(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2021年2月4日(04.02.2021)

WIPO | PCT

(10) 国際公開番号
WO 2021/019636 A1

(51) 国際特許分類:
H04L 12/46 (2006.01)

(21) 国際出願番号： PCT/JP2019/029627

(22) 国際出願日： 2019年7月29日(29.07.2019)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(71) 出願人: オムロン株式会社 (**OMRON CORPORATION**) [JP/JP]; 〒6008530 京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地 Kyoto (JP).

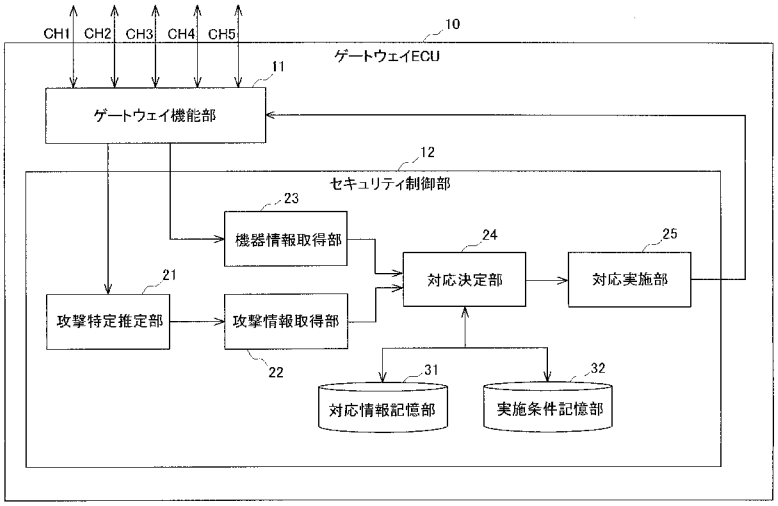
(72) 発明者: 山本 泰生 (**YAMAMOTO Taisei**); 〒6008530 京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地 オムロン株式会社内 Kyoto (JP). 廣部 直樹 (**HIROBE Naoki**); 〒6008530 京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地 オムロン株式会社内 Kyoto (JP). 小河原 徹 (**KOGAWARA Toru**); 〒6008530 京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地 オムロン株式会社内 Kyoto (JP).

(74) 代理人: 井内 龍二, 外 (**IUCHI Ryuji** et al.); 〒5300047 大阪府大阪市北区西天満４丁目１４番３号 リゾートトラスト御堂筋ビル１８階 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,

(54) **Title:** SECURITY DEVICE, INCIDENT HANDLING METHOD, PROGRAM, AND STORAGE MEDIUM

(54) 発明の名称： セキュリティ装置、インシデント対応処理方法、プログラム、及び記憶媒体



10 Gateway ECU
11 Gateway function unit
12 Security control unit
21 Attach identification estimation unit
22 Attack information acquisition unit
23 Device information acquisition unit
24 Handling determination unit
25 Handling execution unit
31 Handling information storage unit
32 Execution condition storage unit

(57) **Abstract:** The purpose of the present invention is to provide a security device capable of quickly executing incident handling under an appropriate condition with the state of equipment taken into consideration with respect to a plurality of attacks to an equipment network. The security device is provided with: an attack information acquisition unit; an equipment information acquisition unit; a handling information storage unit; a handling determination unit; and a handling execution unit, wherein when the acquired attack information includes two or more attacks, the handling determination unit determines incident handling execution conditions with respect to the two or more attacks in view of the function limiting levels of the attacks and the acquired equipment information, and the handling execution unit executes the incident

WO 2021/019636 A1

[続葉有]

BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, 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:

— 国際調査報告(条約第21条(3))

handling with respect to the two or more attacks on the basis of the determined execution conditions.

(57) 要約:本発明は、機器ネットワークに対する複数の攻撃に対して、機器の状態が考慮された適切な条件でインシデント対応を迅速に実施できるセキュリティ装置を提供することを目的とし、攻撃情報取得部と、機器情報取得部と、対応情報記憶部と、対応決定部と、対応実施部とを備え、前記対応決定部が、取得した攻撃情報に、２以上の攻撃が含まれている場合、これら攻撃の機能制限のレベルと、取得した機器情報とを考慮して、２以上の前記攻撃に対するインシデント対応の実施条件を決定し、前記対応実施部が、決定された前記実施条件に基づいて、２以上の前記攻撃に対する前記インシデント対応を実施する。

明　細　書

発明の名称 ：

セキュリティ装置、インシデント対応処理方法、プログラム、及び記憶媒体

技術分野

[0001] 本発明は、セキュリティ装置、インシデント対応処理方法、プログラム、及び記憶媒体に関する。

背景技術

[0002] 特許文献１には、車両に構築されたネットワークに接続された複数の車両制御装置と、これら車両制御装置間の通信を管理するゲートウェイ通信制御装置とから構成された車載通信システムが開示されている。

[0003] 前記ゲートウェイ通信制御装置は、ある車両制御装置からのメッセージの受信完了時または受信途中に、メッセージに含まれる信頼性が確認できるデータや信号に基づいて、通信信頼性（正常又は異常）を判断する。そして、前記ゲートウェイ通信制御装置は、通信結果が正常な場合、他の車両制御装置に対するゲートウェイ送信を継続する一方、通信結果が異常な場合、ゲートウェイ送信を中断するか、または異常メッセージをゲートウェイ送信データに付加する処理を実行するようになっている。

[0004] 従来の車載通信システムでは、ゲートウェイ通信制御装置を介した複数の車両制御装置間の通信時に、前記ゲートウェイ通信制御装置が、前記各車両制御装置から受信した情報に基づいて異常を検出すると、安全性確保の観点から、前記車両制御装置間の通信を停止させたり、受信情報を中継しなかったりする対策がとられている。

[0005] ［発明が解決しようとする課題］

しかしながら、車両制御装置間の通信を停止したり、情報を中継しなかったりする対策が実施されると、各車両制御装置で必要な情報であるにもかかわらず、これら情報が前記各車両制御装置で受信されず、前記車両制御装置

による制御が必要以上に制限されたり、制御が適切に実行できなくなったりして、車両の利便性が損なわれるという課題があった。

さらに、複数の異常が同時に検出された場合、これら異常に対する対応が重複して実行されるなどの過剰な対応が実施されることによって、前記車両制御装置で行われるべき制御が過剰に制限されて、車両の利便性が大きく損なわれたり、ハードウェアのリソースが必要以上に奪われたりするという課題があった。

先行技術文献

特許文献

[0006] 特許文献1：特開２０１５－８８９４１号公報

発明の概要

課題を解決するための手段及びその効果

[0007] 本発明は上記課題に鑑みなされたものであって、機器ネットワークに対する複数の攻撃の情報を取得した場合であっても、これら攻撃に対して、機器の状態が考慮された適切な条件でインシデント対応を迅速に実施することができるセキュリティ装置、インシデント対応処理方法、プログラム、及び記憶媒体を提供することを目的としている。

[0008] 上記目的を達成するために本開示に係るセキュリティ装置（１）は、１以上の機器が通信路を介して接続された機器ネットワークに含まれるセキュリティ装置であって、

前記機器ネットワークに発生した異常に基づいて特定又は推定された攻撃の情報（以下、攻撃情報という）を取得する攻撃情報取得部と、

前記機器の状態に関する情報（以下、機器情報という）を取得する機器情報取得部と、

前記攻撃の種類ごとに、インシデント対応と該対応による機能制限のレベルとが紐付けられた情報（以下、対応情報という）が記憶される対応情報記憶部と、

取得した前記攻撃情報と前記対応情報とに基づいて、前記攻撃情報に含まれる前記攻撃に対して実施すべき前記インシデント対応を決定する対応決定部と、

決定された前記インシデント対応を実施する対応実施部とを備え、

前記対応決定部が、

取得した前記攻撃情報に、一の前記通信路又は一の前記機器に対する２以上の前記攻撃が含まれている場合、これら攻撃の前記機能制限のレベルと、取得した前記機器情報とを考慮して、前記２以上の前記攻撃に対する前記インシデント対応の実施条件を決定するものであり、

