を示す図である。

[0087] 左端の欄は第一車両20が持つ車両機能の名称を示す。その右の欄は、各車両機能の種類を示す。さらにその右の欄は、各車両機能がセキュリティリスク対策システム1において制限される場合の、その制限の詳細な内容である。また、さらにその右の欄は、各車両機能がセキュリティリスク対策システム1において無効化される場合の詳細な内容である。ここまでの各欄の内容は基本的に変更されない。ただし、第一車両20の車両機能に増減があれば、その車両機能に関する行がリストに追加又はリストから削除される。また、セキュリティリスク対策システム1で第一車両20の車両機能の制限又は無効化に関する運用ルールに変更が生じた場合には、各欄の内容は変更され得る。

[0088] リスク判定部14によって判定された各車両機能のリスクレベルは、この例では右端の欄に入力されているリスクスコアで表されている。この欄に入力されるリスクスコアの算出の処理の手順について、フロー図を用いて次に説明する。

[0089] 図13は、リスク判定部14によるリスクスコアの算出処理の手順例を示すフロー図である。この処理は図5のフロー図のステップS4及び図9のシーケンス図のステップS40に相当する。以下の説明は、図7Aから図7Gに示されるリスクポイントテーブル、図10及び図11の車両情報、並びに図12に示されるリスクレベル管理リストを適宜参照して理解されたい。また、以下の説明では、図11に示される車両情報を取得したセキュリティリスク対策サーバ10のリスク判定部14が、この車両情報の走行状態の欄にある「自動運転」の車両機能についてのリスクスコアを算出する場合を例に用いる。

[0090] リスク判定部14は、リスクレベル管理リスト内のリスクスコアをいったん初期化する（ステップS410）。次いでリスク判定部14は、蓄積部13に保存されている車両情報である図10の機器リストを読み込むと（ステ

ップS 4 1 1)、ステップS 4 1 2からステップS 4 1 4までを、機器リストに型番が挙げられている機器に対して順次実行する(図12中、機器ループ)。

[0091] ステップS 4 1 2では、リスク判定部14は、車両機能が機器と関連するか否かを判定する。この判定は、図10に示す機器リストの関連機能の情報に基づいて行われる。車両機能「自動運転」についてのリスクスコアが算出されるこの例では、型番「E C U - a」に対するステップS 4 1 2で、車両機能がこの機器と関連すると判定される(ステップS 4 1 2でY e s)。

[0092] ステップS 4 1 2でY e sの場合、リスク判定部14は、この機器のリスクポイントを算出する(ステップS 4 1 3)。図14Aは、第一車両20が備える各機器のリスクポイントの算出処理の手順例である。

[0093] リスク判定部14は、第一車両20が備える機器のリスクポイントをいったん初期化してから、リスクポイントの算出対象である機器の型番及び当該機器のソフトウェアバージョンを機器リストから読み出す(ステップS 4 1 30、S 4 1 31、S 4 1 32)。

[0094] 次にリスク判定部14は、図7Aに示す機器のリスクポイントテーブルを参照して、ステップS 4 1 31及びS 4 1 32でそれぞれ読み出した型番及びソフトウェアバージョンに対応するリスクポイントを読み取る(ステップS 4 1 33)。この例で図10に示す機器リストの先頭にある型番「E C U - a」及びソフトウェアバージョン「1. 0. 2」を読み出したリスク判定部14は、図7Aのリスクポイントテーブルからリスクポイント「2」を読み取る。ステップS 4 1 33で読み取られたリスクポイントは、当該機器のリスクポイントに加算される(ステップS 4 1 34)。

[0095] 次にリスク判定部14は、当該機器の製造者を読み出し(ステップS 4 1 35)、読み出した製造者に対応するリスクポイントを、図7Bに示す機器の製造者のリスクポイントテーブルを参照して読み取る(ステップS 4 1 36)。この例で図10に示す機器リストの先頭にある製造者「A社」を読み出したリスク判定部14は、ステップS 4 1 36でリスクポイントテーブル

からリスクポイント「1」を読み取る。ステップS 4 1 3 6で読み取られたリスクポイントは、当該機器のリスクポイントに加算される（ステップS 4 1 3 7）。つまりこの例では、ステップS 4 1 3 7の後の当該機器のリスクポイントは $2 + 1 = 3$ である。リスク判定部1 4は、このリスクポイントを当該機器のリスクポイントとして出力して（ステップS 4 1 3 8）、当該機器についてのリスクポイントの算出を終了する。

[0096] ステップS 4 1 3 8で出力されたリスクポイントは、現在のリスクスコアの算出対象の車両機能、つまりこの例では「自動運転」のリスクスコアに加算される（ステップS 4 1 4）。ステップS 4 1 4の実行後、又はステップS 4 1 2でN oの場合、リスク判定部1 4の処理は図1 3のフロー図のステップS 4 1 2に戻って、車両機能「自動運転」が、図1 0の機器リストにおける次の機器と関連するかの判定に移る。以降、リスク判定部1 4は、機器ループを機器リストに含まれる全ての機器について実行する。

[0097] このようにして算出される第一車両2 0が備える機器のリスクポイントの大きさには、第一車両2 0以外の車両で発生したものも含むサイバー攻撃のインシデント情報に基づく車載機器のリスクの高さが反映されている。

[0098] ステップS 4 1 5からは、リスク判定部1 4は図1 1に示す車両情報を用いて、機器以外の第一車両2 0の状態について、サイバー攻撃に対するリスクの大きさを判定する。

[0099] ステップS 4 1 5では、第一車両2 0の状態としての走行位置についてのリスクの大きさを示すリスクポイントが算出される。図1 4 Bは、第一車両2 0の走行位置のリスクポイントの算出処理の手順例である。

[0100] リスク判定部1 4は、走行位置のリスクポイントをいったん初期化してから、リスクポイントの算出対象である第一車両2 0の走行位置を図1 1の車両情報から読み出す（ステップS 4 1 5 0、S 4 1 5 1）。

[0101] 次にリスク判定部1 4は、図7 Cに示す走行位置のリスクポイントテーブルを参照して、ステップS 4 1 5 1で読み出した走行位置に対応するリスクポイントを読み取る（ステップS 4 1 5 2）。この例で図1 1に示す車両情

報にある走行位置「東京都〇〇区」を読み出したリスク判定部14は、図7Cのリスクポイントテーブルからリスクポイント「2」を読み取る。ステップS4152で読み取られたリスクポイントは、ステップS4150で初期化されていた走行位置のリスクポイントに加算され、出力される（ステップS4153、S4154）。以上で走行位置についてのリスクポイントの算出は終了する。

[0102] ステップS4154で出力されたリスクポイントは、現在のリスクスコアの算出対象の車両機能、つまりこの例では、ステップS414後の「自動運転」のリスクスコアに加算される（ステップS416）。

[0103] 続くステップS417では、第一車両20の状態としての車種についてのリスクの大きさを示すリスクポイントが算出される。図14Cは、第一車両20の車種のリスクポイントの算出処理の手順例である。

[0104] リスク判定部14は、車種のリスクポイントをいったん初期化してから、リスクポイントの算出対象である第一車両20の車種を図11の車両情報から読み出す（ステップS4170、S4171）。

[0105] 次にリスク判定部14は、図7Dに示す車種のリスクポイントテーブルを参照して、ステップS4171で読み出した車種に対応するリスクポイントを読み取る（ステップS4172）。この例で図11に示す車両情報にある車種「X」を読み出したリスク判定部14は、図7Dのリスクポイントテーブルからリスクポイント「1」を読み取る。ステップS4172で読み取られたリスクポイントは、ステップS4170で初期化されていた車種のリスクポイントに加算され、出力される（ステップS4173、S4174）。以上で車種についてのリスクポイントの算出は終了する。

[0106] ステップS4174で出力されたリスクポイントは、現在のリスクスコアの算出対象の車両機能、つまりこの例では、ステップS416後の「自動運転」のリスクスコアに加算される（ステップS418）。

[0107] 続くステップS419では、第一車両20の状態としての使用されている通信プロトコルについてのリスクの大きさを示すリスクポイントが算出され

る。図 1 4 D は、第一車両 2 0 で使用されている通信プロトコルのリスクポイントの算出処理の手順例である。

[0108] リスク判定部 1 4 は、通信プロトコルのリスクポイントをいったん初期化してから、リスクポイントの算出対象である第一車両 2 0 で使用されている通信プロトコルを図 1 1 の車両情報から読み出す（ステップ S 4 1 9 0、S 4 1 9 1）。

[0109] 次にリスク判定部 1 4 は、図 7 E に示す侵入経路のリスクポイントテーブルを参照して、ステップ S 4 1 9 1 で読み出した通信プロトコルに対応するリスクポイントを読み取る（ステップ S 4 1 9 2）。この例で図 1 1 に示す車両情報にある通信プロトコル「CAN」、「FlexRay」及び「MOST」を読み出したリスク判定部 1 4 は、図 7 E のリスクポイントテーブルから、各通信プロトコルに対応付けられているリスクポイント「8」、「1」、「2」を読み取る。ステップ S 4 1 9 2 で読み取られたリスクポイントは、ステップ S 4 1 7 0 で初期化されていた通信プロトコルのリスクポイントに加算され、出力される（ステップ S 4 1 9 3、S 4 1 9 4）。以上で通信プロトコルについてのリスクポイントの算出は終了する。

[0110] ステップ S 4 1 9 4 で出力されたリスクポイントは、現在のリスクスコアの算出対象の車両機能、つまりこの例では、ステップ S 4 1 8 後の「自動運転」のリスクスコアに加算される（ステップ S 4 2 0）。

[0111] 続くステップ S 4 2 1 では、第一車両 2 0 の状態としての搭載される車両機能（各図では搭載機能と表記）についてのリスクの大きさを示すリスクポイントが算出される。図 1 4 E は、第一車両 2 0 が搭載する車両機能のリスクポイントの算出処理の手順例である。

[0112] リスク判定部 1 4 は、搭載される車両機能のリスクポイントをいったん初期化してから、リスクポイントの算出対象である第一車両 2 0 が搭載する車両機能を図 1 1 の車両情報から読み出す（ステップ S 4 2 1 0、S 4 2 1 1）。

[0113] 次にリスク判定部 1 4 は、図 7 F に示す搭載される車両機能のリスクポイ

ントテーブルを参照して、ステップS 4 2 1 1で読み出した搭載される車両機能に対応するリスクポイントを読み取る（ステップS 4 2 1 2）。この例で図1 1に示す車両情報にある搭載される車両機能「運転支援」、「自動運転」及び「W i - F i」を読み出したリスク判定部1 4は、図7 Fのリスクポイントテーブルから、各機能名に対応付けられているリスクポイント「2 0」、「5」、「1 0」を読み取る。ステップS 4 2 1 2で読み取られたリスクポイントは、ステップS 4 2 1 0で初期化されていた搭載される車両機能のリスクポイントに加算され、出力される（ステップS 4 2 1 3、S 4 2 1 4）。以上で搭載される車両機能についてのリスクポイントの算出は終了する。

[0114] ステップS 4 2 1 4で出力されたリスクポイントは、現在のリスクスコアの算出対象の車両機能、つまりこの例では、ステップS 4 2 0後の「自動運転」のリスクスコアに加算される（ステップS 4 2 2）。

[0115] 続くステップS 4 2 3では、第一車両2 0の状態としての走行状態についてのリスクの大きさを示すリスクポイントが算出される。図1 4 Fは、第一車両2 0の走行状態のリスクポイントの算出処理の手順例である。

[0116] リスク判定部1 4は、走行状態のリスクポイントをいったん初期化してから、リスクポイントの算出対象である第一車両2 0の走行状態を図1 1の車両情報から読み出す（ステップS 4 2 3 0、S 4 2 3 1）。

[0117] 次にリスク判定部1 4は、図7 Gに示す走行状態のリスクポイントテーブルを参照して、ステップS 4 2 3 1で読み出した走行状態に対応するリスクポイントを読み取る（ステップS 4 2 3 2）。この例で図1 1に示す車両情報に走行状態「自動運転」及び「停止」を読み出したリスク判定部1 4は、図7 Gのリスクポイントテーブルから、機能名「自動運転」下の「停止」に対応付けられているリスクポイント「3」を読み取る。ステップS 4 2 3 2で読み取られたリスクポイントは、ステップS 4 2 3 0で初期化されていた走行状態のリスクポイントに加算され、出力される（ステップS 4 2 3 3、S 4 2 3 4）。以上で走行状態についてのリスクポイントの算出は終了する

。

[0118] ステップS 4 2 3 4 で出力されたリスクポイントは、現在のリスクスコアの算出対象の車両機能、つまりこの例では、ステップS 4 2 2 後の「自動運転」のリスクスコアに加算される（ステップS 4 2 4）。

[0119] ここまでの手順で、第一車両20の状態に関する各種の項目（自動運転に関連する機器、走行位置、車種、通信プロトコル、搭載機能、走行状態）についてのリスクポイントが算出され、その合計が自動運転のリスクスコアとして算出される。リスク判定部14は、このように算出したリスクスコアを、図12に示すリスクレベル管理リストにおける自動運転のリスクスコアの欄にいったん書き込む（ステップS 4 2 5）。これによりリスクレベル管理リストが作成される。

[0120] このように、セキュリティリスク対策サーバ10は、目下のセキュリティリスク対策の実行対象である第一車両以外の車両を含む多数の車両から集められた、その発生時の各車両の状態と、実際に発生したサイバー攻撃の脅威度とを示すインシデント情報を取得する。そしてこのインシデント情報に基づいて、サイバー攻撃の発生時の車両の様々な状態別のリスクポイントを、発生件数、発生時期、脅威度等に応じて数値化して取得する。

[0121] さらに、セキュリティリスク対策サーバ10では、第一車両から取得される車両情報が示す当該車両の状態のうち、上記のインシデント情報が示すサイバー攻撃の発生時の車両の状態との一致するものについてのリスクポイントが積算されてリスクスコアとして算出される。つまり、車両情報が示す第一車両の状態とインシデント情報が示す状態との一致度が高いほどリスクスコアは高くなる。また、第一車両の状態が、より最近の、より高頻度な、又はより脅威度の高いサイバー攻撃が発生した時の車両の状態と一致すれば、リスクスコアはより高くなる。

[0122] このようなリンクスコアは、車両情報が示す状態にある第一車両がサイバー攻撃を受ける可能性の高さ（リスクレベル）を示すものである。また、リスクポイントの数値化には、セキュリティリスク対策サーバ10が取得した

最新のインシデント情報が用いられ、例えば第一車両では未発生のサイバー攻撃の事例又はさらにその傾向も反映され得る。したがって、車両単体にとっては既知のサイバー攻撃のみならず、未知のものについてもリスクレベルを示すものである。

[0123] 次に、このようなリスクスコアを用いた第一車両でのリスク制御の処理について説明する。

[0124] [2. 2. 2 リスクレベルに応じたリスク制御（機能制限まで）]

図15は、セキュリティリスク対策サーバ10において実行される、リスクレベル管理リストに含まれるリスクスコアを用いたリスク制御処理の手順例を示すフロー図であり、図5に示される処理手順例の第二段階の一部に関する。

[0125] まずリスク判定部14によって、リスクレベル管理リストに含まれる、現在有効な車両機能についてのリスクスコアが読み取られる（ステップS500）。このステップは、図5のフロー図のステップS5及び図9のシーケンス図のステップS50に相当する。

[0126] 以下のステップでは、このリスクスコアと、リスクスコアに関する2つの閾値（第一閾値、第二閾値）とを用いて、この有効な車両機能の制限（無効化を含む）を実行するか否かについて判断される。第一閾値は、車両機能を制限するか否かの判断のためのリスクレベルを示す基準である。第二閾値は第一閾値よりも大きいリスクスコアの値であり、車両機能を無効化するか否かの判断のためのより高いリスクレベルを示す基準である。第一閾値は、本実施の形態における第一基準の例であり、第二閾値は第二基準の例である。

[0127] リスク判定部14は、ステップS500で読み取ったリスクスコアが第二閾値以上であるか判定する（ステップS600）。リスクスコアが第二閾値未満である場合（ステップS600でN）、リスク判定部14はさらにこのリスクスコアが第一閾値以上であるか判定する（ステップS601）。ステップS600及びステップS601は、図5のフロー図のステップS6及び図9のシーケンス図のステップS60に相当する。

- [0128] リスクスコアが第一閾値未満の場合（ステップS601でNo）、車両機能は制限も無効化もされないでリスク制御の処理がいったん終了する。
- [0129] リスクスコアが第二閾値以上の場合（ステップS600でYes）、リスク判定部14は、リスク対策指示生成部16に当該車両機能に対する無効化の指示（以下、機能無効化指示ともいう）を生成させる。リスク対策指示生成部16は、リスクレベル管理リストでリスク制御対象の車両機能の「無効化」欄の内容に従って、機能無効化指示を生成する（ステップS610）。生成された機能無効化指示は、指示出力部17から出力され（ステップS620）、第一車両20に送信される。
- [0130] リスクスコアが第二閾値未満かつ第一閾値以上の場合（ステップS601でYes）、リスク判定部14は、リスク対策指示生成部16に当該車両機能に対する制限の指示（以下、機能制限指示ともいう）を生成させる。リスク対策指示生成部16は、リスクレベル管理リストでリスク制御対象の車両機能の「制限」欄の内容に従って、機能制限指示を生成する（ステップS611）。
- [0131] 生成された機能制限指示は指示出力部17から出力され（ステップS620）、第一車両20に送信される。ステップS610及びステップS611は、図9のシーケンス図のステップS61に相当する。また、ステップS620は、図9のシーケンス図のステップS62に相当する。
- [0132] このように、図15のフロー図に手順例が示される処理によって、第一段階で算出されたリスクスコア、つまりリスクレベルに応じた車両機能の制限が実行される。有効である車両機能のサイバー攻撃を受ける可能性がある程度以上に高い場合には、この車両機能を制限することで、車載ネットワークへの攻撃者による侵入、不正データの送出又は送出されても悪影響の発生若しくは拡大を抑えることができる。
- [0133] [2. 2. 3 リスクレベルに応じたリスク制御（リスクレベルの再判定を含む）]