前記対応実施部が、

決定された前記実施条件に基づいて、前記２以上の前記攻撃に対する前記インシデント対応を実施するものであることを特徴としている。

[0009] 上記セキュリティ装置（１）によれば、取得した前記攻撃情報に、前記２以上の前記攻撃が含まれている場合であっても、これら攻撃に対する前記インシデント対応に紐付けられた前記機能制限のレベルと、取得した前記機器情報とが考慮された、前記２以上の前記攻撃に対する前記インシデント対応の実施条件が決定され、決定された前記実施条件に基づいて、前記２以上の前記攻撃に対する前記インシデント対応が実施される。

[0010] したがって、当該セキュリティ装置単体で、前記攻撃情報に含まれる前記２以上の前記攻撃に対して、これら攻撃の前記機能制限のレベルと前記機器の状態とが考慮された適切な条件で前記インシデント対応を効率良く迅速に実施することができる。

[0011] 例えば、前記２以上の前記攻撃に対して、重複した対応など、必要以上に過剰な対応を実施しないようにすることが可能となり、ハードウェアリソースの消耗を抑制することができる。また、前記機器の状態に応じて、前記機器の機能が過剰に制限されることを抑制しつつ、前記攻撃への前記インシデント対応を実施することも可能となる。

なお、前記通信路は、有線の通信路であってもよいし、無線の通信路であ

ってもよいし、有線と無線とを含む通信路であってもよい。

[0012] また本開示に係るセキュリティ装置（２）は、上記セキュリティ装置（１）において、

前記攻撃の対象に含まれる前記通信路の種別と、前記機器情報と、前記実施条件との関係を示すテーブル情報が記憶される実施条件記憶部を備え、

前記対応決定部が、

取得した前記攻撃情報に、前記２以上の前記攻撃が含まれている場合、前記テーブル情報に基づいて、前記攻撃の対象となった前記一の前記通信路と、取得した前記機器情報とに対応する前記実施条件を決定するものであることを特徴としている。

[0013] 上記セキュリティ装置（２）によれば、前記テーブル情報には、前記通信路の種別と、前記機器情報と、前記実施条件との関係が記憶されているので、前記対応決定部が前記テーブル情報を用いることで、前記攻撃の対象となった前記一の前記通信路と、取得した前記機器情報とに対応する前記実施条件を効率良く決定することができ、処理の高速化を図ることができる。

[0014] また本開示に係るセキュリティ装置（３）は、上記セキュリティ装置（１）又は（２）において、

前記実施条件には、前記機能制限のレベルの降順又は昇順に実施する条件が含まれていることを特徴としている。

[0015] 前記攻撃の種類は、多種多様であり、前記機器又は前記通信路などの設備に軽微な影響しか与えない攻撃もあれば、前記設備に甚大な影響を与える攻撃もあり、前記設備がこれら攻撃により受ける影響は一律ではない。また、前記攻撃に対する前記インシデント対応も、その攻撃の種類によって異なる。

したがって、前記攻撃に対する前記インシデント対応が、例えば、一部のメッセージを遮断する、又は一部のメッセージを転送しないといった、前記設備の一部分にしか影響を与えないような内容であれば、前記インシデント対応に伴う前記機能制限のレベルは低くなる。

一方、前記攻撃に対する前記インシデント対応が、例えば、全メッセージを遮断する、又は全メッセージを転送しないといった、前記設備の多くの部分に影響を与える内容であれば、前記インシデント対応に伴う前記機能制限のレベルは高くなる。

[0016] 上記セキュリティ装置（３）によれば、前記２以上の前記攻撃に対して、前記機能制限のレベルの降順に（換言すれば、前記機能制限が大きい方の対応から順に）、前記インシデント対応を実行させたり、前記機能制限のレベルの昇順に（換言すれば、前記機能制限が小さい方の対応から順に）、前記インシデント対応を実行させたりすることが可能となる。したがって、前記機器の状態に適した順番で前記インシデント対応を実行することができる。

[0017] 例えば、前記攻撃の対象となった前記機器の状態が、緊急性が高い状態である場合、前記機能制限のレベルの降順に、前記インシデント対応を実行することで、重複した対応を回避しつつ、前記攻撃による被害の拡大を速やかに阻止することが可能となる。

また、前記攻撃の対象となった前記機器の状態が、緊急性がさほど高くない状態である場合、前記機能制限のレベルの昇順に、前記インシデント対応を実行することで、重複した対応を回避しつつ、また、前記機器の機能が過剰に制限されることを抑制することができ、前記機器による利便性を損なわないように前記インシデント対応を実行することが可能となる。

[0018] また本開示に係るセキュリティ装置（４）は、上記セキュリティ装置（１）又は（２）において、

前記実施条件には、前記機能制限のレベルが高い方又は低い方の前記攻撃に対する前記インシデント対応を実施する条件が含まれていることを特徴としている。

[0019] 上記セキュリティ装置（４）によれば、前記２以上の前記攻撃に対して、前記機能制限のレベルが高い方の前記インシデント対応を実行させたり、前記機能制限のレベルが低い方の前記インシデント対応を実行させたりすることが可能となる。したがって、前記機器の状態に適した方の前記インシデン

ト対応を優先的に実行することができ、上記セキュリティ装置（３）と同様の効果を得ることができる。

[0020] また本開示に係るセキュリティ装置（５）は、上記セキュリティ装置（１）～（４）のいずれかにおいて、

前記機器が、車両に搭載される制御装置であり、

前記機器ネットワークが、車載ネットワークであることを特徴としている。

[0021] 上記セキュリティ装置（５）によれば、１以上の前記制御装置が前記通信路を介して接続された前記車載ネットワークに対して前記攻撃を受けた場合、前記車両単体で、前記攻撃情報に含まれる前記２以上の前記攻撃に対して、これら攻撃の前記機能制限のレベルと前記機器の状態とが考慮された適切な条件で前記インシデント対応を効率良く迅速に実施することができる。したがって、前記車両のユーザは、セキュリティの脅威に対して不安を抱くことなく、より安心して乗車することが可能となる。

[0022] また本開示に係るセキュリティ装置（６）は、上記セキュリティ装置（５）において、

前記制御装置には、前記車両の走行系制御装置、運転支援系制御装置、ボディ系制御装置、情報系制御装置、及び診断用コネクタ装置のうちの少なくとも１つが含まれ、

前記機器情報には、手動運転中、運転支援中、リプログラミング中、及び駐車中のうちの少なくとも１つの車両状態に関する情報が含まれていることを特徴としている。

[0023] 上記セキュリティ装置（６）によれば、上記した制御装置のいずれか、又はこれら制御装置の前記通信路のいずれかに対する２以上の攻撃が含まれている場合であっても、これら攻撃に対して、これら攻撃の前記機能制限のレベルと、前記車両状態とが考慮された適切な条件で前記インシデント対応を効率良く迅速に実施することができる。

[0024] 例えば、前記手動運転中、前記運転支援中、又は前記駐車中に、前記走行

系制御装置の前記通信路に対する２以上の攻撃が特定又は推定された場合、前記機能制限のレベルが高い方の前記インシデント対応から実行することで、重複した対応を回避しつつ、前記攻撃による被害の拡大を速やかに阻止することが可能となる。

また、例えば、前記制御装置の前記リプログラミング中に、前記走行系制御装置の前記通信路に対する２以上の攻撃が特定又は推定された場合、前記機能制限のレベルが低い方の前記インシデント対応から実行することで、重複した対応を回避しつつ、また、前記制御装置の機能が過剰に制限されることを抑制しつつ、前記インシデント対応を実行することが可能となる。

[0025] また本開示に係るセキュリティ装置（７）は、上記セキュリティ装置（１）～（４）のいずれかにおいて、

前記機器が、ＦＡ（Factory Automation）システムを構成する産業機器に搭載される制御機器であり、

前記機器ネットワークが、前記ＦＡシステムを構成する産業機器ネットワークであることを特徴としている。

[0026] 上記セキュリティ装置（７）によれば、１以上の前記制御機器が前記通信路を介して接続された前記産業機器ネットワークに対して前記攻撃を受けた場合、前記産業機器単体で、前記攻撃情報に含まれる前記２以上の前記攻撃に対して、これら攻撃の前記機能制限のレベルと前記制御機器の状態とが考慮された適切な条件で前記インシデント対応を効率良く迅速に実施することができる。したがって、前記産業機器のユーザ（例えば、オペレータ）は、セキュリティの脅威に対して不安を抱くことなく、より安心して前記産業機器を使用することが可能となる。

[0027] また本開示に係るセキュリティ装置（８）は、上記セキュリティ装置（７）において、

前記制御機器には、

前記産業機器のプログラマブルコントローラ、フィールドネットワーク機器、無線機器、センサ、アクチュエータ、ロボット、ＨＭＩ（Human Machine

Interface）機器、及びデータ収集機器のうちの少なくとも１つが含まれ、

前記機器情報には、前記産業機器の運用フェーズである、立ち上げ中、通常稼動中、一時停止中、停止中、及びリプログラミング中のうちの少なくとも１つの前記運用フェーズに関する情報が含まれていることを特徴としている。

[0028] 上記セキュリティ装置（８）によれば、上記した制御機器のいずれか、又はこれら制御機器の前記通信路のいずれかに対する２以上の攻撃が含まれている場合であっても、これら攻撃に対して、これら攻撃の前記機能制限のレベルと、前記産業機器の運用フェーズとが考慮された適切な条件で前記インシデント対応を効率良く迅速に実施することができる。

[0029] 例えば、前記産業機器の前記立ち上げ中、前記通常稼動中、前記一時停止中、又は前記停止中に、前記プログラマブルコントローラ、又は前記フィールドネットワーク機器の前記通信路に対する２以上の攻撃が特定又は推定された場合、前記機能制限のレベルが高い方の前記インシデント対応から実行することで、重複した対応を回避しつつ、前記攻撃による被害の拡大を速やかに阻止することが可能となる。

また、例えば、前記制御機器の前記リプログラミング中に、前記プログラマブルコントローラ、又は前記フィールドネットワーク機器の前記通信路に対する２以上の攻撃が特定又は推定された場合、前記機能制限のレベルが低い方の前記インシデント対応から実行することで、重複した対応を回避しつつ、また、前記制御機器の機能が過剰に制限されることを抑制しつつ、前記インシデント対応を実行することが可能となる。

[0030] また本開示に係るインシデント対応処理方法は、１以上の機器が通信路を介して接続された機器ネットワークに含まれる少なくとも１以上のコンピュータが実行するインシデント対応処理方法であって、

前記機器ネットワークに発生した異常に基づいて特定又は推定された攻撃の情報（以下、攻撃情報という）を取得する攻撃情報取得ステップと、

前記機器の状態に関する情報（以下、機器情報という）を取得する機器情

報取得ステップと、

取得した前記攻撃情報、及び前記攻撃の種類ごとに、インシデント対応と該対応による機能制限のレベルとを紐付けて記憶された情報（以下、対応情報という）に基づいて、前記攻撃情報に含まれる前記攻撃に対して実施すべき前記インシデント対応を決定する対応決定ステップと、

決定された前記インシデント対応を実施する対応実施ステップとを含み、

前記対応決定ステップが、

取得した前記攻撃情報に、一の前記通信路又は一の前記機器に対する２以上の前記攻撃が含まれている場合、これら攻撃の前記機能制限のレベルと、取得した前記機器情報とを考慮して、前記２以上の前記攻撃に対する前記インシデント対応の実施条件を決定するステップを含み、

前記インシデント対応実施ステップが、

決定された前記実施条件に基づいて、前記２以上の前記攻撃に対する前記インシデント対応を実施するステップを含むことを特徴としている。

[0031] 上記インシデント対応処理方法によれば、取得した前記攻撃情報に、前記２以上の前記攻撃が含まれている場合であっても、これら攻撃の前記機能制限のレベルと、取得した前記機器情報とが考慮された、前記２以上の前記攻撃に対する前記インシデント対応の実施条件を決定し、決定した前記実施条件に基づいて、前記２以上の前記攻撃に対する前記インシデント対応を実施することが可能となる。

[0032] したがって、前記機器ネットワークに含まれる前記コンピュータ単体で、前記攻撃情報に含まれる前記２以上の前記攻撃に対して、これら攻撃の前記機能制限のレベルと前記機器の状態とが考慮された適切な条件で前記インシデント対応を効率良く迅速に実施することができる。

[0033] 例えば、前記２以上の前記攻撃に対して、重複した対応など、必要以上に過剰な対応を実施しないようにすることが可能となり、ハードウェアリソースの消耗を抑制することができる。また、前記機器の状態に応じて、前記機器の機能が過剰に制限されることを抑制しつつ、前記攻撃への前記インシデ

ント対応を実施することも可能となる。

[0034] また本開示に係るプログラムは、上記インシデント対応処理方法の各ステップを前記機器ネットワークに含まれる少なくとも１以上のコンピュータに実行させるためのプログラムであることを特徴としている。

[0035] 上記プログラムによれば、前記機器ネットワークに含まれる少なくとも１以上のコンピュータに、前記攻撃情報に含まれる前記２以上の前記攻撃に対して、これら攻撃の前記機能制限のレベルと前記機器の状態とが考慮された適切な条件で前記インシデント対応を効率良く迅速に実施させることができる。上記プログラムは、記憶媒体に保存されたプログラムであってもよいし、通信ネットワークなどを介して転送可能なプログラムであってもよい。

[0036] また本開示に係る記憶媒体は、上記インシデント対応処理方法の各ステップを前記機器ネットワークに含まれる少なくとも１以上のコンピュータに実行させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体であることを特徴としている。

[0037] 上記記憶媒体によれば、前記機器ネットワークに含まれる少なくとも１以上のコンピュータに前記プログラムを読み込ませて実行させることにより、前記攻撃情報に含まれる前記２以上の前記攻撃に対して、これら攻撃の前記機能制限のレベルと前記機器の状態とが考慮された適切な条件で前記インシデント対応を効率良く迅速に実施させることができる。

図面の簡単な説明

[0038] [図1]実施の形態に係るセキュリティ装置が適用された車載ネットワークシステムの概略ブロック図である。

[図2]実施の形態に係るゲートウェイＥＣＵの機能構成例を示すブロック図である。

[図3]攻撃情報取得部で取得される攻撃情報の一例と、機器情報取得部で取得される機器情報の一例とを説明するための図である。

[図4]対応情報記憶部に記憶されている、攻撃の種別ごとの対応情報の一例を説明するための図である。

[図5]実施条件記憶部に記憶されている、テーブル情報の一例を説明するための図である。

[図6]攻撃例１～４における攻撃情報、実施条件、及びインシデント対応の内容を説明するためのテーブルである。

[図7]実施の形態に係るゲートウェイＥＣＵを構成するセキュリティ制御部が行う処理動作を示す概略フローチャートである。

[図8]実施の形態に係るゲートウェイＥＣＵを構成するセキュリティ制御部が行うインシデント対応処理動作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

[0039] 以下、本発明に係るセキュリティ装置、インシデント対応処理方法、プログラム、及び記憶媒体の実施の形態を図面に基づいて説明する。

[0040] ［適用例］

図１は、実施の形態に係るセキュリティ装置が適用された車載ネットワークシステムの概略ブロック図である。

[0041] 車載ネットワーク２は、車両１に搭載された通信ネットワークシステムであり、ＯＢＤII（On-board diagnostics II）４、走行系ＥＣＵ（Electronic Control Unit）群５、運転支援系ＥＣＵ群６、ボディ系ＥＣＵ群７、情報系ＥＣＵ群８、及びゲートウェイＥＣＵ１０を含んで構成されている。本実施の形態における車載ネットワーク２は、ＣＡＮ（Controller Area Network）プロトコルに従って通信するネットワークである。なお、車載ネットワーク２には、ＣＡＮ以外の他の通信規格が採用されてもよい。また、走行系ＥＣＵ群５、運転支援系ＥＣＵ群６、ボディ系ＥＣＵ群７、及び情報系ＥＣＵ群８（以下、これらをまとめてＥＣＵ群ともいう）は、車両１に搭載される制御装置の一例である。