ここまで、第一車両20の車両機能を、第一車両20の状態に応じて制限

するか否かの判定までの処理手順を説明した。以下では、第一車両 20 の状態に変化があった場合に、車両機能への制限に変化を加える処理手順について例を用いて説明する。これにより、第一車両 20 の状態の変化に追従性の高いリスク対策が可能になる。

[0134] なお、上述のとおり、図 11 に示される車両情報のうち、走行位置及び走行状態は比較的頻繁に変わり得る。走行位置又は走行状態が変化した場合、セキュリティリスク対策サーバ 10 では、これらの点のみについてのリスクスコアの修正（リスクレベルの再判定）がなされてもよい。これにより、セキュリティリスク対策サーバ 10 の負荷増大、及びリスクレベル判定実行周期の長期化を抑え、第一車両 20 の状態の変化に追従性の高いリスク対策が可能になる。以下では、走行位置に変化があった場合、走行状態に変化があった場合の二つの例を用いて車両機能への制限に変化を加える処理手順について説明する。

[0135] 図 16A 及び図 16B は、それぞれ第一車両 20 とセキュリティリスク対策サーバ 10 との連携を含む手順を示すシーケンス図である。また、各シーケンス図が示すのは、図 9 のシーケンス図が示す手順の変形であり、共通の手順は共通の参照符号で示される。以下、各図が示す手順と図 9 が示す手順との差異を中心に説明する。

[0136] 図 16A の手順では、第一車両 20 から送信されるのは図 10 及び図 11 に示される第一車両情報に代えて、走行位置変化通知である点が図 9 のシーケンス図が示す手順と異なる。走行位置変化通知は、例えば第一車両 20 が地域間の境界を越えた時にセキュリティリスク対策サーバ 10 に送信され、新たな現在の走行位置を示す通知である。なお、この通知は、図 11 に示される車両情報の一部である、車両 ID 及び走行位置の項目のみが送信されることで行われてもよい。この通知を受けたセキュリティリスク対策サーバ 10 では、走行位置変化通知が蓄積部 13 に保存された後（ステップ S30A）、リスク判定部 14 が、図 13 に示すフロー図の手順ではステップ S415、S416 及び S425 を行い（ステップ S40A）、引き続いて第二段

階の処理を実行する。

[0137] 図16Bの手順では、第一車両20から送信されるのが図10及び図11に示される第一車両情報に代えて、走行状態変化通知である点が図9のシーケンス図が示す手順と異なる。走行状態変化通知は、例えば第一車両20の走行状態が低速走行から所定の速度以上である高速走行に移行した場合にセキュリティリスク対策サーバ10に送信される、新たな現在の走行速度帯を示す通知である。なお、この通知は、図11に示される車両情報の一部である、車両ID及び走行状態の項目のみが送信されることで行われてもよい。この通知を受けたセキュリティリスク対策サーバ10では、走行状態変化通知が蓄積部13に保存された後（ステップS30B）、リスク判定部14が、図13に示すフロー図の手順ではステップS423からS425を行い（ステップS40B）、引き続いて第二段階の処理を実行する。

[0138] [2.2.4 リスクレベルに応じたリスク制御（機能制限解除）]

ここまでの説明では、リスクレベルに応じて有効である車両機能に制限が加えられる例を挙げたが、本実施の形態に係るセキュリティリスク対策サーバ10を含むセキュリティリスク対策システム1では、リスクレベルが第一基準よりも低下したとの判定がされたことに応じて車両機能の制限の解除処理が実行されてもよい。これにより、第一車両20のドライバーは、リスクレベルが高まったためにいったんは制限された、情報処理を伴う高度な機能の利益を再び受けることができる。以下、この車両機能の制限の解除処理について説明する。

[0139] 図17は、セキュリティリスク対策サーバ10において実行される、リスクレベル管理リストに含まれるリスクスコアを用いたリスク制御処理の手順例を示すフロー図であり、図5に示される処理手順例の第二段階の一部に関する。この手順が実行されるのは、例えば図15のフロー図に手順例が示される処理によってリスク対策指示がいったん出力されたより後に、第一車両20からの新しい第一車両情報が受信され、リスクレベル管理リストが再作成（更新）された場合であり、図5のフロー図でいえば、2回目以降のリス

ク制御ループで実行され得る。また、この手順は、第一車両 20 から上述の走行位置変化通知又は走行状態変化通知が受信された時、又はリスクポイントテーブルが更新された場合に実行されてもよい。

[0140] リスク判定部 14 は、リスクレベル管理リストからあらためて読み取ったリスクスコアが第一閾値未満か否か判定する（ステップ S 700）。リスクスコアが第一閾値未満の場合（ステップ S 700 で Yes）、リスク判定部 14 は、機能無効化指示が未発行か否か判定する（ステップ S 701）。機能無効化指示が未発行である場合（ステップ S 701 で Yes）、リスク判定部 14 は、当該車両機能に対する機能制限の解除の指示（以下、機能制限解除指示ともいう）を機能制限解除指示生成部 18 に生成させる。機能制限解除指示生成部 18 は機能制限解除指示を生成し（ステップ S 710）、生成された機能制限解除指示は、指示出力部 17 から出力され（ステップ S 720）、第一車両 20 に送信される。ステップ S 700 及びステップ S 701 は、図 5 のフロー図のステップ S 7 に相当する。

[0141] リスクスコアが第一閾値以上の場合（ステップ S 700 で No）、又は機能無効化指示が発行済みである場合（ステップ S 701 で No）、機能制限には変更が加えられることなくこの処理は終了する。

[0142] なお、上記の処理手順例では、車両機能が無効化されている場合には機能制限は解除されない。これは、車両機能が無効化されるのは、リスクレベルが非常に高い場合であることを考慮して、第一車両 20 をサイバー攻撃からより確実に守るための措置である。車両機能の無効化は、例えば第一車両 20 の車両メーカー又は SOC によって安全が確認された後に解除されてもよい。

[0143] また、車両機能の制限の解除処理は、上述した走行位置又は走行状態が変化した場合のリスクスコアの再算出の後に実行されてもよい。図 18 A は、リスクスコアの再算出の後に実行される車両機能の制限の解除処理の手順例を示すフロー図である。

[0144] この手順例では、セキュリティリスク対策サーバ 10 において走行位置変

化通知が取得され（ステップS300A）、蓄積部13に保存された後、リスク判定部14が、走行位置に関するリスクスコアの再算出（図13に示すフロー図の手順ではステップS415及びS416に相当）を実行し（ステップS400A）、リスクレベル管理リストに書き込む。リスク判定部14は、再算出したリスクスコアをリスクレベル管理リストからあらためて読み取り、以降は、図17に示した処理手順と共通である。

[0145] また、走行状態に変化があった場合も、走行位置に変化があった場合と同様の処理手順が実行されてもよい（図18B参照）。図18Bに示す処理手順の図18Aに示す処理手順との差異は、セキュリティリスク対策サーバ10において取得されるのが走行状態変化通知である点（ステップS300B）、及びリスク判定部14が走行状態に関するリスクスコアを再算出するステップが、図13に示すフロー図の手順ではステップS423及びS424に相当する点である。

[0146] なお、車両の通信関連機能については、走行状態が停止に変化した場合には、速やかに機能制限が解除されることで、第一車両20からSOC等への通報が迅速に行える、又はSOC等からセキュリティパッチを取得できる等の利点がある。また、第一車両20がサイバー攻撃の影響で停止状態から危険な動作に移行する可能性が低いことから、通信関連機能の機能制限の解除による危険性は小さい。このような考えに基づく、走行状態の停止への変化時の通信関連機能の機能制限の解除の処理手順例を図18Cに示す。

[0147] この例では、セキュリティリスク対策サーバ10において走行状態変化通知が取得され（ステップS300B）、蓄積部13に保存された後、リスク判定部14は、図18Aに示すようなリスクスコアの再算出を実行するのではなく、走行状態が停止に変化したか否かを判定する（ステップS700C）。走行状態が停止に変化した場合（ステップS700CでYes）、リスク判定部14は、機能無効化指示が未発行か否かを判定する（ステップS701）。機能無効化指示が未発行である場合（ステップS701でYes）、リスク判定部14は、通信関連機能に対する機能制限解除指示を機能制限解除

指示生成部 18 に生成させる。機能制限解除指示生成部 18 は、通信関連機能に対する機能制限解除指示を生成し（ステップ S 710C）、生成された通信関連機能に対する機能制限解除指示は、指示出力部 17 から出力され（ステップ S 720C）、第一車両 20 に送信される。

[0148] 走行状態が停止以外に変化した場合（ステップ S 700C で N o）又は機能無効化指示が発行済みである場合（ステップ S 701 で N o）、通信関連機能に対する機能制限には変更が加えられることなくこの処理は終了する。

[0149] セキュリティリスク対策システム 1 では、ここまで説明した第二段階が繰り返し実行される（図 5 中、リスク制御ループ）。これにより、セキュリティリスク対策の実行対象である第一車両 20 に、その車両状態に応じて変化する車両機能のリスクレベルに適したセキュリティリスク対策を持続的に適用することができる。

[0150] （実施の形態 2）

実施の形態 2 に係る情報処理装置を含むセキュリティリスク対策システムでは、目下のセキュリティリスク対策の実行対象の車両である第一車両が持つ車両機能のリスクレベルの判定に、多数の車両を対象に集められたサイバー攻撃のインシデント情報を用いる点は実施の形態 1 と共通である。

[0151] 一方、実施の形態 2 では、このリスクレベルの判定に、インシデント情報とあわせて、第一車両以外の車両（以下、第二車両ともいう）の車両情報が用いられる点が実施の形態 1 と異なる。以下、この実施の形態 1 との差異点を中心に本実施の形態を説明する。なお、実施の形態 1 との共通点については、説明を簡略化又は省略する。

[0152] ここでの第二車両とは、例えば第一車両と通信し得る車両である。より具体的には、例えば第一車両の近隣にあって、第一車両と直接の通信が可能な車両である。また例えば、それぞれが接続する中継局、路側機、又は他の車両等に仲介されて第一車両との通信が確立し得る車両である。通信相手である第二車両のサイバー攻撃に対するリスクレベルが高い場合、第二車両との情報の授受をする第一車両のリスクレベルも上がる。別の例として、第二車

両は、第一車両と同じECUであって所定の大きさ以上のリスクポイントのECU（以下、リスクECUともいう）を搭載している車両、同一車種の車両、又は共通の車両機能を持つ車両であってもよい。このような第二車両のサイバー攻撃に対するリスクレベルが高い場合、第一車両も共通の脆弱性を有する可能性が高いため、同様にサイバー攻撃に対するリスクレベルが高い。また別の例として、第二車両は、第一車両との通信の有無にかかわらず第一車両の近くを走行する車両であってもよい。第二車両が地域的なサイバー攻撃を受けている場合、近くを走行する第一車両も同様にサイバー攻撃にさらされる可能性があり、リスクレベルが高い。したがって、このように第一車両以外のリスクレベルに応じて第一車両の車両機能を制限することも、第一車両のセキュリティリスク対策として有効である。

[0153] [1. 構成]

図19は、本実施の形態に係る情報処理装置を含むセキュリティリスク対策システム1Aの構成例の概要を示す図である。

[0154] 図1に示される構成例では、セキュリティリスク対策サーバ10Aと、第一車両である車両20A、インシデント情報収集サーバ30とがインターネット等の通信ネットワークを介して接続されて相互に情報の授受が可能である。また、第一車両20Aとは別の第二車両20Bも、セキュリティリスク対策サーバ10A及びインシデント情報収集サーバ30とインターネット等の通信ネットワークを介して接続されて相互に情報の授受が可能である。

[0155] インシデント情報収集サーバ30については、実施の形態1と共通の構成でよいいため詳細な説明は省略する。また、インシデント情報収集サーバ30からセキュリティリスク対策サーバ10Aに提供されるインシデント情報の構成も実施の形態1と共通でよいいため詳細な説明は省略する。

[0156] また、第一車両20A及び第二車両20Bについても、各々が備える車載ネットワーク200A及び200Bの構成は、図3を用いて説明した、実施の形態1における第一車両20の車載ネットワーク200の構成と共通でよく、詳細な説明は省略する。

[0157] セキュリティリスク対策サーバ10Aは、実施の形態1のセキュリティリスク対策サーバ10と基本的な構成は共通である。セキュリティリスク対策サーバ10Aもまた、プロセッサ及びメモリを含む1台又は複数台の情報処理装置で構成され、本実施の形態における本発明の情報処理装置の例である。セキュリティリスク対策サーバ10Aのセキュリティリスク対策サーバ10との差異点は、上述のとおり、インシデント情報収集サーバ30から取得するインシデント情報と、第二車両20Bから取得した第二車両の状態に関する情報とを用いて、第一車両20Aが持つ車両機能のサイバー攻撃に関するリスクレベルを判定するという第二段階の処理にある。なお、この処理は、実施の形態1における、セキュリティリスク対策の実行対象の車両20から取得された第一車両情報を用いた処理と合わせての実行が可能であり、処理を実行する各構成要素は、セキュリティリスク対策サーバ10の構成要素と共通でよいので、詳細な説明は省略する。

[0158] [2. 動作]

次に、セキュリティリスク対策システム1Aで実行されるセキュリティリスク対策の処理の動作について、実施の形態1との差異点を中心に説明する。

[0159] 図20は、セキュリティリスク対策サーバ10で実行されるこの処理の手順例を示すフロー図である。

[0160] インシデント情報収集サーバ30からのインシデント情報の取得（ステップS21）から蓄積、及び取得されたインシデント情報に基づく、リスクポイント管理部15によるリスクポイントテーブルの更新（ステップS22）の処理手順は図5に示される実施の形態1と共通でよく、説明を省略する。以下の手順については、実施の形態1との比較のため、図9のシーケンス図に対応する図21のシーケンス図も参照しながら説明する。図21のシーケンス図を参照すると、セキュリティリスク対策の実行対象である第一車両20A以外の車両である第二車両20Bが第一車両20Aのセキュリティリスク対策の処理に関与している。

- [0161] 次にセキュリティリスク対策システム 1 A では、第二車両 20 B から送信された第二車両 20 B の状態に関する情報（以下、第二車両情報ともいう）が、車両情報取得部 12 によっていったん蓄積部 13 に保存される（図 20 のステップ S 23、図 21 のステップ S 22030、S 230）。
- [0162] 次にセキュリティリスク対策システム 1 A では、リスク判定部 14 が、リスクポイントテーブル及び第二車両情報を用いて第二車両のリスクレベルを判定し、リスクレベル管理リストを作成（更新の場合を含む）する（図 20 のステップ S 24、図 21 のステップ S 240）。第二車両のリスクレベルの判定及びリスクレベル管理リストの作成の処理手順については、実施の形態 1 について図 10 から図 14 F を用いて説明した第一車両 20 A の場合の処理手順と共通でよいので、ここでは説明を省略する。
- [0163] 第二車両 20 B のリスクスコアをいったんリスクレベル管理リストに書き込んだリスク判定部 14 は、次にこのリスクスコアを読み取り（図 20 のステップ S 25、図 21 のステップ S 250）第一車両 20 A のリスク制御処理、つまり有効な車両機能の機能制限（無効化の場合を含む）の可否についての判定（図 20 のステップ S 26）に用いる。
- [0164] 図 22 は、セキュリティリスク対策サーバ 10 A において実行される、第二車両 20 B のリスクスコアを用いた第一車両 20 A のリスク制御処理の手順例を示すフロー図である。
- [0165] 本実施の形態における第一車両 20 A のリスク制御処理の基本的な流れは、図 15 を用いて説明した実施の形態 1 でのリスク制御処理と共通でよい。図中の第一閾値、第二閾値、機能無効化指示、機能制限指示、及びリスク対策指示については、実施の形態 1 と共通でよいので、説明を省略する。
- [0166] リスク判定部 14 は、リスクレベル管理リストから第二車両 20 B のリスクスコアを読み取ると（ステップ S 2500）、このリスクスコアが第二閾値以上であるか判定する（ステップ S 2600）。第二車両 20 B のリスクスコアが第二閾値未満である場合（ステップ S 2600 で No）、リスク判定部 14 はさらにこのリスクスコアが第一閾値以上であるか判定する（ステ

ップS 2 6 0 1)。ステップS 2 6 0 0及びステップS 2 6 0 1は、図2 0のフロー図のステップS 2 6及び図2 1のシーケンス図のステップS 2 6 0に相当する。

[0167] 第二車両2 0 Bのリスクスコアが第一閾値未満の場合（ステップS 2 6 0 1でN o）、第一車両2 0 Aの車両機能は制限も無効化もされないでリスク制御の処理が終了する。

[0168] 第二車両2 0 Bのリスクスコアが第二閾値以上の場合（ステップS 2 6 0 0でY e s）、リスク判定部1 4は、リスク対策指示生成部1 6に第一車両2 0 Aの車両機能に対する機能無効化指示を生成させる。リスク対策指示生成部1 6は、リスクレベル管理リスト（図1 2）でリスク制御対象の車両機能の「無効化」欄の内容に従って、機能無効化指示を生成する（ステップS 2 6 1 0）。生成された機能無効化指示は、指示出力部1 7から出力され（ステップS 2 6 2 0）、第一車両2 0 Aに送信される。