[0042] ＯＢＤII４、走行系ＥＣＵ群５、運転支援系ＥＣＵ群６、ボディ系ＥＣＵ群７、及び情報系ＥＣＵ群８は、それぞれ通信路であるバス３を介して、ゲートウェイＥＣＵ１０のＣＨ１、ＣＨ２、ＣＨ３、ＣＨ４、及びＣＨ５に接続されている。なお、ゲートウェイＥＣＵ１０の有するＣＨ数は、この５つ

に限定されるものではない。また、図１の例では、ＥＣＵ群が機能系統ごとにゲートウェイＥＣＵ１０に接続されたセントラルゲートウェイ方式が採用されているが、ゲートウェイＥＣＵ１０の接続方式は、この方式に限定されず、各ＥＣＵ群の間にゲートウェイＥＣＵ１０が設けられた方式などであってもよい。

[0043] ＯＢＤII４は、故障診断、又は保守等を行うための診断器又はスキャンツールなどが接続されるポートを備えている診断用コネクタ装置の一例である。

[0044] 走行系ＥＣＵ群５には、駆動系ＥＣＵと、シャーシ系ＥＣＵとが含まれている。駆動系ＥＣＵには、エンジン制御、モータ制御、燃料電池制御、EV（Electric Vehicle）制御、又はトランスミッション制御等の「走る」機能に関する制御ユニットが含まれている。シャーシ系ＥＣＵには、ブレーキ制御、又はステアリング制御等の「止まる、曲がる」機能に関する制御ユニットが含まれている。

[0045] 運転支援系ＥＣＵ群６には、自動ブレーキ支援機能、車線維持支援機能（ＬＫＡ／Lane Keep Assistともいう）、定速走行・車間距離支援機能（ＡＣＣ／Adaptive Cruise Controlともいう）、前方衝突警告機能、車線逸脱警報機能、死角モニタリング機能、交通標識認識機能、ドライバモニタリング機能等、走行系ＥＣＵ群５などとの連携により自動的に安全性の向上、又は快適な運転を実現する機能（運転支援機能、又は自動運転機能）に関する制御ユニットが少なくとも１つ以上含まれている。

[0046] 運転支援系ＥＣＵ群６には、例えば、米国自動車技術会（SAE）が提示している自動運転レベルにおけるレベル１（ドライバ支援）、レベル２（部分的自動運転）、及びレベル３（条件付自動運転）の機能が装備されていてもよい。さらに、自動運転レベルのレベル４（高度自動運転）、レベル５（完全自動運転）の機能が装備されていてもよいし、またはレベル２、３のみの機能が装備されていてもよい。

[0047] ボディ系ＥＣＵ群７には、ドアロック、スマートキー、パワーウインドウ

、エアコン、ライト、又はウインカ等の車体の機能に関する制御ユニットが少なくとも１つ以上含まれている。

[0048] 情報系ＥＣＵ群８は、インフォテイメント装置、テレマティクス装置、又はＩＴＳ（Intelligent Transport Systems）関連装置が含まれている。インフォテイメント装置には、カーナビゲーション装置、又はオーディオ機器などが含まれ、テレマティクス装置には、携帯電話網等へ接続するための通信ユニットなどが含まれている。ＩＴＳ関連装置には、ＥＴＣ（Electronic Toll Collection System）、又はＩＴＳスポットなどの路側機との路車間通信、若しくは車々間通信を行うための通信ユニットなどが含まれている。

[0049] また、外部インターフェースがゲートウェイＥＣＵ１０に接続されてもよい。外部インターフェースには、例えば、Bluetooth（登録商標）、Wi-Fi（登録商標）、USB(Universal Serial Bus)ポート、又はメモリーカードスロットなどが含まれる。

[0050] ゲートウェイＥＣＵ１０は、車載ネットワーク２に含まれる各ＥＣＵ群との間で、ＣＡＮプロトコルに従ってフレーム（メッセージ）の授受を行う機能を有し、本実施の形態に係るセキュリティ装置として機能する。

[0051] ゲートウェイＥＣＵ１０は、車載ネットワーク２に発生した異常を検出し、検出した異常に基づいて攻撃（セキュリティ攻撃、又はサイバー攻撃ともいう）の種類を特定又は推定し、特定又は推定した攻撃に対するインシデント対応を速やかに実行する処理を行う。

[0052] 特に本実施の形態に係るゲートウェイＥＣＵ１０は、ＣＨ１～ＣＨ５のうちの一のバス３、又は一のＥＣＵ群に対する攻撃に、２以上の攻撃が含まれている場合であっても、これら攻撃のインシデント対応による機能制限のレベルと、ＥＣＵ群から取得した車両情報とを考慮して、２以上の攻撃に対するインシデント対応の処理順序などの実施条件を決定し、決定した実施条件に基づいて、２以上の攻撃に対するインシデント対応を迅速かつ効率よく実施する処理を行う。

これにより、車両１がセキュリティ攻撃を受けた場合であっても、車両１

の機能が過剰に制限されることなく、換言すれば、車両１の利便性を損なくことなく、インシデント対応を実行することができ、車両１のユーザは、セキュリティ攻撃の脅威に対して不安を抱くことなく、安心して車両１に乗車することが可能となる。

[0053] 走行系ＥＣＵ群５、運転支援系ＥＣＵ群６、ボディ系ＥＣＵ群７、及び情報系ＥＣＵ群８、及びゲートウェイＥＣＵ１０は、１つ以上のプロセッサ、メモリ、及び通信モジュールなどを含むコンピュータ装置で構成されている。そして、各ＥＣＵに搭載されたプロセッサが、メモリに記憶されたプログラムを読み出し、プログラムを解釈し実行することで、各ＥＣＵで所定の制御が実行されるようになっている。

[0054] ［構成例］

図２は、実施の形態に係るゲートウェイＥＣＵ１０の機能構成例を示すブロック図である。

ゲートウェイＥＣＵ１０は、ゲートウェイ機能部１１と、セキュリティ制御部１２とを含んでいる。セキュリティ制御部１２が、本実施の形態に係るセキュリティ装置の機能が実装される部分である。ゲートウェイＥＣＵ１０は、ハードウェアとして、プログラムが格納されるＲＯＭ（Read Only Memory）、ＲＡＭ（Random Access Memory）などを含むメモリ、該メモリからプログラムを読み出して実行するＣＰＵ（Central Processing Unit）などのプロセッサ、及び車載ネットワーク２に接続するための通信モジュールなどを含んで構成されている。

[0055] ゲートウェイ機能部１１は、各ＥＣＵ群とバス３を介してフレーム（メッセージ）を転送する制御を行う機能を備えており、例えば、図示しないフレーム送受信部、フレーム解釈部、及びフレーム変換部など、車載ネットワーク２の各ＥＣＵ群との間でＣＡＮプロトコルに従って相互通信するために必要な構成が含まれている。

[0056] ＣＡＮプロトコルにおけるフレームは、例えば、データフレーム、リモートフレーム、オーバーロードフレーム、及びエラーフレームを含んで構成さ

れている。データフレームは、ＳＯＦ（Start Of Frame）、ＩＤ、ＲＴＲ（Remote Transmission Request）、ＩＤＥ（Identifier Extension）、予約ビット、ＤＬＣ（Data Length Code）、データフィールド、ＣＲＣ（Cyclic Redundancy Check）シーケンス、ＣＲＣデリミタ（ＤＥＬ）、ＡＣＫ（Acknowledgement）スロット、ＡＣＫデリミタ（ＤＥＬ）、及びＥＯＦ（End Of Frame）の各フィールドを含んで構成されている。