[0169] 第二車両2 0 Bのリスクスコアが第二閾値未満かつ第一閾値以上の場合（ステップS 2 6 0 1でY e s）、リスク判定部1 4は、リスク対策指示生成部1 6に機能制限指示を生成させる。リスク対策指示生成部1 6は、リスクレベル管理リストでリスク制御対象の車両機能の「制限」欄の内容に従って、機能制限指示を生成する（ステップS 2 6 1 1）。生成された機能制限指示は、指示出力部1 7から出力され（ステップS 2 6 2 0）、第一車両2 0 Aに送信される。ステップS 2 6 1 0及びステップS 2 6 1 1は、図2 1のシーケンス図のステップS 2 6 1に相当する。また、ステップS 2 6 2 0は、図2 1のシーケンス図のステップS 2 6 2に相当する。

[0170] このように、図1 5にフロー図に手順例が示される処理によって、第二車両2 0 Bのリスクスコア、つまりリスクレベルに応じて第一車両2 0 Aの車両機能の制限が実行される。これにより、例えば第二車両2 0 Bが第一車両2 0 Aと通信が可能であり、かつサイバー攻撃に対する脆弱性があるリスクレベルが高い場合にも、第一車両2 0 Aの車両機能に、第二車両2 0 Bで発生するインシデントの影響が通信を介して及ぶことを防ぐことができる。

[0171] なお、第一車両 20A にとっての第二車両 20B の選定は、図 21 のシーケンス図におけるステップ S26 の手前までに、例えばリスク判定部 14 又はリスク対策指示生成部 16 によって随時行われ得る。例えば、ステップ S24 まではセキュリティリスク対策システム 1A による監視対象の全ての車両に対して実行される。そしてリスク判定部 14 は、監視対象の一台である第一車両 20A の車両情報に含まれる走行位置の情報と、第一車両 20A 以外の監視対象の車両の車両情報に含まれる走行位置の情報とを用いて第一車両 20A と所定の近さ（所定の距離以下）にある車両を第二車両 20B として選択してステップ S20B 以降を実行してもよい。または、第一車両 20A と所定の近さ（所定の距離以下）にあつて第一車両 20A と通信し得る機能を備える車両を第二車両 20B として選択してもよい。または、車両情報の機器リスト（図 10）を参照して、第一車両 20A と共通の機器を備える車両を第二車両 20B として選択してもよい。または、セキュリティリスク対策システム 1A による監視対象の全ての車両に対して、図 5 に示す実施の形態 1 のセキュリティリスク対策の処理を実行した上で、何らかの機能制限が適用された車両がまず第二車両 20B として選定され、上述のように走行位置、備える機能又は機器等に基づいて第一車両 20A が選定されてもよい。

[0172] また、第二車両 20B のリスクスコアと比較された第一閾値及び第二閾値は、実施の形態 1 では第一車両 20 で用いられた第一閾値及び第二閾値と共通であってもよいし、これらと異なるリスクレベルを示す基準であってもよい。第二車両 20B で用いられる第一閾値が示す基準（第三基準）と第二閾値が示す基準（第四基準）との間で、第四基準が第三基準より高いものであればよい。

[0173] また、第二車両 20B のリスクスコアが第二閾値未満かつ第一閾値以上の場合に第一車両 20A に適用される制限は、第一車両 20A が自車のリスクスコアが第二閾値未満かつ第一閾値以上の場合に適用される制限と異なるものであってもよい。例えば、これらの制限は、リスクレベル管理リストに 2

列の「制限」欄があり、各欄に分けて規定されていてもよい。

[0174] また、第一車両 20A で制限又は無効化される車両機能は、第二車両 20B でリスクスコアが第一閾値又は第二閾値を超える車両機能に対応する第一車両 20A の車両機能である。ここでの第二車両 20B の車両機能に対応する第一車両 20A の車両機能とは、例えばリスクスコアが各閾値を超える第二車両 20B の車両機能と同じ車両機能である。またさらに、第一車両 20A において制限又は無効化される車両機能を提供する ECU が提供する他の車両機能も、この対応する車両機能に含まれてもよい。別の例として、対応する車両機能は、第一車両 20A で提供する機能は異なっているが、第二車両 20B でリスクスコアが第一閾値又は第二閾値を超える車両機能を提供している ECU と、製造元が同じ ECU もしくは同型の ECU が提供する車両機能であってもよい。このような対応する車両機能は、機器リストを参照して把握される。

[0175] また、本実施の形態における第二車両 20B のリスクレベルに応じた第一車両 20A のリスク制御としても、実施の形態 1 と同様に機能制限の解除が実行されてもよい。図 23 は第二車両 20B のリスクスコアの再算出の後に実行される車両機能の制限の解除処理の手順例を示すフロー図である。

[0176] この手順例では、まず、リスク判定部 14 によって、第二車両 20B の走行状態について変化の有無が判定される（ステップ S2300）。第二車両 20B の走行状態に変化があった場合（ステップ S2300 で Yes）、リスク判定部 14 は、第二車両 20B の走行状態に関するリスクスコアの再算出（図 13 に示すフロー図の手順ではステップ S423 及び S424 に相当）を実行し（ステップ S2400）、リスクレベル管理リストに書き込む。次にリスク判定部 14 は、再算出した第二車両 20B のリスクスコアをリスクレベル管理リストからあらためて読み取り、以降は、このリスクスコアを用いて図 17 に示した処理手順と共通の手順を実行する。ステップ S2700、S2701、S2710 及び S2720 は、図 17 に示す実施の形態 1 におけるステップ S700、S701、S710 及び S720 に相当する。

ステップS 2 7 0 1で機能無効化指示の発行についての判定が行われるのは、実施の形態1において車両機能が無効化されている場合には機能制限は解除されないのと同じ理由による。

[0177] また、本実施の形態においては、第二車両20Bとの通信の確立の可否に応じて、第一車両20Aの車両機能が第二車両20Bで発生するインシデントの影響を受ける可能性も変わる。つまり、通信の確立が不可能であれば、第二車両20Bで発生するインシデントの影響が通信を介して第一車両20Aの車両機能に及ぶ可能性がない。したがって、例えば第一車両20Aとリスクレベルの高い第二車両20Bとの間の距離が、車車間の通信の確立が可能な距離であるか否かに応じて第一車両20Aの車両機能を制限するか否かが決定されてもよい。図24Aは、この態様での第一車両20Aの車両機能に対する機能制限処理の手順例を示すフロー図である。また、図24Bは、図24Aに示す手順例で第一車両20Aの車両機能に対する機能制限指示が出力された後の、第一車両20Aの車両機能に対する機能制限解除処理の手順例を示すフロー図である。

[0178] 図24Aに示す手順例では、リスク判定部14は、リスクレベル管理リストから読み取った第二車両20Bのリスクスコアが第一閾値以上であるか否かを判定する（ステップS 2 6 0 1 A）。第二車両20Bのリスクスコアが第一閾値以上である場合（ステップS 2 6 0 1 AでY e s）、リスク判定部14は、さらに第一車両20Aの第二車両20Bとの距離が、所定の基準距離d未満であるか否かを判定する。基準距離dは、例えば第一車両20Aの第二車両20Bとの間で確立され得る通信が準拠する規格での、通信可能距離の上限に基づいて定められる。第一車両20Aの第二車両20Bとの距離が基準距離d未満である場合（ステップS 2 6 0 2 AでY e s）、リスク判定部14は、この例では、第一車両20Aの車両機能のうち、走行関連機能に対する機能制限指示をリスク対策指示生成部16に生成させている。そしてこの走行関連機能に対する機能制限指示が、指示出力部17から出力され（ステップS 2 6 0 3 A）、第一車両20Aに送信される。

- [0179] 第二車両 20B のリスクスコアが第一閾値未満の場合（ステップ S 2601A で No）又は第一車両 20A の第二車両 20B との距離が基準距離 d 以上である場合、第一車両 20A の車両機能に対する機能制限指示は生成されない。これらのいずれの場合も第二車両 20B で発生するインシデントの影響が通信を介して第一車両 20A の車両機能に及ぶ可能性がないので、第一車両 20A で第二車両 20B のリスクレベルに応じたセキュリティ対策の実行の必要はない。
- [0180] なお、上記の手順例で制限の対象が走行関連機能であるのは、少なくとも第二車両 20B が比較的近距離に存在しながら走行している状況でインシデントの影響を受けるともっとも深刻な事態を招き得るのが走行関連機能であるためである。
- [0181] ステップ S 2702A が実行された場合に実行される図 24B に示す手順例では、リスク判定部 14 は、第一車両 20A の第二車両 20B との距離が、所定の基準距離 d 以上であるか否かを判定する（ステップ S 2701A）。第一車両 20A の第二車両 20B との距離が、所定の基準距離 d 以上である場合（ステップ S 2701A で Yes）、第二車両 20B でインシデントが発生したとしてもその影響が通信を介して第一車両 20A の車両機能に及ぶ可能性がないので、第一車両 20A の車両機能に対する走行関連機能に対する機能制限解除指示が生成されて出力される（ステップ S 2702B）。第一車両 20A の第二車両 20B との距離が、所定の基準距離 d 未満である間（ステップ S 2701A で No）、この機能制限解除指示の出力には至らない。つまり、第一車両 20A での走行関連機能に対する機能制限が維持される。
- [0182] また、インシデントが発生した車両を特定可能な情報がインシデント情報に含まれる場合は、第二車両 20B にインシデント発生の履歴がある場合に第二車両 20B のリスクスコアを上昇させてもよい。サイバー攻撃のインシデントが発生した実績のある車両には、攻撃を許した何らかの脆弱性、又はその攻撃の影響が残る可能性があり、そのような車両と通信可能な車両では

警戒して予防的対策がなされるのが妥当である。そのような第二車両 20B のリスクスコアを第一閾値以上にしておくことで、第一車両 20A では、車両機能に対する機能制限がなされる。これにより、第二車両 20B でインシデントが発生した場合にも、その影響が通信を介して第一車両 20A の車両機能に及ぶ可能性を抑えることができる。図 25 は、このような第二車両のインシデント履歴に応じたセキュリティ対策の処理の手順例を示すフロー図である。

[0183] 図 25 に示す手順例では、リスク判定部 14 は、蓄積部 2113 に保存されたインシデント情報で第二車両 20B に関するインシデント情報のレコードを検索する（ステップ S2900）。第二車両 20B に関するインシデント情報のレコードが見つからなかった場合（ステップ S2901 で No）、第二車両 20B のリスクスコアは変動しない。第二車両 20B に関するインシデント情報のレコードが見つかった場合（ステップ S2901 で Yes）、第二車両 20B のリスクスコアが第一閾値以上に設定される（ステップ S2902）。この場合に第一閾値以上に設定されるリスクスコアは、例えば見つかったインシデント情報のレコードの中身に応じた車両機能についてのリスクスコアであってもよい。具体例としては、例えば第二車両 20B で発生していたのが自動運転機能に影響を受けたインシデントであれば、自動運転機能のリスクスコアが第一閾値以上に設定されてもよい。また、このインシデントを引き起こしたサイバー攻撃では同一の機能系統も影響を受ける可能性が他の機能系統よりも高いため、自動運転機能と同一の機能系統、つまり走行系に属する運転支援及び走行制御の機能（図 12 のリスクレベル管理リスト参照）のリスクスコアも各々第一閾値以上に設定されてもよい。

[0184] （変形例等）

以上、一つまたは複数の態様に係る、セキュリティリスク対策システムに含まれるセキュリティリスク対策サーバを構成する情報処理装置について、実施の形態に基づいて説明したが、本発明はこれらの実施の形態に限定されるものではない。本発明の趣旨を逸脱しない限り、当業者が思いつく各種変

形を本実施の形態に施したものや、異なる実施の形態における構成要素を組み合わせて構築される形態も、一つまたは複数の態様の範囲内に含まれてもよい。以下に、そのような変形の例を挙げる。

[0185] (1) 上記の実施の形態の説明のために例示した情報処理装置はサーバであるが、情報処理装置の構成要素の少なくとも一部は、1個以上のECU等の車載の情報処理装置であってもよい。例えば図3に示すECUのうち、ECU210Aがセキュリティリスク対策サーバ10又は10Aと同じ機能的構成を備えてもよい。図26は、このようなECU210Aの機能的構成例を示すブロック図である。なお、図26の車両情報取得部2112は、第一車両20の車両情報は外部の通信ネットワーク経由で受信するのではなく、車載ネットワーク上の通信で取得する。また、指示出力部2117から出力される機能制限指示及び機能制限解除指示は直接車載ネットワークに送出され、外部の通信ネットワークは経由しない。

[0186] また、車載の情報処理装置がセキュリティリスク対策サーバ10又は10Aの一部の機能を備える例としては、例えばリスクポイント管理部による、インシデント情報に基づくリスクポイントの更新、つまり図5のフロー図におけるステップS2まではセキュリティリスク対策サーバで実行され、リスクポイントテーブルが通信ネットワークを介して車載の情報処理装置に提供されてもよい。この場合、車載の情報処理装置は、提供された最新のリスクポイントテーブルと車載の他の情報処理装置から取得した車両情報を用いてステップS4以降を実行する。

[0187] また例えば、図5のフロー図におけるステップS4のリスクレベル管理リストの作成(更新)までがセキュリティリスク対策サーバで実行され、リスクレベル管理リストが通信ネットワークを介して車載の情報処理装置に提供されてもよい。この場合、車載の情報処理装置は、提供された最新のリスクレベル管理リストを用いてステップS5以降を実行する。また、リスクポイントテーブルもセキュリティリスク対策サーバから車載の情報処理装置に提供され、走行位置又は走行状態に関するリスクレベルの比較的小規模な更新

、及びその後の機能制限判定等が車載の情報処理装置で実行されてもよい。この場合、例えば第一車両の車両情報が各日の深夜等に日次処理でセキュリティリスク対策サーバに提供されてもよい。セキュリティリスク対策サーバでは、夜間の日次処理としてインシデント情報に基づくリスクポイントテーブルの更新及び第一車両のリスクレベル管理リストの全面的な更新が実行される、そして早朝までにセキュリティリスク対策サーバから第一車両へ最新のリスクポイントテーブル及びリスクレベル管理リストが送信される。第一車両の車載の情報処理装置では、早朝から深夜までリスクレベルの小規模な更新及び機能制限判定等が実行される。また、日次処理のような定期的な処理ではなく、第一車両のドライバーの要求に応じて、第一車両の車両情報のセキュリティリスク対策サーバへの提供又はセキュリティリスク対策サーバから第一車両への最新のリスクポイントテーブル及びリスクレベル管理リストの提供が実施されてもよい。

[0188] (2) 機能制限の態様は、図12のリスクレベル管理リスト及び図15等を参照しての機能制限に関する上記の説明に限定されない。例えばより多くの基準を用いて判断されるより多段階な制限であってもよい。その場合、リスク判定部14又は2114が行う機能制限の解除の判定には、機能制限の緩和も概念的に含まれる。

[0189] (3) インシデント情報におけるインシデントの発生場所及び車両情報における車両の走行位置の表現は、上記の市区町村のような地名を用いる例に限定されず、統計的にインシデントの発生の多い又は少ない場所と第一車両の走行位置との位置関係が分かる表現であればよい。走行位置の表現には、例えばランドマーク若しくは通信基地局等の施設の名称、道路の名称及びその区間、経緯度、又はセルを並べたグリッド地図が用いられてもよい。そして、位置関係は、例えばこれらのとの距離及び方角、包含又は重複で表現され得る。経緯度の情報は、例えば、各車両から提供される経緯度の情報として取得される。その他の表現は、例えばインシデント情報収集サーバ30又はセキュリティリスク対策サーバ10において、各車両から提供された経緯

度の情報から変換して実現されてもよい。

[0190] そして、リスク判定部 14 又は 2114 は、第一車両の走行位置に、リスクレベルが変わり得る所定の変化があった場合に車両機能のリスクレベルの再判定を実行する。この所定の変化の例としては、最寄りの施設の切り換わり、道路又はその区間の切り換わり、経緯度の所定量の変化、グリッド地図において走行位置を含むセルの切り換わりが挙げられる。

[0191] (4) 上記実施の形態で示した各種処理の手順（例えば図 5、図 8、図 13～図 18C、図 20、図 22～図 25 等に示した手順等）の実行順序は、必ずしも、上述した通りの順序に制限されるものではない。本発明の要旨を逸脱しない範囲で、実行順序を入れ替えたり、複数の手順を並列に行ったり、その手順の一部を省略したりすることができる。

[0192] (5) 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又は全部は、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よい。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よいし、一部又は全部を含むように 1 チップ化されてもよい。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、専用回路又は汎用プロセッサで実現してもよい。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プログラマブルプロセッサを利用してもよい。さらには、半導体技術の進歩又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よい。

[0193] (6) 上記各装置を構成する構成要素の一部又は全部は、各装置に脱着可能なＩＣカード又は単体のモジュールから構成されているとしてもよい。ＩＣカード又はモジュールは、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カード又はモジュールは、上記の超多機能ＬＳＩを含むとしてもよい。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カード又はモジュールは、その機能を達成する。このＩＣカード又はこのモジュールは、耐タンパ性を有するとしてもよい。

[0194] (7) 本発明の一態様としては、例えば図５、図８、図１３～図１８Ｃ、図２０、図２２～図２５等にした手順に示す処理手順の全部又は一部を含む情報処理方法であるとしてもよい。また、これら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）であるとしてもよい。