[0057] セキュリティ制御部１２は、攻撃特定推定部２１、攻撃情報取得部２２、機器情報取得部２３、対応決定部２４、対応実施部２５、対応情報記憶部３１、及び実施条件記憶部３２を含んで構成されている。

[0058] セキュリティ制御部１２は、ハードウェアとして、上記各部で実行されるプログラムが格納されるＲＯＭ、ＲＡＭなどを含むメモリ、該メモリからプログラムを読み出して実行するプロセッサなどを含んで構成され、これらハードウェアとプログラムとが協働することによって、上記各部の機能が実現されるようになっている。

[0059] 攻撃特定推定部２１は、ゲートウェイ機能部１１から取得したフレームに基づいて、車載ネットワーク２に発生した異常（フレーム異常、又はバス異常など）を検出し、検出された異常に対応する攻撃の種類を特定する処理を行う。また、攻撃特定推定部２１は、攻撃の種類が特定できなかった（例えば、未知の攻撃であった）場合に、検出された異常に対応する攻撃の種類を推定する処理を行う。攻撃特定推定部２１で特定又は推定された攻撃の情報が攻撃情報取得部２２に送出される。

[0060] フレーム異常は、例えば、フレームのＩＤ毎に設定されるＲＴＲ、ＤＬＣ、ペイロード、受信周期などのパラメータを確認することで検出される。フレーム異常は、ＣＡＮ信号単体での異常を表している。

また、バス異常は、例えば、ＣＨ１～ＣＨ５の各バス３のバス負荷率、バス状態（バスエラーの有無などの状態）、これらバス３に出現するＩＤなどのパラメータを確認することで検出される。バス異常は、ＣＡＮ信号の状況的な異常を表している。

[0061] 攻撃の種類を特定する処理では、例えば、最初の異常を検出してから所定時間内に収集された異常のデータと、攻撃の種類ごとに予め保持されている異常検出パターン（複数の異常検出パラメータを含む）とを照合して、検出した異常に対応する攻撃の種類を特定する処理を行ってもよい。

また、攻撃の種別を推定する処理では、例えば、最初の異常を検出してから所定時間内に収集された異常のデータと、攻撃の種類ごとに予め保持されている攻撃推定パターン（複数の攻撃推定パラメータを含む）とを照合して、検出した異常に近しい攻撃の種類を推定する処理を行ってもよい。

[0062] 攻撃情報取得部２２は、車載ネットワーク２に発生した異常に基づいて特定又は推定された攻撃の情報（攻撃情報）を取得する処理を行うものであり、本実施の形態では、攻撃特定推定部２１で特定又は推定された攻撃情報を取得する処理を行う。そして攻撃情報取得部２２で取得された攻撃情報が対応決定部２４に送出される。

[0063] なお、ゲートウェイＥＣＵ１０が、攻撃情報を取得する構成はこれに限定されない。例えば、別の実施の形態では、攻撃特定推定部２１と同様の機能をクラウドコンピュータ上に設け、クラウドコンピュータ側で特定又は推定された攻撃情報を、外部の通信ネットワークを介した通信により取得する構成としてもよい。

[0064] 機器情報取得部２３は、ゲートウェイＥＣＵ１０とバス３を介して接続された各ＥＣＵ群のうちの少なくとも１以上のＥＣＵ群の状態に関する情報（機器情報）を取得する処理を行う。いずれか１以上のＥＣＵ群から取得する機器情報は、換言すれば、車両１の状態に関する情報（以下、車両情報ともいう）である。そして機器情報取得部２３で取得された車両情報が対応決定部２４に送出される。対応決定部２４に送出される車両情報は、例えば、攻撃特定推定部２１で異常のデータが収集された所定時間に対応する期間に取得された車両情報（換言すれば、攻撃を受けたタイミングでの車両情報）とすることができる。

[0065] 図３は、攻撃情報取得部２２で取得される攻撃情報の一例と、機器情報取

得部２３で取得される車両情報の一例を説明するための図である。

攻撃情報には、少なくとも特定又は推定された攻撃の種類の情報が含まれ、さらに、攻撃されたＣＨ（バス）、及び攻撃されたＥＣＵのうちの少なくともいずれかの情報が含まれてもよい。

[0066] 特定又は推定された攻撃の種類の情報には、「攻撃Ａ」、「攻撃Ｂ」のように、１種類の攻撃が特定された場合の情報の他、「攻撃Ａ、攻撃Ｂ、及び攻撃Ｃ」のように、複数の攻撃が特定された場合の情報、又は「攻撃Ａ、攻撃Ｂ、又は攻撃Ｃ」のように、複数の攻撃が推定された（一意に特定できない）場合の情報などが含まれる。

[0067] 攻撃されたＣＨ（バス）には、攻撃の対象となったＣＨ１～ＣＨ５の情報が含まれる。

攻撃されたＥＣＵには、走行系ＥＣＵ群５、運転支援系ＥＣＵ群６、ボディ系ＥＣＵ群７、情報系ＥＣＵ群８、及びゲートウェイＥＣＵ１０のうち、攻撃を受けたと特定又は推定されたＥＣＵの情報が含まれる。なお、走行系ＥＣＵ－１は、走行系ＥＣＵ群５に含まれている一のＥＣＵを示している。また、ゲートウェイＥＣＵ１０に対する直接的な攻撃も含まれる。

[0068] また、車両情報には、現在の車両１の状態（換言すれば、攻撃を受けたタイミングでの車両１の状態）に関する情報が含まれる。

例えば、手動運転中の状態を示す信号、運転支援（運転支援又は自動運転）中の状態を示す信号、リプログラミング中（ＥＣＵのプログラムを書換中）の状態を示す信号、又は駐車中の状態を示す信号などが含まれる。

[0069] 手動運転中の状態を示す信号には、例えば、走行系ＥＣＵ群５又は運転支援系ＥＣＵ群６から取得した手動運転モードを示す信号などが含まれる。

運転支援中の状態を示す信号には、例えば、運転支援系ＥＣＵ群６から取得した運転支援モード又は自動運転モードを示す信号などが含まれる。

リプログラミング中の状態を示す信号には、例えば、プログラムの書き換えが実行されているＥＣＵから取得したリプログラミング中の信号などが含まれる。

駐車中の状態を示す信号には、例えば、ボディ系ＥＣＵ群７から取得したスマートキーの状態を示す信号などが含まれる。

攻撃情報取得部２２で取得された攻撃情報と、機器情報取得部２３で取得された車両情報とが対応決定部２４に送出される。

[0070] 対応決定部２４は、攻撃情報取得部２２で取得した攻撃情報と、対応情報記憶部３１に記憶されている対応情報とに基づいて、攻撃情報に含まれる攻撃の種類に対して実施すべきインシデント対応を決定する処理を行う。対応決定部２４で決定されたインシデント対応の情報が対応実施部２５に送出される。

[0071] また、対応決定部２４は、取得した攻撃情報に、ＣＨ１～ＣＨ５のうち一のバス３又はＥＣＵ群のうちの一のＥＣＵに対する２以上の攻撃の種別が含まれている場合、これら攻撃の機能制限のレベルと、機器情報取得部２３で取得した機器情報とを考慮して、２以上の攻撃に対するインシデント対応の実施条件を決定する処理も行う。

[0072] 対応実施部２５は、対応決定部２４で決定されたインシデント対応を実施する。また、対応実施部２５は、対応決定部２４で決定された実施条件に基づいて、２以上の攻撃に対するインシデント対応を実施する。

[0073] 対応情報記憶部３１は、攻撃の種類ごとに、実施すべきインシデント対応と該対応による機能制限のレベルとが紐付けられた情報（対応情報）が記憶されている。

図４は、対応情報記憶部３１に記憶されている対応情報リストの一例を説明するための図である。

[0074] 図４に示す対応情報リストは、攻撃に関する情報と、実施する対応（インシデント対応）の内容と、該対応による機能制限レベルとが、攻撃の種類ごとに紐付けられたデータ構成となっている。