[0195] (8) 本発明の一態様としては、上記のコンピュータプログラム又はこのコンピュータプログラムを表す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（Blu-ray（登録商標）Disc）、半導体メモリ等に記録したものとしてもよい。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よい。また、本発明の一態様としては、上記のコンピュータプログラム又はデジタル信号を、電気通信回線、無線又は有線通信回線、インターネットに代表されるネットワーク、データ放送等を経由して伝送するものとしてもよい。また、本発明の一態様としては、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よい。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、又は、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。

[0196] (9) 上記実施の形態及び上記変形例で示した各構成要素及び機能を任意に組み合わせることによって実現される形態も本発明の範囲に含まれる。

産業上の利用可能性

[0197] 本発明は、車両で利用される情報を処理する情報処理装置、情報処理方法、及びプログラムに利用可能である。

符号の説明

[0198] 1、1 A セキュリティリスク対策システム
1 0、1 0 A セキュリティリスク対策サーバ
1 1、2 1 1 1 インシデント情報取得部
1 2、2 1 1 2 車両情報取得部
1 3、2 1 1 3 蓄積部
1 4、2 1 1 4 リスク判定部
1 5、2 1 1 5 リスクポイント管理部
1 6、2 1 1 6 リスク対策指示生成部
1 7、2 1 1 7 指示出力部
1 8、2 1 1 8 機能制限解除指示生成部
2 0 車両（第一車両）
2 0 A 車両（第一車両）
2 0 B 車両（第二車両）
3 0 インシデント情報収集サーバ
2 0 0、2 0 0 A、2 0 0 B 車載ネットワーク
2 1 0 A、2 1 0 B、2 1 0 C、2 1 1 A、2 1 1 B、2 1 1 C、2 1 2
A、2 1 2 B、2 1 2 C ECU
2 2 0 ゲートウェイ
2 3 0 I V I システム
2 4 0 外部通信装置

請求の範囲

- [請求項1] 第一車両及び第二車両の情報を処理する情報処理装置であって、
車両で発生したサイバー攻撃のインシデントに関するインシデント情報を取得するインシデント情報取得部と、
前記第二車両との通信を介して前記第二車両の状態に関する第二車両情報を取得する車両情報取得部と、
前記インシデント情報及び前記第二車両情報を蓄積する蓄積部と、
前記インシデント情報と前記第二車両情報との一致度に基づいて、前記第二車両が持つ車両機能のリスクレベルを判定するリスク判定部と、
前記リスクレベルが第一基準より高い場合、前記第二車両の車両機能に対応する前記第一車両の車両機能に対する機能制限指示を生成するリスク対策指示生成部と、
前記機能制限指示を出力する指示出力部とを備える
情報処理装置。
- [請求項2] 前記リスク対策指示生成部は、前記リスクレベルが前記第一基準より上の第二基準よりも高い場合、前記機能制限指示として前記第二車両の車両機能に対応する前記第一車両の車両機能に対する機能無効化指示を生成する
請求項 1 に記載の情報処理装置。
- [請求項3] 前記第二車両の車両機能のリスクレベルが前記第一基準より低い場合、前記第二車両の車両機能に対応する前記第一車両の車両機能に対する機能制限解除指示を生成する機能制限解除指示生成部を備え、
前記指示出力部は、前記機能制限解除指示を出力する
請求項 1 又は 2 に記載の情報処理装置。
- [請求項4] 前記第二車両情報が示す前記第二車両の走行状態が変化した場合、前記リスク判定部は、前記第二車両の車両機能のリスクレベルを再判定する

請求項 3 に記載の情報処理装置。

- [請求項5] 前記第二車両の走行状態が走行中状態から停止状態に変化した場合、前記機能制限解除指示生成部は、前記第一車両の車両機能のうち通信関連機能に対する機能制限を解除する前記機能制限解除指示を生成する

請求項 4 に記載の情報処理装置。

- [請求項6] 前記蓄積部に蓄積されている前記インシデント情報に前記第二車両で発生したインシデント情報が含まれている場合、前記第二車両の車両機能のリスクレベルを前記第一基準より高くする

請求項 3 から 5 のいずれか一項に記載の情報処理装置。

- [請求項7] 前記第二車両の車両機能のリスクレベルが第三基準より高く、かつ前記第一車両の走行位置と前記第二車両の走行位置との距離が所定距離以下の場合、前記リスク対策指示生成部は、前記第一車両の車両機能のうち走行系機能に対する機能制限指示を生成する

請求項 3 から 6 のいずれか一項に記載の情報処理装置。

- [請求項8] 前記第一車両の走行位置と前記第二車両の走行位置との距離が所定距離より遠い場合、前記機能制限解除指示生成部は、前記第一車両の前記走行系機能に対する前記機能制限解除指示を生成する

請求項 7 に記載の情報処理装置。

- [請求項9] 第一車両及び第二車両の情報を処理する情報処理装置が
車両で発生したサイバー攻撃のインシデントに関するインシデント情報を取得し、

前記第二車両との通信を介して前記第二車両の状態に関する第二車両情報を取得し、

前記インシデント情報と前記第二車両情報との一致度に基づいて、前記第二車両が持つ車両機能のリスクレベルを判定し、

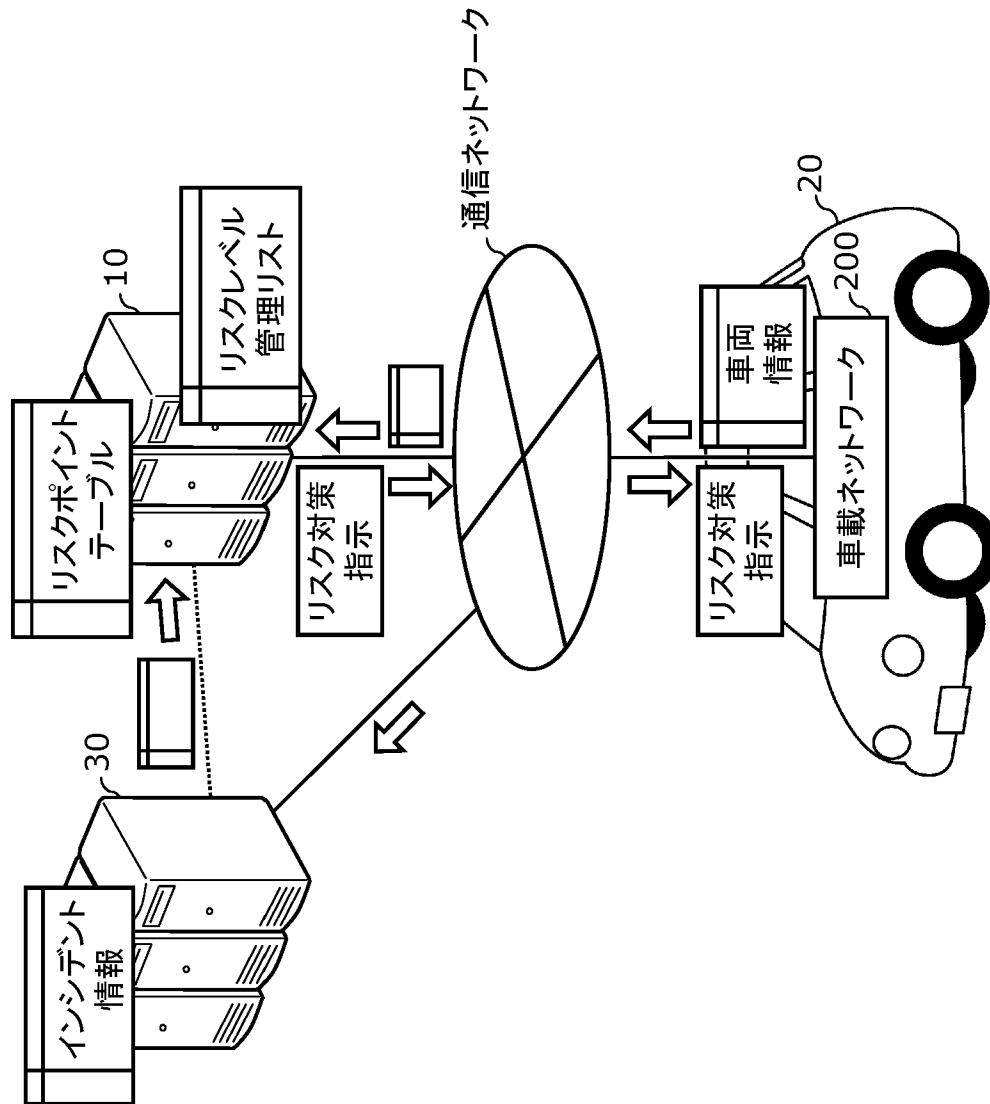
前記リスクレベルが第一基準より高い場合、前記第二車両の車両機能に対応する前記第一車両の車両機能に対する機能制限指示を生成し

、前記機能制限指示を出力する
情報処理方法。

[請求項10] プロセッサ及びメモリを備え、第一車両及び第二車両の情報を処理する情報処理装置において、前記メモリを用いて前記プロセッサによって実行されることで、前記プロセッサに、
 車両で発生したサイバー攻撃のインシデントに関するインシデント情報を取得させ、
 前記第二車両との通信を介して前記第二車両の状態に関する第二車両情報を取得させ、
 前記インシデント情報と前記第二車両情報との一致度に基づいて、前記第二車両が持つ車両機能のリスクレベルを判定させ、
 前記リスクレベルが第一基準より高い場合、前記第二車両の車両機能に対応する前記第一車両の車両機能に対する機能制限指示を生成させ、前記機能制限指示を出力させる
 プログラム。

[図1]

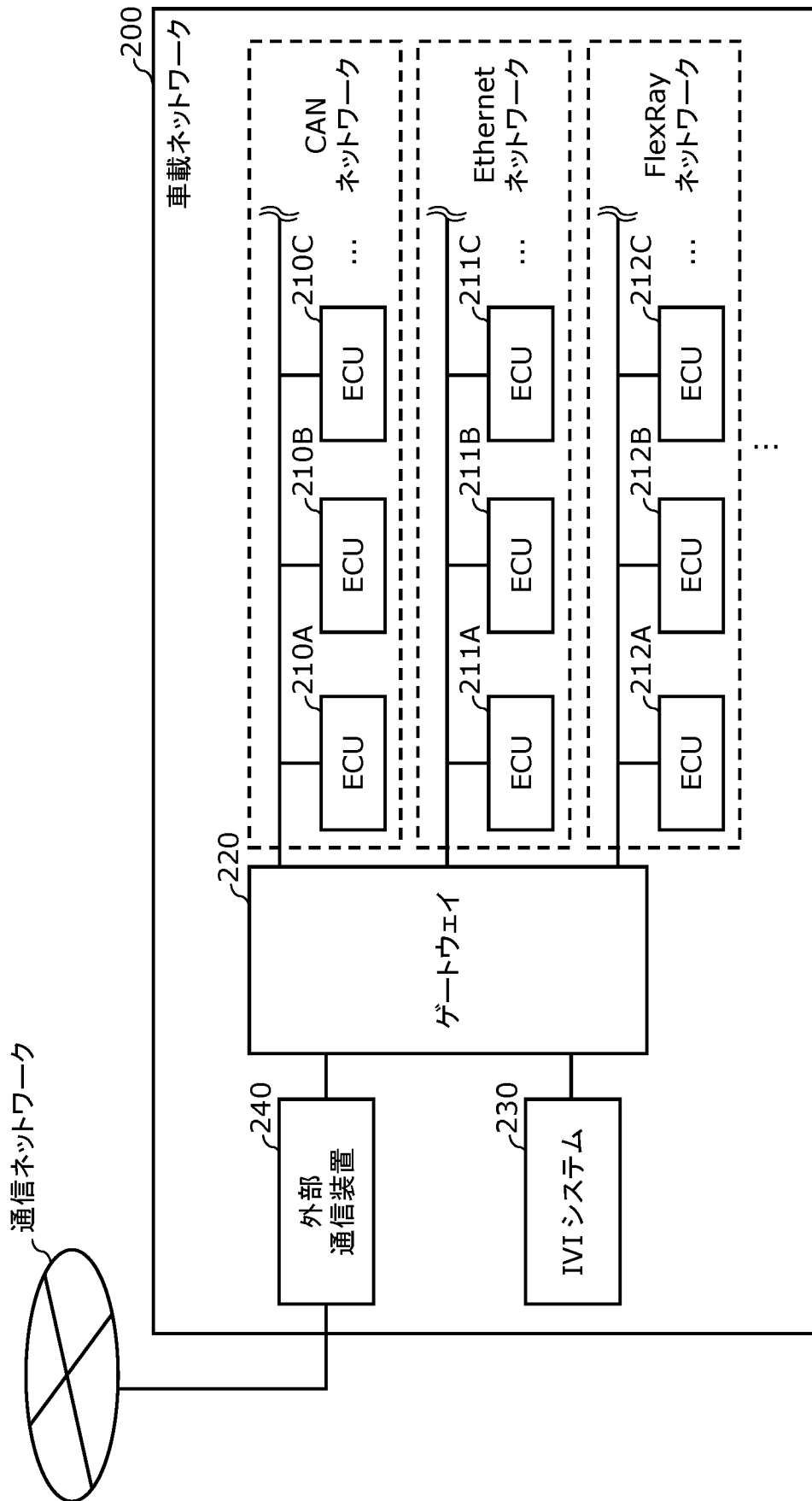
1



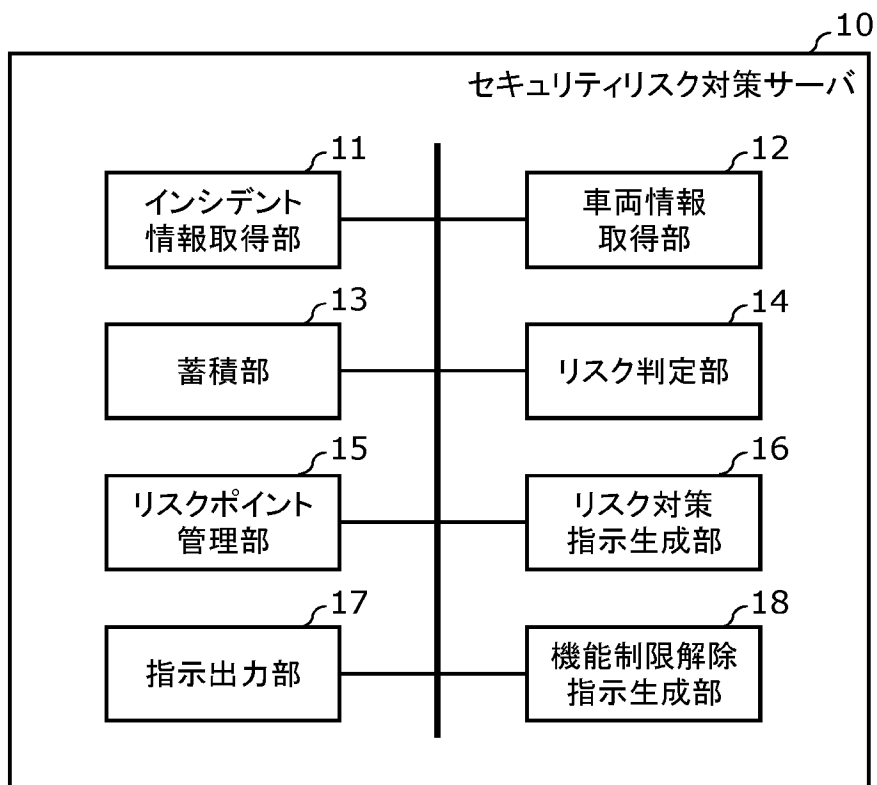
[図2]

インシデント ID	発生日時	発生地域	車種	リスク部品	リスク機能	侵入経路	脅威度
cs-A01	2020/12/04	東京都〇〇区	X	ECU-a	IPA	IVI, CAN	中
cs-B01	2020/11/04	大阪府□□市	X	ECU-b	Wi-Fi 接続	IVI	低
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
cs-C01	2019/04/03	沖縄県△△市	Y	IVI-a	自動運転	CAN, Ethernet	高
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
cs-D01	2018/03/03	北海道〇□市	Z	IVI-b	Bluetooth 接続	Bluetooth	低
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

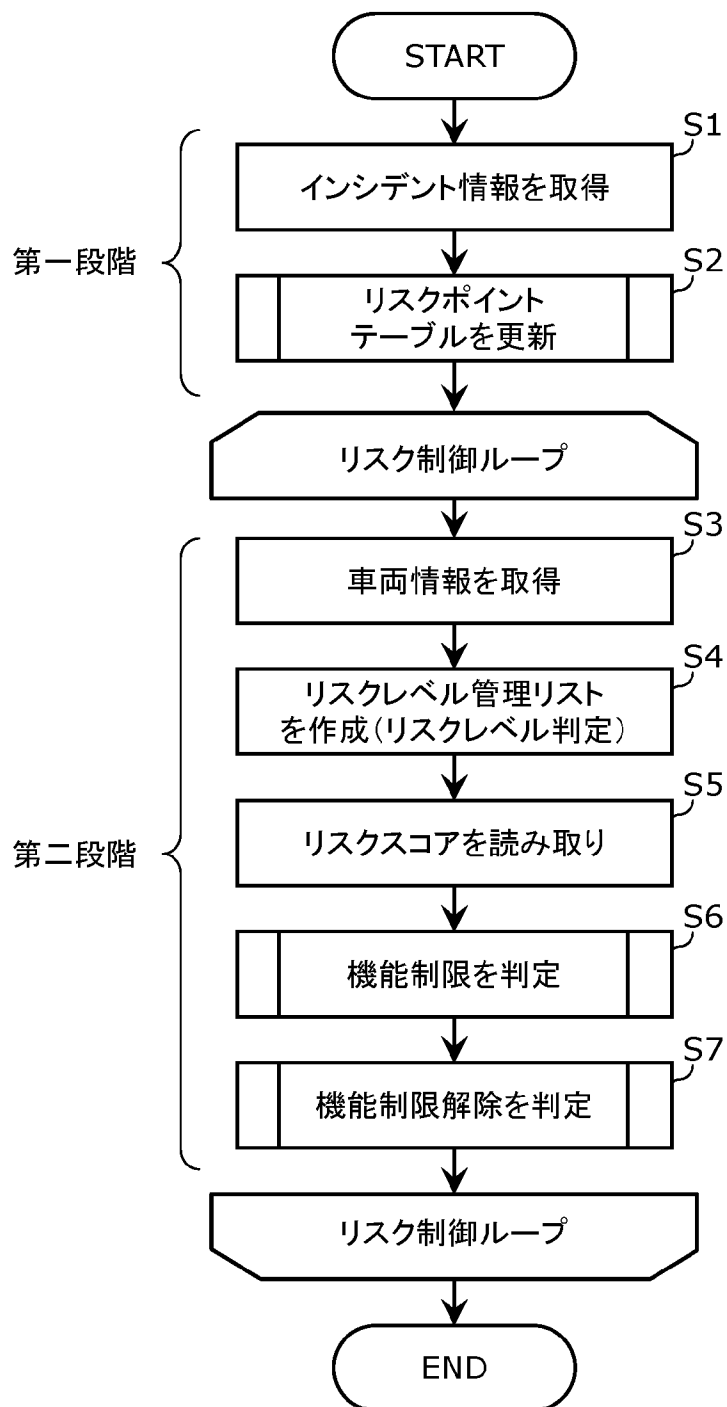
[図3]



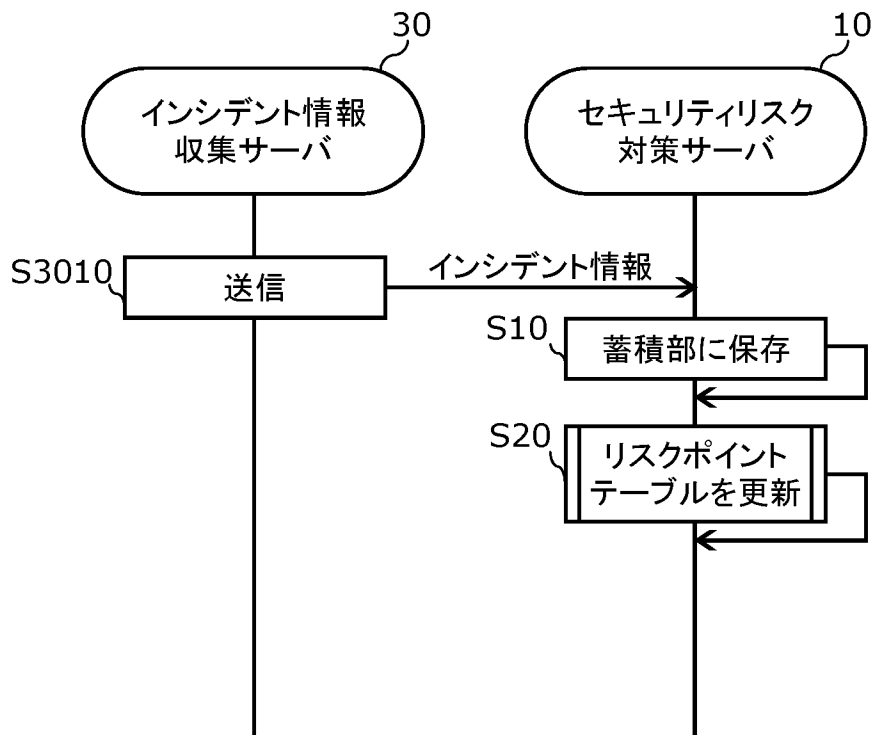
[図4]



[図5]



[図6]



[図7A]

型番	ソフトウェアバージョン	リスクポイント
ECU-a	1.0.1	5
	1.0.2	2
	1.0.3	1
ECU-b	1.0	1
⋮	⋮	⋮
IVI-a	1.0	1
	1.1	5
	1.2	4
	1.3	3
IVI-b	1.0.0	10
	2.0.0	2
⋮	⋮	⋮

[図7B]

製造者	リスクポイント
A 社	1
B 社	2
C 社	1
D 社	5
⋮	⋮

[図7C]

地域	リスクポイント
東京都〇〇区	2
大阪府□□市	4
神奈川県□〇市	8
愛知県△〇市	10
⋮	⋮

[図7D]

車種	リスクポイント
X	1
Y	2
Z	1
A	14
⋮	⋮

[図7E]

侵入経路	リスクポイント
CAN	8
Ethernet	5
FlexRay	1
MOST	2
TCP/IP	2
HTTP	2
⋮	⋮

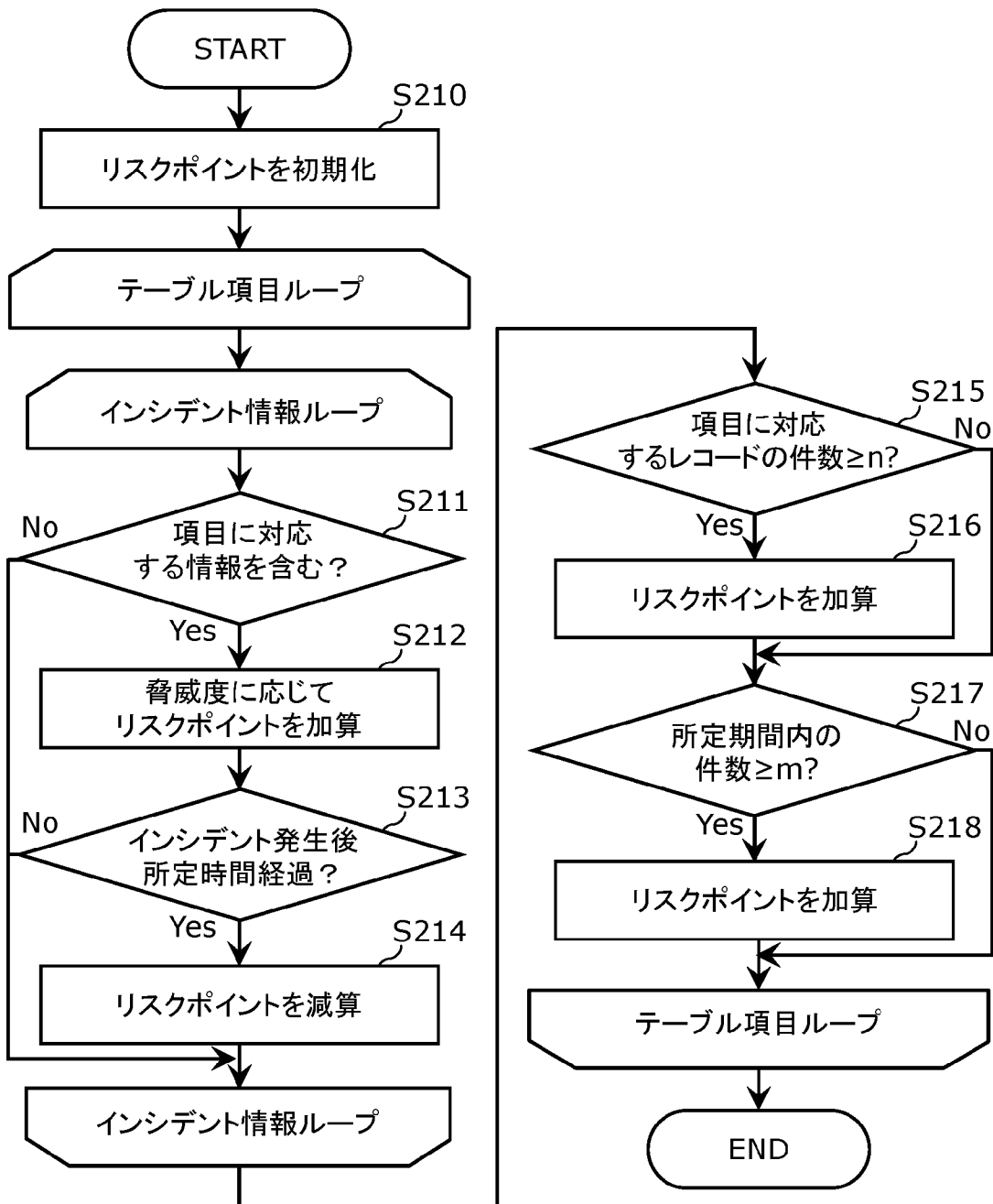
[図7F]

機能名	リスクポイント
自動運転	20
運転支援	5
Wi-Fi 接続	10
Bluetooth 接続	5
走行制御	40
LTE 通信	5
OTA 機能	20
⋮	⋮

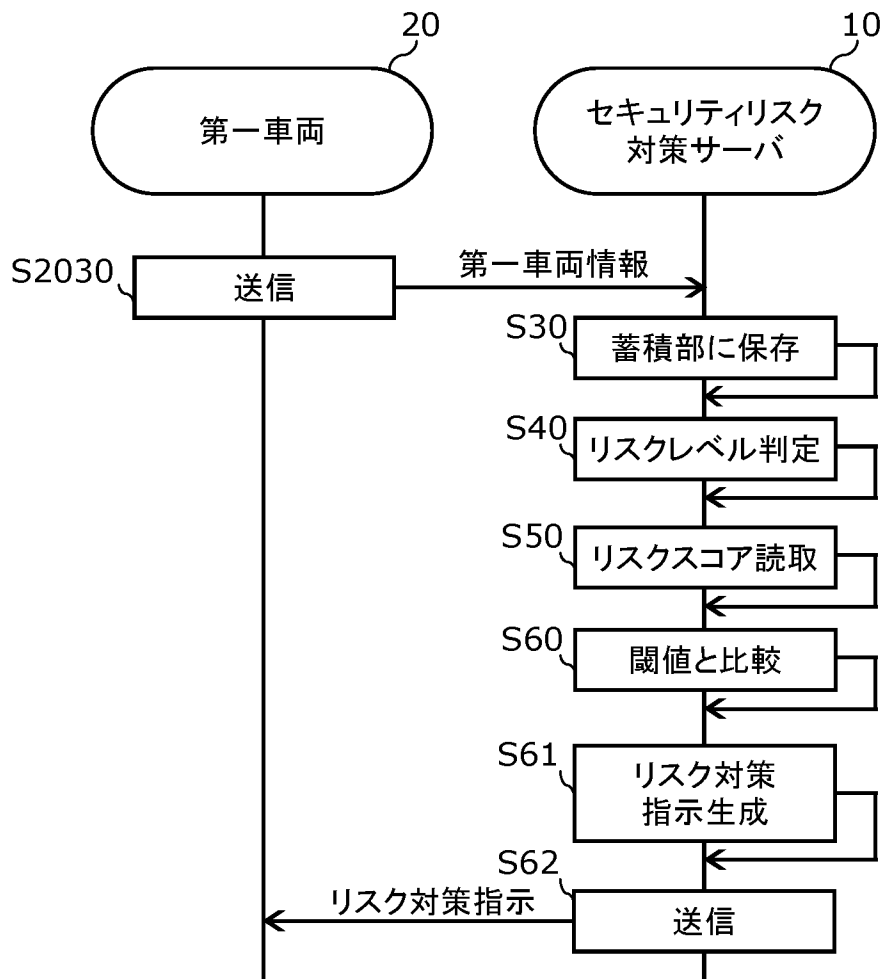
[図7G]

機能名	走行状態	リスクポイント
自動運転	高速走行	15
	低速走行	5
	停止	3
運転支援	高速走行	10
	低速走行	5
	停止	1
Wi-Fi 接続	高速走行	5
	低速走行	5
	停止	0
Bluetooth 接続	高速走行	5
	低速走行	5
	停止	0
走行制御	高速走行	20
	低速走行	10
	停止	0
LTE 通信	高速走行	5
	低速走行	5
	停止	0
OTA 機能	高速走行	5
	低速走行	5
	停止	0
⋮	⋮	⋮

[図8]



[図9]



[図10]

車両 ID: 10000A 2020/12/05				
型番	製造者	ソフトウェアバージョン	関連機能	
ECU-a	A 社	1.0.2	自動運転	
ECU-b	A 社	3.0.3	運転支援, 自動運転	
ECU-c	B 社	2.0.1	速度制御	
⋮	⋮	⋮	⋮	
IVI-a	B 社	1.0.0	LTE 通信, Wi-Fi 通信	
IVI-b	C 社	3.1.0	OTA	
⋮	⋮	⋮	⋮	

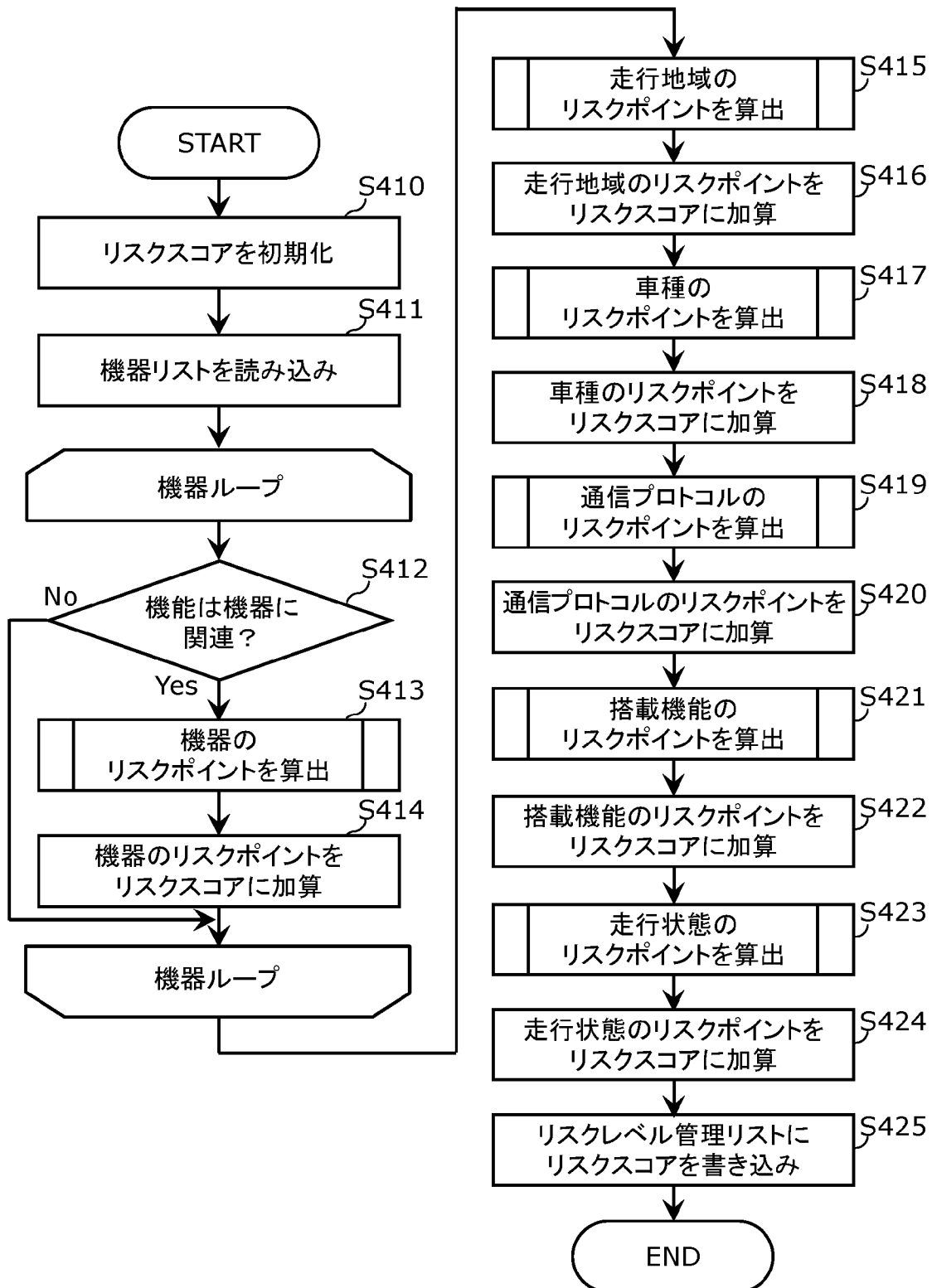
[図11]

車両 ID	日時	走行位置	車種	通信プロトコル	搭載機能	走行状態
10000A	2020/10/12 08:00:30	東京都〇〇区	X	CAN, FlexRay, MOST	運転支援, 自動運転, Wi-Fi	自動運転/ 停止