攻撃に関する情報には、攻撃種別と、攻撃の対象となったバスと、攻撃の対象となったＥＣＵとに関する情報が含まれている。

[0075] 攻撃種別の項目には、車載ネットワーク２において想定され得る攻撃の種

類（攻撃Ａ、Ｂ、・・・Ｋ、Ｌ・・）が記憶されている。これら攻撃の種類は、車載ネットワーク２のシステムに対する脅威分析（すなわち、ゲートウェイＥＣＵ１０、これに接続される走行系ＥＣＵ群５、運転支援系ＥＣＵ群６、ボディ系ＥＣＵ群７、情報系ＥＣＵ群８、及びＯＢＤII４に接続される機器、その他、車載ネットワーク２に繋がる通信機器などについての脆弱性や脅威の分析）により抽出された既知の攻撃を表している。これら攻撃を抽出するための脅威分析の手法は特に限定されない。例えば、ＤＦＤ（Date Flow Diagram）を用いた脅威抽出、STRIDEによる脅威分類、脅威ツリー、又はDREADによる脅威評価などの手法が採用され得る。これら攻撃（攻撃Ａ、Ｂ、…、Ｋ、Ｌ…）には、例えば、不正利用、不正設定、不正中継、不正挿入、情報漏洩、Ｄｏｓ攻撃、メッセージ喪失、又は偽メッセージなどの攻撃が含まれる。

[0076] バスの項目には、攻撃種別の項目に記憶された攻撃の対象となったバス（この場合、ＣＨ１～ＣＨ５のいずれか）の情報が記憶され、ＥＣＵの項目には、攻撃種別の項目に記憶された攻撃の対象となったＥＣＵ（例えば、走行系ＥＣＵ－１等）の情報が記憶されている。

[0077] 実施する対応の項目には、攻撃種別の項目に記憶された各攻撃に対処するために実施すべきインシデント対応の内容（対応Ａ、Ｂ、…、Ｋ、Ｌ…）が記憶されている。これら対応（対応Ａ、Ｂ、…、Ｋ、Ｌ…）には、例えば、バス遮断、メッセージ遮断、メッセージ破棄、代替メッセージ生成、再起動、又は再認証などの対応が含まれる。バス遮断には、両方向、転送先、又は転送元バスの遮断が含まれてもよい。メッセージ遮断には、両方向、転送先、又は転送元メッセージの遮断が含まれてもよい。

[0078] 機能制限レベルの項目には、実施すべきインシデント対応によって、ＥＣＵの機能が制限されるレベルを示す情報が記憶されている。ここでは、機能制限レベルの値が大きいほど、インシデント対応時におけるＥＣＵの機能の制限（換言すれば、縮退制御）が大きくなることを示している。

[0079] 図４に示す対応情報リストにおいて、例えば、攻撃Ａは、ＣＨ２のバス３

、走行系ＥＣＵ－１に対する攻撃であり、攻撃Ａに対するインシデント対応は対応Ａであり、対応Ａの機能制限レベルは５であることが紐付けて記憶されている。

[0080] 実施条件記憶部３２には、攻撃の対象に含まれるバスの種類と、車両情報と、実施条件との関係を示すテーブル情報が記憶されている。

このテーブル情報は、対応決定部２４において、攻撃情報取得部２２から取得した攻撃情報に、一のバス３（ＣＨ１～ＣＨ５のいずれか）又は一のＥＣＵ（ＥＣＵ群に含まれるいずれかのＥＣＵ）に対する２以上の攻撃（攻撃の種類）が含まれている場合に、これら攻撃に対するインシデント対応の実施条件を決定するために用いられる。

[0081] 図５は、実施条件記憶部３２に記憶されているテーブル情報の一例を説明するための図である。

図５に示すテーブル情報は、攻撃の対象に含まれるバス（ＣＨ１～ＣＨ５）と、車両情報（手動運転中、運転支援中、リプログラミング中、駐車中、…）と、実施条件（機能制限レベルの昇順又は降順）との関係を示すデータ構成となっている。

[0082] 例えば、ＣＨ１に対する２以上の攻撃については、車両情報が、手動運転中、運転支援中、リプログラミング中、駐車中のいずれの状態であっても機能制限レベルの昇順にインシデント対応を実行するという実施条件が記憶されている。

[0083] また、ＣＨ２又はＣＨ４のバス３に対する２以上の攻撃については、車両情報が、手動運転中、運転支援中、又は駐車中である場合、機能制限レベルの降順にインシデント対応を実行するという実施条件が記憶され、車両情報が、リプログラミング中である場合、機能制限レベルの昇順にインシデント対応を実行するという実施条件が記憶されている。

[0084] また、ＣＨ３のバス３に対する２以上の攻撃については、車両情報が、手動運転中、又は運転支援中である場合、機能制限レベルの降順にインシデント対応を実行するという実施条件が記憶され、車両情報が、リプログラミン

グ中、又は駐車中である場合、機能制限レベルの昇順にインシデント対応を実行するという実施条件が記憶されている。

[0085] また、ＣＨ５のバス３に対する２以上の攻撃については、車両情報が、手動運転中、リプログラミング中、又は駐車中である場合、機能制限レベルの昇順にインシデント対応を実行するという実施条件が記憶され、車両情報が、運転支援中である場合、機能制限レベルの降順にインシデント対応を実行するという実施条件が記憶されている。

[0086] なお、インシデント対応の実施条件は、上記した機能制限レベルの昇順又は降順の他、機能制限レベルが所定レベル以上又は所定レベル以下のインシデント対応を実施する条件でもよいし、機能制限レベルが最も高いインシデント対応のみ実施する条件などでもよい。攻撃の対象となったバス３と、車両１の状態に関する車両情報とに応じて、これらの実施条件を組み合わせてもよい。

なお、本実施の形態では、対応情報記憶部３１に記憶されている対応情報リストと、実施条件記憶部３２に記憶されているテーブル情報とを別々に設けているが、これらを一つのデータベースにまとめてもよい。

[0087] 次に攻撃情報を取得した場合における、対応決定部２４と、対応実施部２５とで行われる処理例について説明する。

図６は、攻撃例１～４における攻撃情報、実施条件、及びインシデント対応の内容を説明するためのテーブルである。

[0088] ［攻撃例１］

対応決定部２４は、攻撃情報（攻撃Ａ、ＣＨ２、走行系ＥＣＵ－１）を取得すると、対応情報記憶部３１に記憶された対応情報リスト（図４）を読み出し、この対応情報リストから攻撃種別が攻撃Ａに紐付けられた、実施する対応（対応Ａ）、及び機能制限レベル（５）の情報を抽出する。対応決定部２４は、取得した攻撃情報に２以上の攻撃が含まれていないと判断すると、対応実施部２５に対応Ａを実行させるための実行命令を送る。

[0089] 対応実施部２５は、対応決定部２４から対応Ａの実行命令を受け取ると、

対応Ａを実行する処理を行う。例えば、攻撃された走行系ＥＣＵ－１、又はＣＨ２のバス３に対して、メッセージ遮断、又はバス遮断など、対応Ａに設定されたインシデント対応を実行する。

[0090] ［攻撃例２］

対応決定部２４は、攻撃情報（攻撃Ｆ、ＣＨ４）を取得すると、対応情報記憶部３１に記憶された対応情報リスト（図４）を読み出し、この対応情報リストから攻撃種別が攻撃Ｆに紐付けられた、実施する対応（対応Ｆ）、及び機能制限レベル（２）の情報を抽出する。対応決定部２４は、取得した攻撃情報に２以上の攻撃が含まれていないと判断すると、対応実施部２５に対応Ｆを実行させるための実行命令を送る。

[0091] 対応実施部２５は、対応決定部２４から対応Ｆの実行命令を受け取ると、対応Ｆを実行する処理を行う。例えば、攻撃されたＣＨ４のバス３に対して、バス遮断など、対応Ｆに設定されたインシデント対応を実行する。

[0092] ［攻撃例３］

対応決定部２４は、攻撃情報（攻撃Ｇ又は攻撃Ｊ、ＣＨ３、運転支援系ＥＣＵ－１）を取得すると、対応情報記憶部３１に記憶された対応情報リスト（図４）を読み出し、この対応情報リストから攻撃種別が攻撃Ｇと攻撃Ｊとに紐付けられた、実施する対応（対応Ｇと対応Ｊ）、及び機能制限レベル（３と１）の情報を抽出する。

[0093] 対応決定部２４は、取得した攻撃情報に２以上の攻撃が含まれていると判断すると、機器情報取得部２３から車両情報（例えば、リプログラミング中）を取得する。また、対応決定部２４は、実施条件記憶部３２に記憶されたテーブル情報（図５）を読み出し、このテーブル情報から、攻撃対象のバス３と車両情報との関係に対応する、インシデント対応の実施条件を抽出する。

[0094] この場合、攻撃対象のバス３はＣＨ３、車両情報はリプログラミング（リプロ）中であるので、実施条件として機能制限レベル昇順が抽出される。

対応決定部２４は、対応実施部２５に、機能制限レベルが１の対応Ｊ、機

能制限レベルが３の対応Ｇの順に、これらインシデント対応を実行させるための実行命令を送る。

[0095] 対応実施部２５は、対応決定部２４から実行命令を受け取ると、対応Ｊ、対応Ｇの順（機能制限レベルの昇順）にこれらインシデント対応を実行する処理を行う。例えば、攻撃されたＣＨ３のバス３に接続された運転支援系ＥＣＵ－１に対して、受信メッセージ破棄など、機能制限レベルが低い方の対応Ｊに設定されたインシデント対応を実行し、異常が改善されなければ、運転支援系ＥＣＵ－１に対して、両方向メッセージ破棄など、機能制限レベルが高い方の対応Ｇに設定されたインシデント対応を実行する。

[0096] このように、リプログラミング中に、例えば、ＣＨ３に対する２以上の攻撃が特定された場合、機能制限レベルが低い方のインシデント対応から実行することで、重複した対応を回避しつつ、また、ＥＣＵの機能が過剰に制限されることを抑制することができ、ＥＣＵの制御による車両１の利便性を損なわないようにインシデント対応を実行することが可能となる。

[0097] ［攻撃例４］

対応決定部２４は、攻撃情報（攻撃Ｄ又は攻撃Ｅ、ＣＨ２、走行系ＥＣＵ－２）を取得すると、対応情報記憶部３１に記憶された対応情報リスト（図４）を読み出し、この対応情報リストから攻撃種別が攻撃Ｄと攻撃Ｅとに紐付けられた、実施する対応（対応Ｄと対応Ｅ）、及び機能制限レベル（４と２）の情報を抽出する。

[0098] 対応決定部２４は、取得した攻撃情報に２以上の攻撃が含まれていると判断すると、機器情報取得部２３から車両情報（例えば、手動運転中）を取得する。また、対応決定部２４は、実施条件記憶部３２に記憶されたテーブル情報（図５）を読み出し、このテーブル情報から、攻撃対象のバス３と、車両情報との関係に対応する、インシデント対応の実施条件を抽出する。

[0099] この場合、攻撃対象のバス３はＣＨ２、車両情報は手動運転中であるので、実施条件として機能制限レベル降順が抽出される。

対応決定部２４は、対応実施部２５に、機能制限レベルが４の対応Ｄ、機

能制限レベルが２の対応Ｅの順に、これらインシデント対応を実行させるための実行命令を送る。

[0100] 対応実施部２５は、対応決定部２４から実行命令を受け取ると、対応Ｄ、対応Ｅの順（機能制限レベルの降順）にこれらインシデント対応を実行する処理を行う。例えば、攻撃されたＣＨ２のバス３に対して、両方向バス遮断など、機能制限レベルが高い方の対応Ｄに設定されたインシデント対応を実行する。この場合、機能制限レベルが低い方の対応Ｅに設定されたインシデント対応は実行しないようにしてもよい。このように、機能制限レベルが高い方のインシデント対応から実行することで、重複した対応を回避しつつ、攻撃による被害の拡大を速やかに阻止することが可能となる。

[0101] ［動作例］

図７は、実施の形態に係るゲートウェイＥＣＵ１０を構成するセキュリティ制御部１２が行う処理動作を示した概略フローチャートである。なお、本処理動作は、攻撃者により車載ネットワーク２に何らかのセキュリティ攻撃が実施され、ゲートウェイＥＣＵ１０の防御機能が破られた場合を想定している。

[0102] まず、ステップＳ１では、セキュリティ制御部１２は、車載ネットワーク２に異常が発生したか否かを判断し、異常が発生していないと判断すれば処理を終える一方、異常が発生したと判断すれば、ステップＳ２に処理を進める。

[0103] ステップＳ２では、セキュリティ制御部１２は、各ＥＣＵ群から受信したフレーム又は各ＣＨに接続されたバス３に発生した異常を検出する処理を行い、その後ステップＳ３に処理を進める。

[0104] ステップＳ３では、セキュリティ制御部１２は、受信したフレーム又はバス３に発生した所定期間の異常のデータ（すなわち、異常の検出結果）を収集する処理を行い、その後ステップＳ４に処理を進める。

[0105] ステップＳ４では、セキュリティ制御部１２は、収集された異常のデータを用いて、セキュリティ攻撃の種類を特定する処理を行い、また、攻撃の種

類を特定できない場合に、その攻撃の種類を推定する処理を行い、その後ステップＳ５に処理を進める。

[0106] ステップＳ５では、セキュリティ制御部１２は、特定された攻撃の種類、又は推定された攻撃の種類に対応するインシデント対策を実施する処理を行い、その後処理を終える。

[0107] 図８は、実施の形態に係るゲートウェイＥＣＵ１０を構成するセキュリティ制御部１２が行うインシデント対応処理動作を示したフローチャートである。本処理動作は、図７のステップＳ５で行われるインシデント対応処理動作の一例である。

[0108] まずステップＳ１１では、セキュリティ制御部１２は、攻撃情報取得部２２として機能し、図７のステップＳ４で特定又は推定された攻撃の情報（攻撃情報）を取得する処理を行い、ステップＳ１２に処理を進める。攻撃情報には、少なくとも特定又は推定された攻撃の種類が含まれ、さらに、攻撃の対象となったＣＨ（バス）、及び攻撃されたＥＣＵのうちの少なくともいずれかの情報が含まれてもよい。

[0109] ステップＳ１２では、セキュリティ制御部１２は、機器情報取得部２３として機能し、ＣＨ１～ＣＨ５のバス３を介して接続された各ＥＣＵ群のうちの少なくとも１以上のＥＣＵ群の状態に関する情報（すなわち、車両情報）を取得する処理を行い、ステップＳ１３に処理を進める。

車両情報には、現在の車両１の状態（換言すれば、攻撃を受けたタイミングでの車両１の状態）に関する情報、例えば、図３に示した、手動運転中の状態を示す信号、運転支援（運転支援又は自動運転）中の状態を示す信号、リプログラミング中（ＥＣＵのプログラムを書換中）の状態を示す信号、又は駐車中の状態を示す信号などが含まれている。

[0110] ステップＳ１３では、セキュリティ制御部１２は、対応決定部２４として機能し、Ｓ１１で取得した攻撃情報に、ＣＨ１～ＣＨ５のうちの一のバス３またはＥＣＵ群のうちの一のＥＣＵに対する２以上の攻撃が含まれているか否かを判断し、２以上の攻撃が含まれていないと判断すれば、ステップＳ１

４に処理を進める。

[0111] ステップＳ１４では、セキュリティ制御部１２は、対応決定部２４として機能し、対応情報記憶部３１から対応情報リスト（図４）を読み出し、この対応情報リストから、取得した攻撃情報に含まれる攻撃の種類に該当する対応情報（実施する対応、及び機能制限レベル）を抽出する処理を行い、ステップＳ１５に処理を進める。