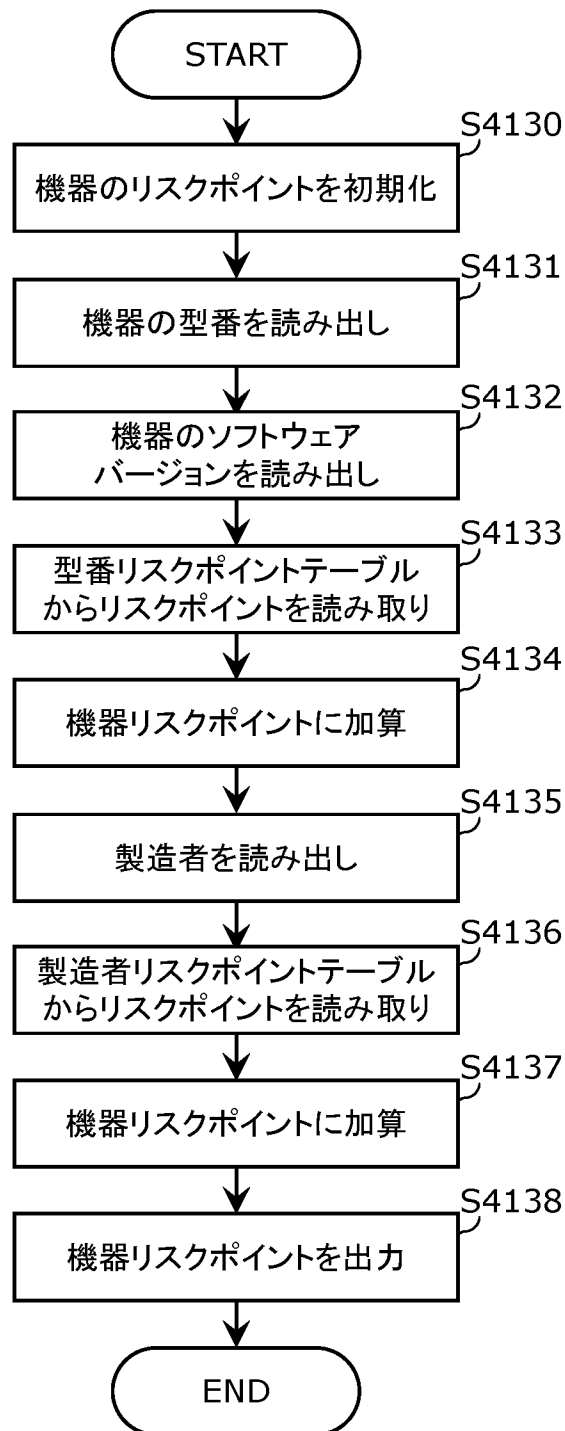
[図12]

機能名	種類	制限	無効化	リスク スコア
自動運転	走行	特定の自動運転機能を停止	自動運転機能を無効化	203
運転支援	走行	特定の運転支援機能を停止	運転支援機能を無効化	53
Wi-Fi 接続	通信	走行中の Wi-Fi 接続を禁止	Wi-Fi 接続機能を無効化	67
Bluetooth 接続	通信	走行中の Bluetooth 接続を禁止	Bluetooth 接続機能を無効化	29
走行制御	走行	速度上限を 80km/h に設定、 最短車間距離の拡大	走行機能を無効化	0
LTE 通信	通信	LTE 通信時帯域制限	LTE 通信機能無効化	10
OTA 機能	通信	OTA 実行時帯域制限	OTA 機能無効化	0
：	：	：	：	：

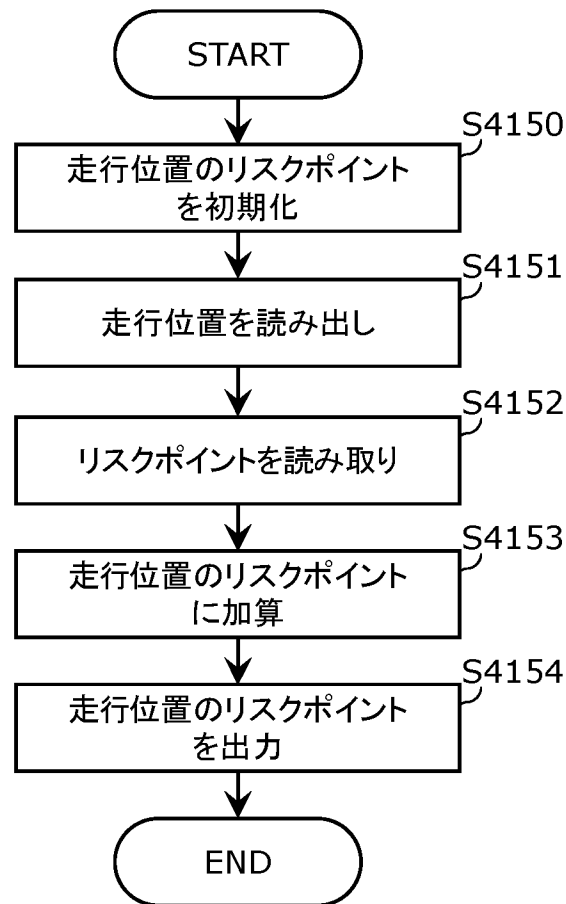
[図13]



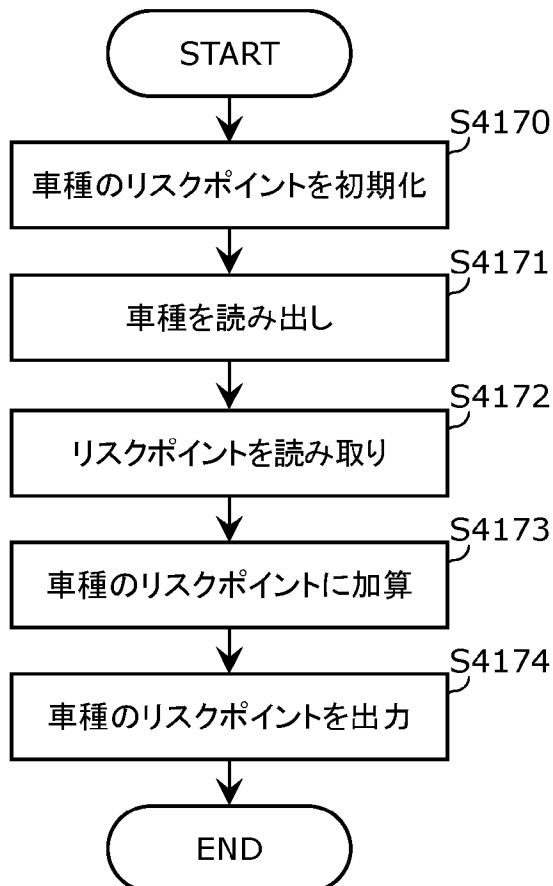
[図14A]



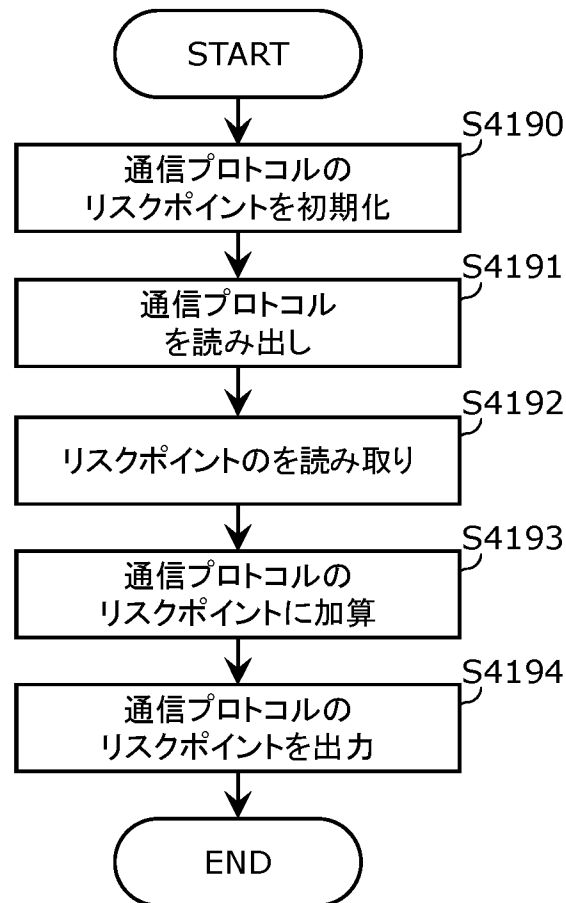
[図14B]



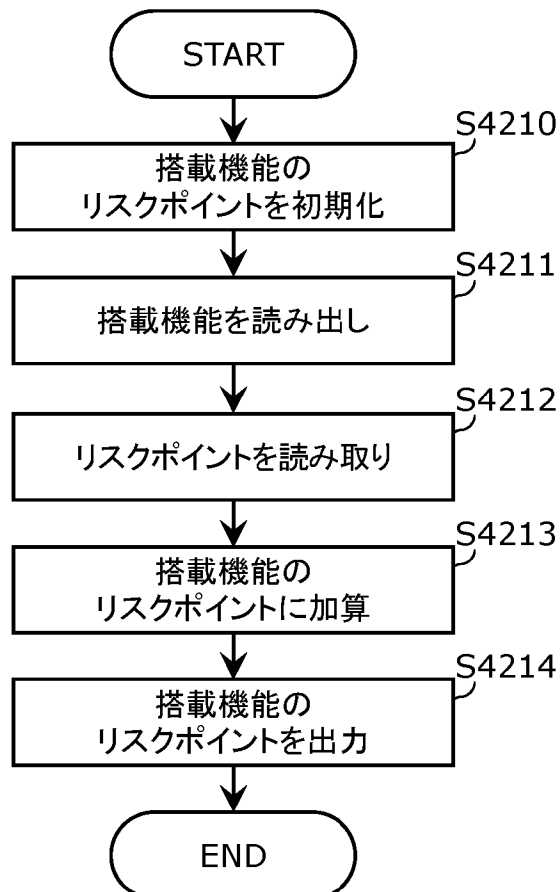
[図14C]



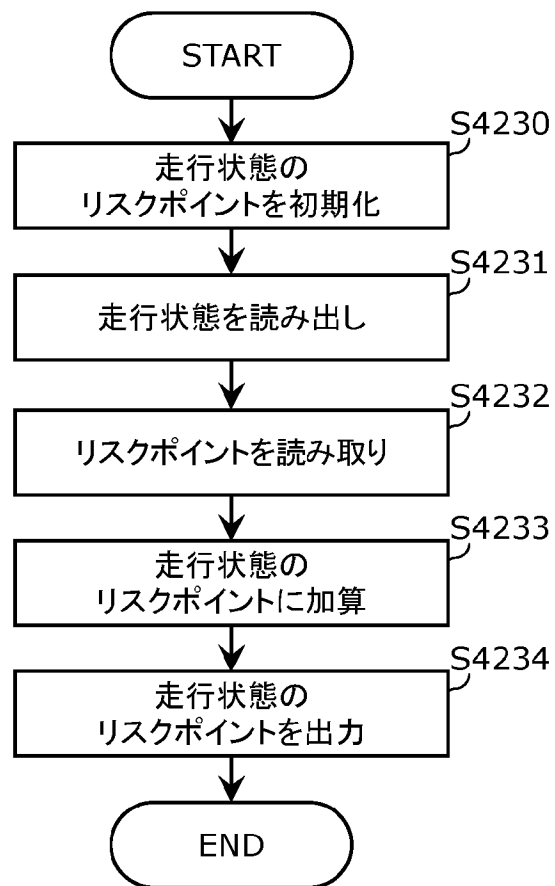
[図14D]



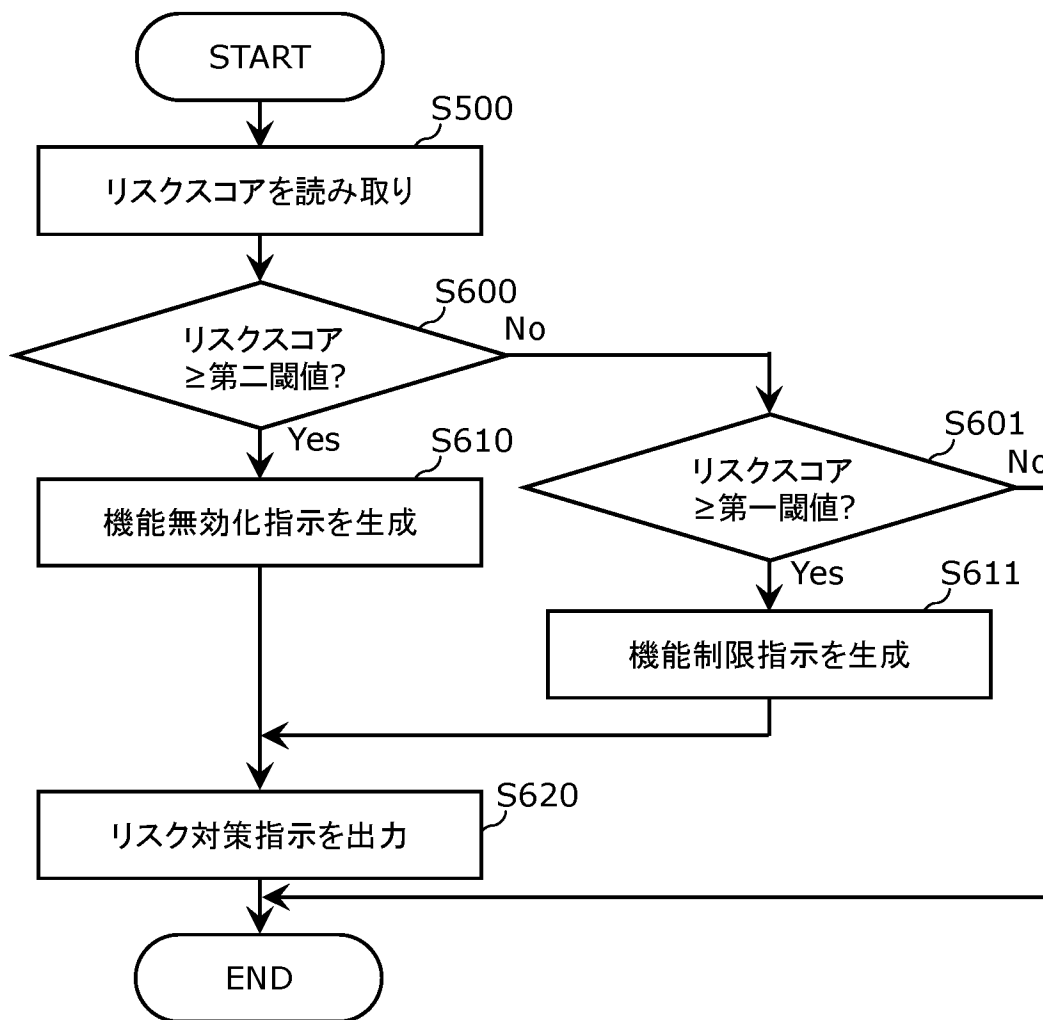
[図14E]



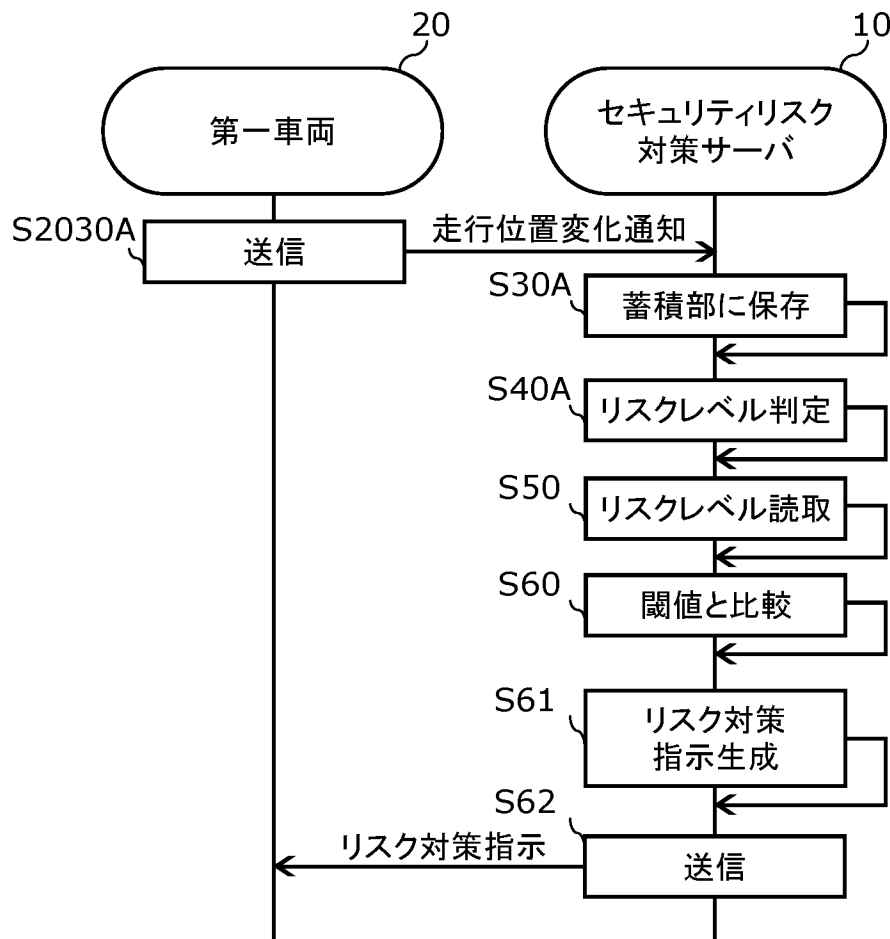
[図14F]



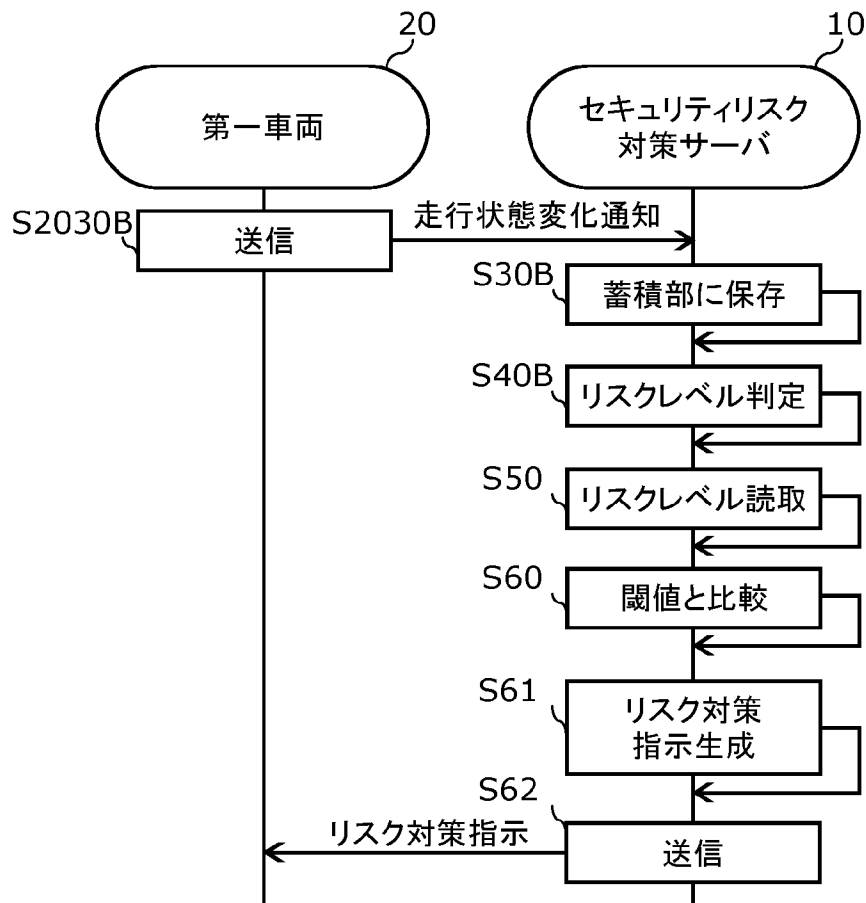
[図15]



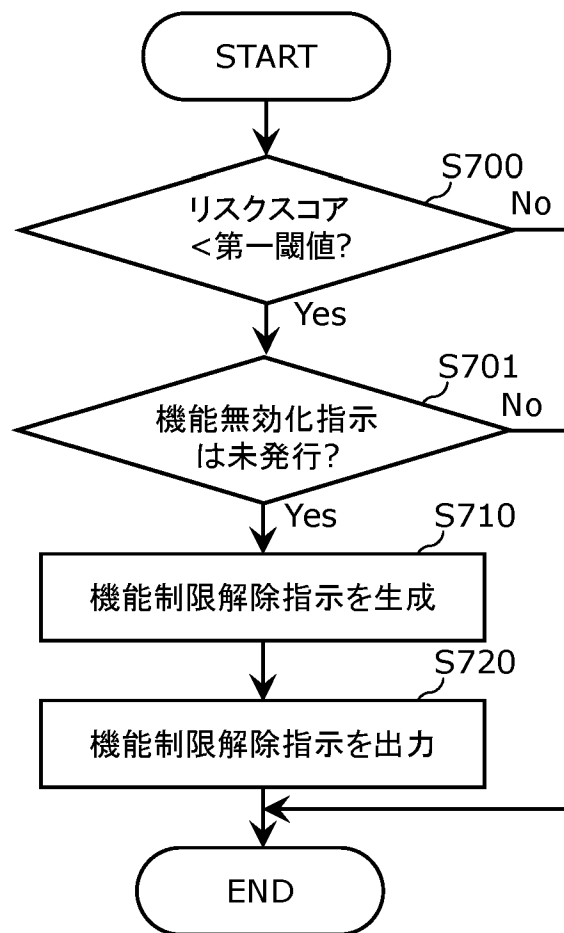
[図16A]



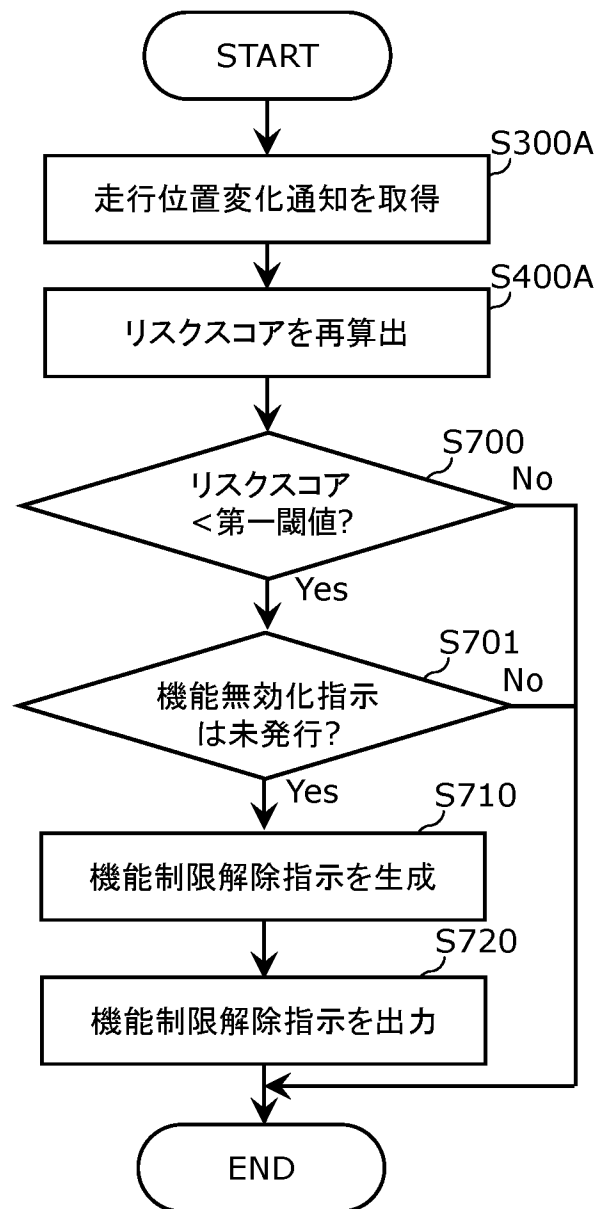
[図16B]



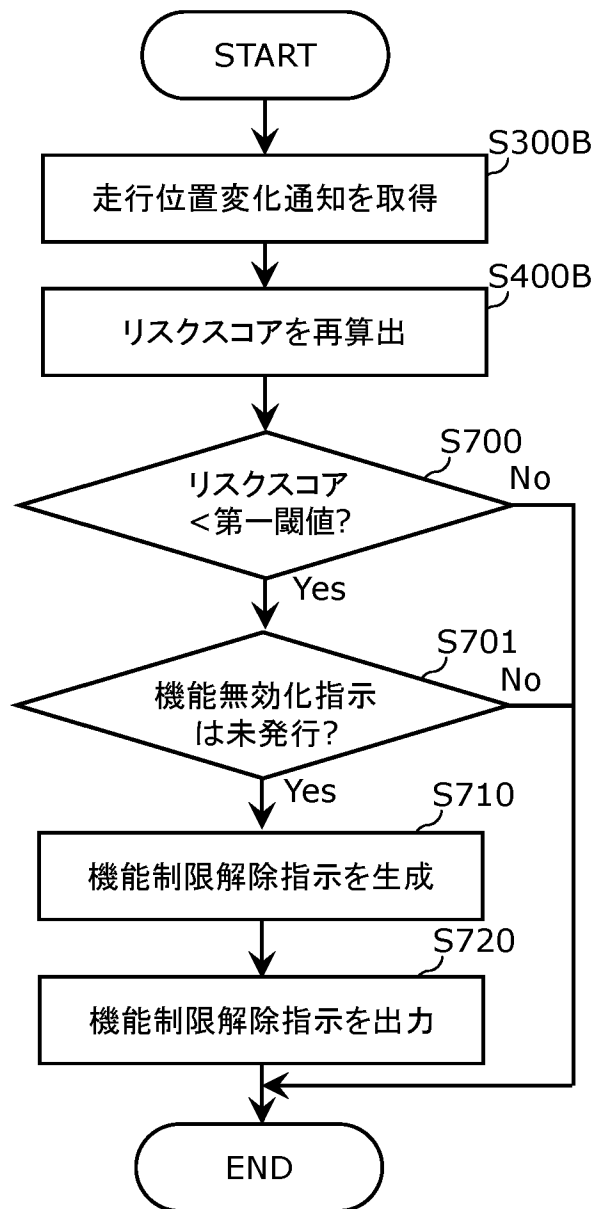
[図17]



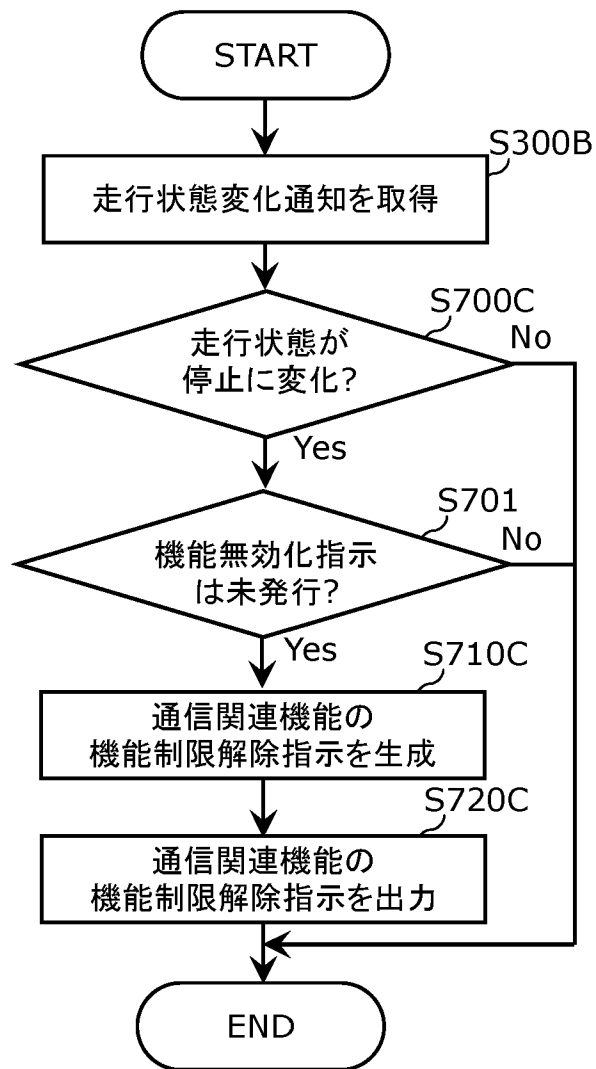
[図18A]



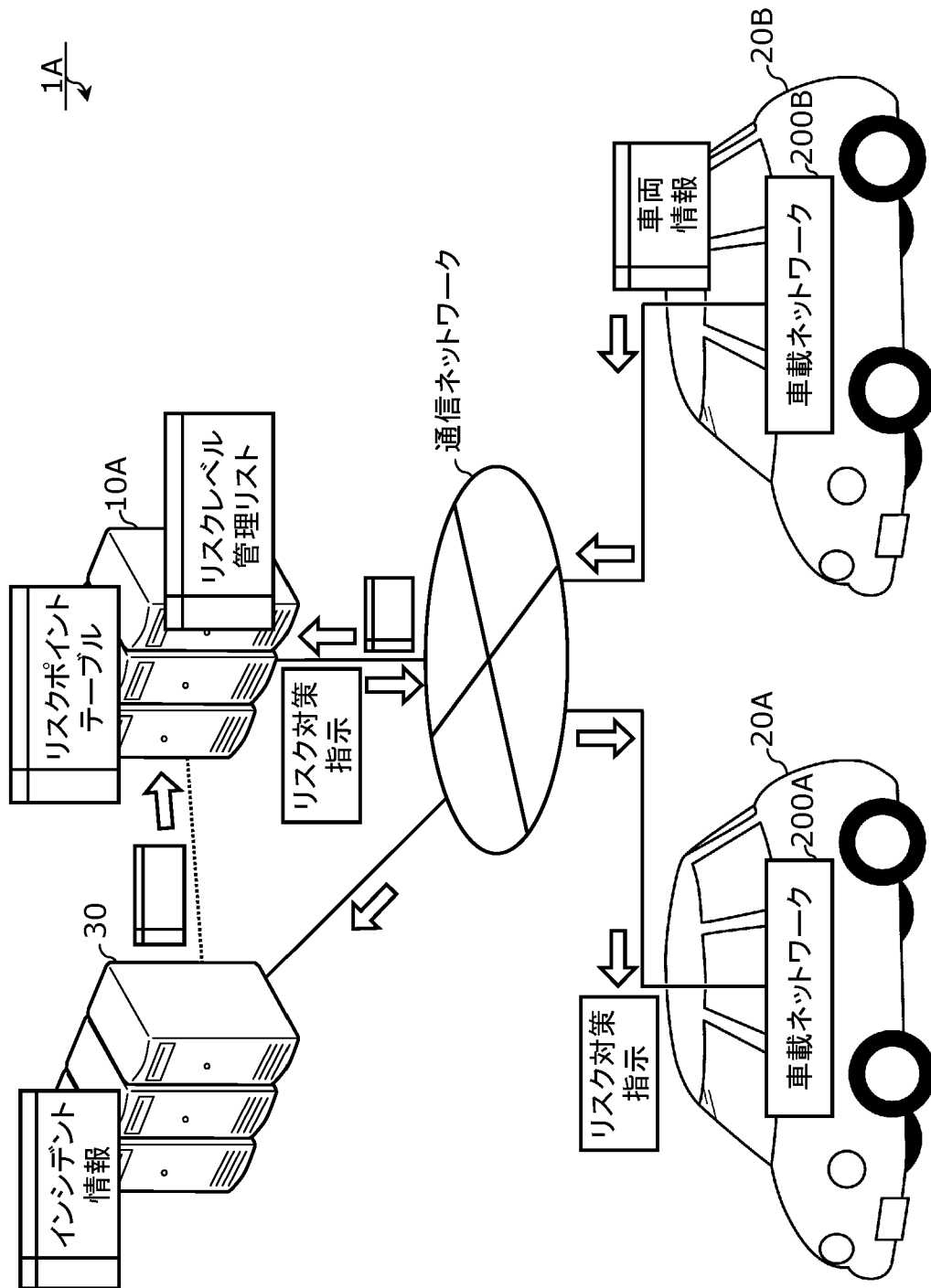
[図18B]



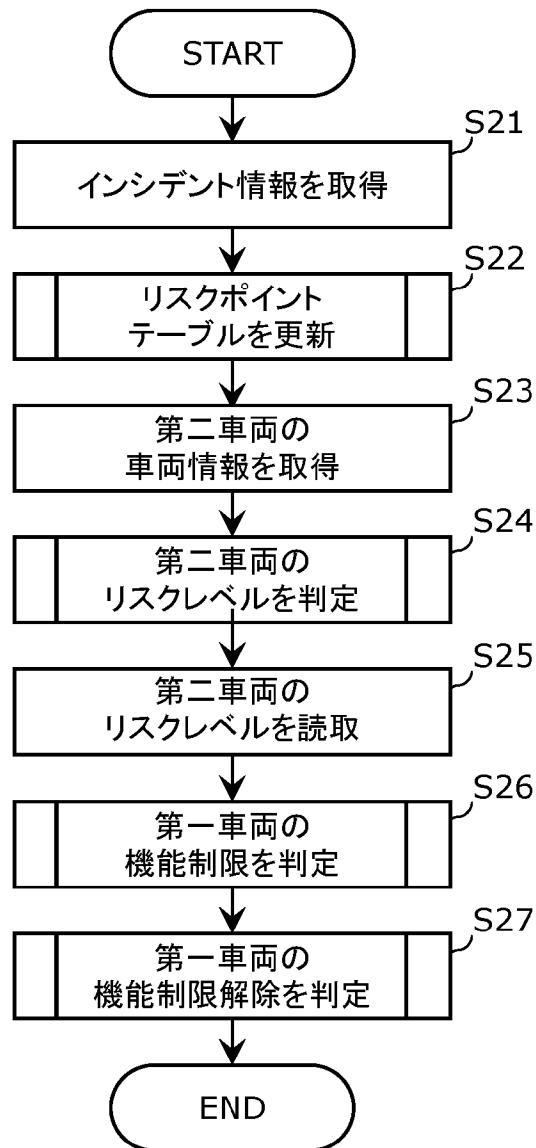
[図18C]



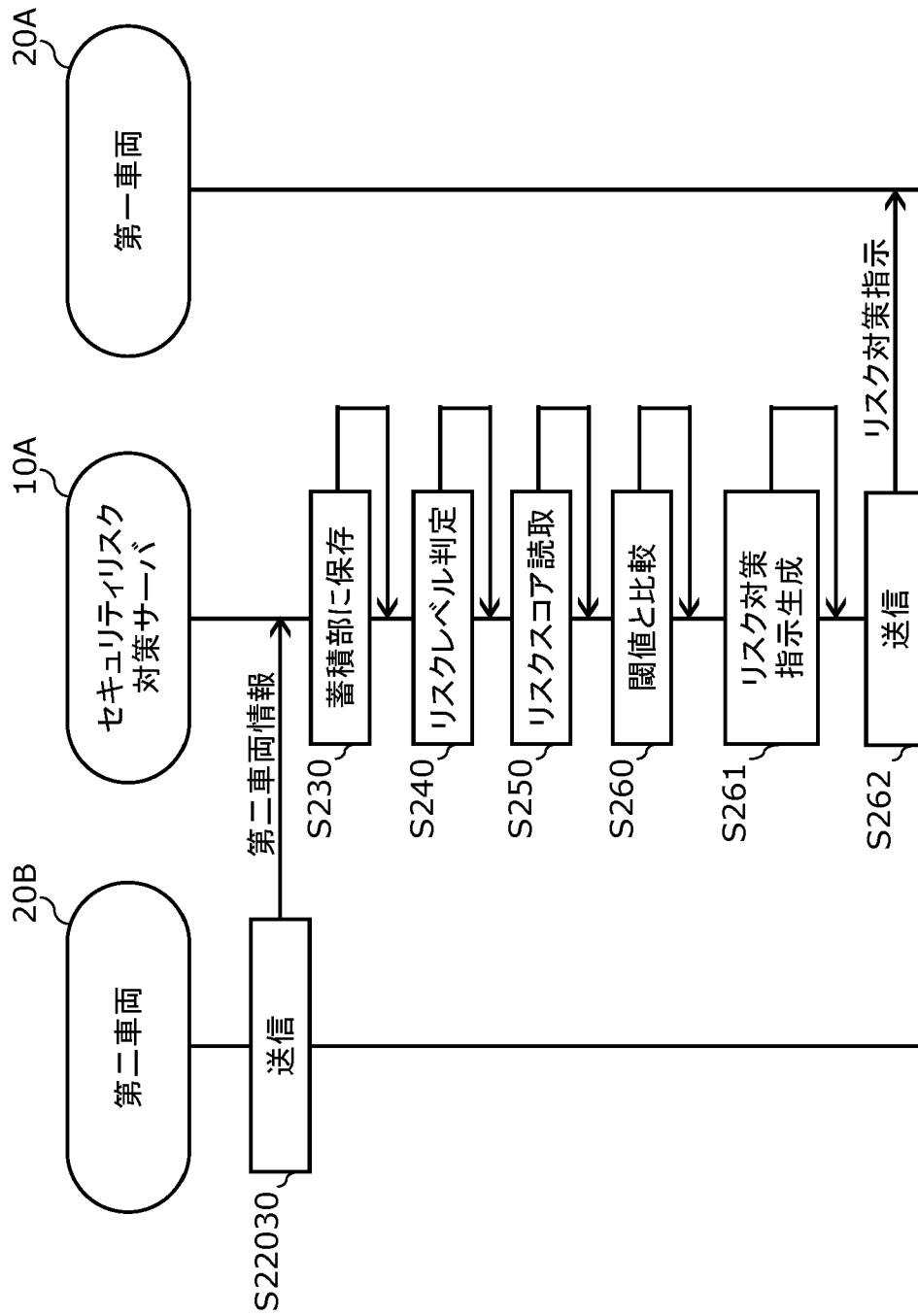
[図19]



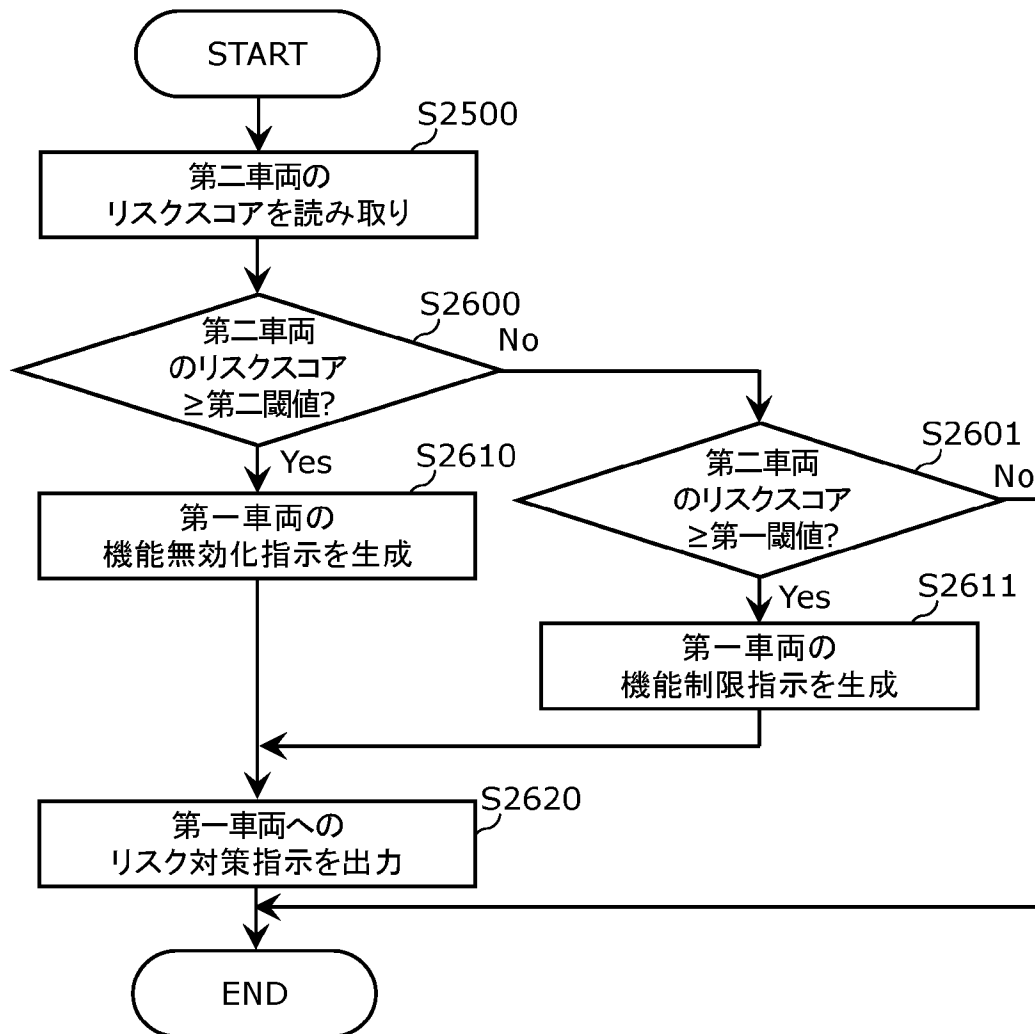
[図20]



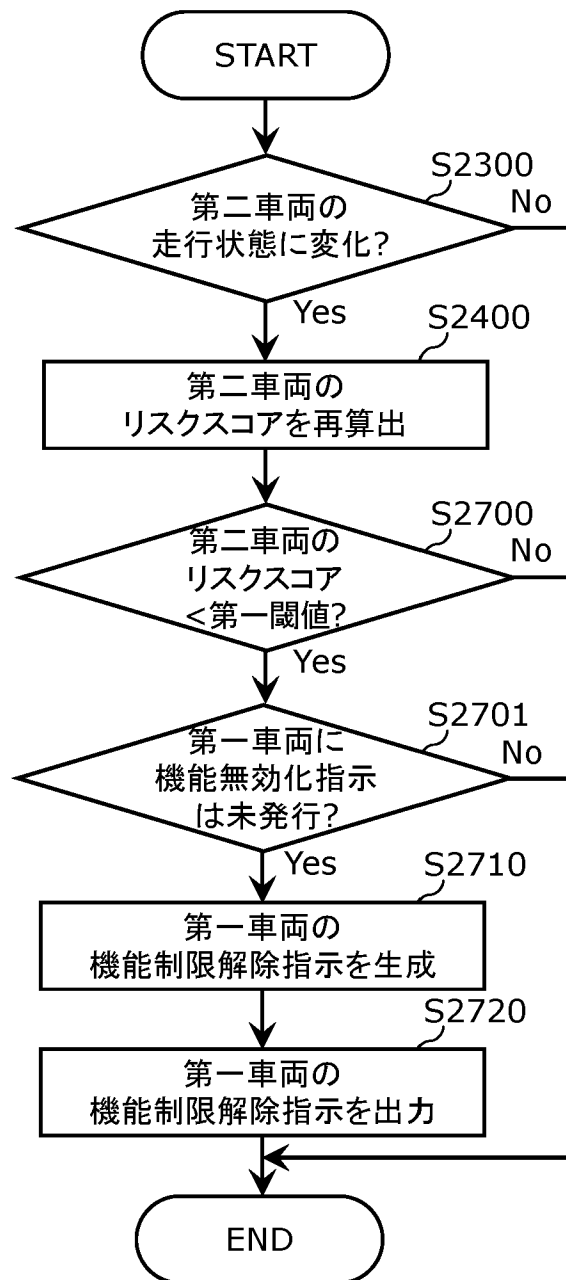
[図21]



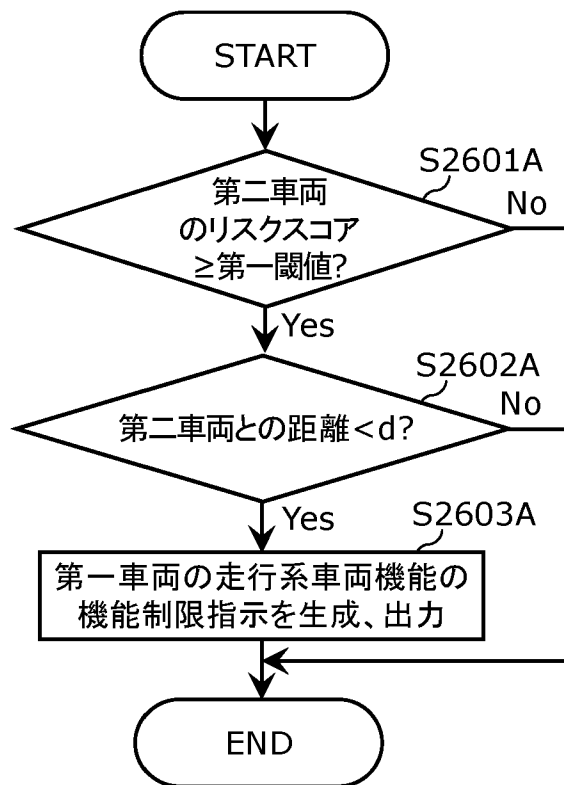
[図22]



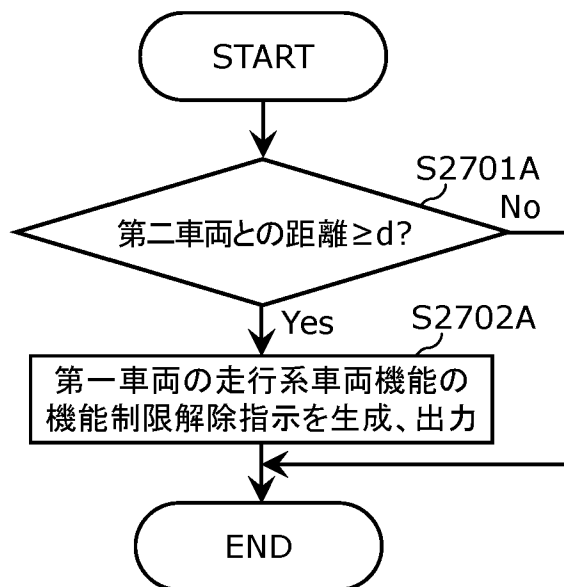
[図23]



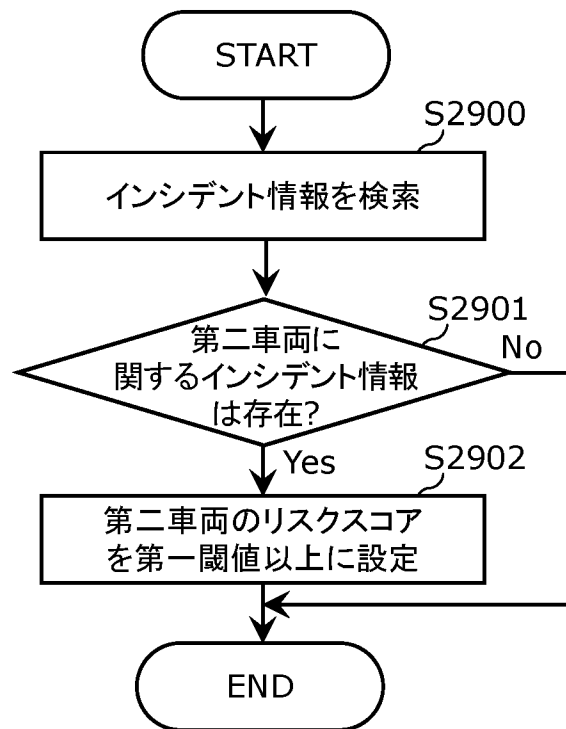
[図24A]



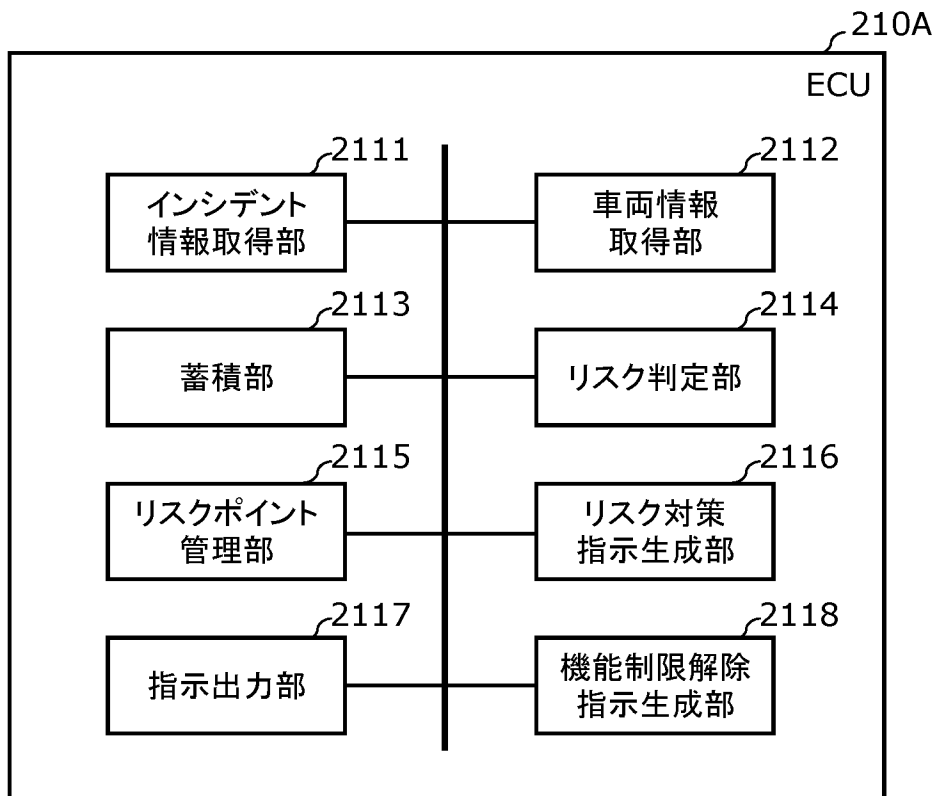
[図24B]



[図25]



[図26]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/032336

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. B60R25/01 (2013.01) i, B60R25/102 (2013.01) i, B60R25/33 (2013.01) i, G06F21/55 (2013.01) i, G08G1/01 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl. B60R25/01, B60R25/102, B60R25/33, G06F21/55, G08G1/01

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

Published examined utility model applications of Japan 1922-1996

Published unexamined utility model applications of Japan 1971-2019

Registered utility model specifications of Japan 1996-2019

Published registered utility model applications of Japan 1994-2019

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2017-111796 A (PANASONIC INTELLECTUAL PROPERTY CORPORATION OF AMERICA) 22 June 2017, paragraphs [0024], [0067], [0070], [0072]-[0087], [0116], fig. 8 & US 2018/0295147 A1, paragraphs [0046], [0089], [0092], [0094]-[0109], [0138], fig. 8 & WO 2017/104112 A1 & EP 3393086 A1 & CN 107925600 A	1-10
A	JP 2018-41200 A (SUMITOMO ELECTRIC INDUSTRIES, LTD.) 15 March 2018 (Family: none)	1-10
A	JP 2017-167916 A (DENSO CORP.) 21 September 2017, & US 2017/0270291 A1	1-10

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search
17.09.2019

Date of mailing of the international search report
01.10.2019

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

Authorized officer

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl. B60R25/01(2013.01)i, B60R25/102(2013.01)i, B60R25/33(2013.01)i, G06F21/55(2013.01)i, G08G1/01(2006.01)i

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl. B60R25/01, B60R25/102, B60R25/33, G06F21/55, G08G1/01

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2019年
日本国実用新案登録公報	1996-2019年
日本国登録実用新案公報	1994-2019年

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

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
X	JP 2017-111796 A (パナソニック インテレクチュアル プロパティ コーポレーション オブ アメリカ) 2017.06.22, [0024], [0067], [0070], [0072]-[0087], [0116], 図 8 & US 2018/0295147 A1 [0046], [0089], [0092], [0094]-[0109], [0138], FIG. 8 & WO 2017/104112 A1 & EP 3393086 A1 & CN 107925600 A	1-10
A	JP 2018-41200 A (住友電気工業株式会社) 2018.03.15, (ファミリーなし)	1-10

☑ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの	「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
「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	「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
「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)	「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
「O」 口頭による開示、使用、展示等に言及する文献	「&」 同一パテントファミリー文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願	

国際調査を完了した日

17.09.2019

国際調査報告の発送日

01.10.2019

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

森本 康正

3Q

2920

電話番号 03-3581-1101 内線 3381

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2017-167916 A (株式会社デンソー) 2017. 09. 21, & US 2017/0270291 A1	1-10