[0112] ステップＳ１５では、セキュリティ制御部１２は、対応決定部２４として機能し、抽出した対応情報に含まれるインシデント対応を実行させるための実行命令を対応実施部２５に送る処理を行い、ステップＳ１６に処理を進める。

[0113] ステップＳ１６では、セキュリティ制御部１２は、対応実施部２５として機能し、実行命令に基づいて、抽出した対応情報に含まれるインシデント対応を実行する処理を行い、その後処理を終える。

[0114] 一方、ステップＳ１３において、２以上の攻撃が含まれていると判断すれば、ステップＳ１７に処理を進める。

ステップＳ１７では、セキュリティ制御部１２は、対応決定部２４として機能し、対応情報記憶部３１に記憶された対応情報リスト（図４）を読み出し、この対応情報リストから２以上の攻撃の種類に該当する対応情報（各攻撃の実施する対応、及び機能制限レベルの情報）を抽出する処理を行い、その後ステップＳ１８に処理を進める。

[0115] ステップＳ１８では、セキュリティ制御部１２は、対応決定部２４として機能し、実施条件記憶部３２に記憶されたテーブル情報（図５）を読み出し、このテーブル情報から、攻撃対象のバス３と車両情報との関係に対応する、インシデント対応の実施条件を抽出する処理を行い、その後ステップＳ１９に処理を進める。

[0116] ステップＳ１９では、セキュリティ制御部１２は、対応決定部２４として機能し、抽出した実施条件に基づいて、対応情報に含まれる２以上の攻撃に対するインシデント対応を実行させるための実行命令を対応実施部２５に送

る処理を行い、ステップＳ２０に処理を進める。

[0117] ステップＳ２０では、セキュリティ制御部１２は、対応実施部２５として機能し、実行命令に基づき、抽出された対応情報に含まれる２以上の攻撃に対するインシデント対応を実施条件に基づいて実行する処理を行い、その後処理を終える。

[0118] ［作用・効果］

上記実施の形態に係るゲートウェイＥＣＵ１０によれば、攻撃情報取得部２２で取得した攻撃情報に、２以上の攻撃が含まれている場合であっても、これら攻撃に対するインシデント対応に紐付けられた機能制限レベルと、機器情報取得部２３で取得した車両情報とが考慮された、２以上の攻撃に対するインシデント対応の実施条件が決定され、決定された実施条件に基づいて、２以上の攻撃に対するインシデント対応が実施される。

[0119] したがって、車両１単体で、攻撃情報に含まれる２以上の攻撃に対して、これら攻撃の機能制限レベルとＥＣＵ群の状態（すなわち、車両情報）とが考慮された適切な条件でインシデント対応を効率良く迅速に実施することが可能となる。

[0120] 例えば、一のバス３又は一のＥＣＵに対する２以上の攻撃に対して、機能制限レベルの降順に（換言すれば、機能制限が大きい方の対応から順に）、インシデント対応を実行させたり、機能制限レベルの昇順に（換言すれば、機能制限が小さい方の対応から順に）、インシデント対応を実行させたりすることが可能となる。したがって、車両１の状態に適した順番でインシデント対応を実行することができる。

[0121] 一例として、攻撃の対象となったバス３又はＥＣＵの状態が、緊急性が高い状態である場合、機能制限レベルの降順にインシデント対応を実行することで、重複した対応を回避しつつ、攻撃による被害の拡大を速やかに阻止することが可能となる。

また、攻撃の対象となったバス３又はＥＣＵの状態が、緊急性がさほど高くない状態である場合、機能制限レベルの昇順にインシデント対応を実行す

ることで、重複した対応を回避しつつ、また、ＥＣＵの機能が過剰に制限されることを抑制することができ、ＥＣＵの制御による車両１の利便性を損なわないようにインシデント対応を実行することが可能となる。

[0122] なお、２以上の攻撃に対して、機能制限レベルが高い方のインシデント対応を実行させたり、機能制限レベルが低い方のインシデント対応を実行させたりしてもよく、これによって、ＥＣＵの状態に適した方のインシデント対応を優先的に実行することができる。

[0123] このように、一のバス３又は一のＥＣＵに対する２以上の攻撃に対して、重複した対応など、必要以上に過剰な対応を実施しないようにすることが可能となり、ハードウェアリソースの消耗を抑制することができる。また、車両１の状態に応じて、ＥＣＵ群の機能が過剰に制限されることを抑制しつつ、攻撃へのインシデント対応を実施することも可能となる。

したがって、車両１のユーザは、セキュリティの脅威に対して不安を抱くことなく、より安心して、快適に（すなわち、利便性が損なわれることなく）、車両１に乗車することができる。

[0124] また実施条件記憶部３２に記憶されているテーブル情報には、ＣＨ１～ＣＨ５のバス３の種別と、車両情報と、実施条件（機能制限レベルの昇順又は降順など）との関係が記憶されているので、対応決定部２４がテーブル情報を用いることで、攻撃の対象となった一のバス３と、ＥＣＵ群から取得した車両情報とに対応する実施条件を効率良く決定することができ、処理の高速化を図ることができる。

[0125] ［変形例］

以上、本発明の実施の形態を詳細に説明したが、前述までの説明はあらゆる点において本発明の例示に過ぎない。本発明の範囲を逸脱することなく、種々の改良や変更を行うことができることは言うまでもない。

[0126] 例えば、ゲートウェイＥＣＵ１０に実装されたセキュリティ制御部１２を、他のＥＣＵに搭載してもよいし、セキュリティ制御部１２が装備されたセキュリティＥＣＵを車載ネットワーク２に接続する構成としてもよい。

[0127] また別の実施の形態に係るゲートウェイＥＣＵ１０では、セキュリティ制御部１２において、車載ネットワーク２に接続された情報系ＥＣＵ群８に含まれる報知装置を介して車内の乗員に、決定されたインシデント対応に応じて、異常が発生したこと、攻撃が発生したことを報知したり、適切な運転操作、縮退運転の開始、継続、復帰、又は解除、異常発生後の対応などを報知したりする報知処理部をさらに備えてもよい。

[0128] このような報知装置には、ナビゲーション装置、又はオーディオ機器などが適用され得る。係る構成によれば、前記報知処理部によって、報知装置を介して車内の乗員に異常などを報知することが可能となるので、乗員に、異常又は攻撃などに対して適切な対応を実施させることが可能となる。

[0129] また別の実施の形態に係るゲートウェイＥＣＵ１０では、セキュリティ制御部１２において、車載ネットワーク２に接続された情報系ＥＣＵ群８に含まれるテレマティクス装置、又はＩＴＳ関連装置を介して車外に、上記した異常の発生又は攻撃の発生などを通報する通報処理部をさらに備えてもよい。係る構成によれば、前記通報処理部によって、テレマティクス装置、又はＩＴＳ関連装置を介して車外に異常の発生又は攻撃の発生などを通報することが可能となる。したがって、例えば、周辺の他車、インフラ設備、ディーラー、メーカー、又は公的機関に、異常又は攻撃の発生などの発生を知らせることができ、車外から異常又は攻撃に対して適切な対応を実施することも可能となる。

[0130] また、上記実施の形態では、車載ネットワーク２に接続されたゲートウェイＥＣＵ１０に本発明に係る技術が適用された例を説明した。車載ネットワーク２は、本発明に係る技術が適用される機器ネットワークの一例である。本発明に係る技術は、他の機器ネットワーク、例えば、ＦＡ（Factory Automation）システムを構成する１以上の産業機器が通信路を介して接続された産業機器ネットワーク、家庭用機器が接続されたホーム機器ネットワーク、又は事務用機器が接続された事務機器ネットワークなどに含まれるセキュリティ装置にも適用可能である。例えば、図１～図８を用いて説明した車載ネッ

トワーク２への適用例を、産業機器ネットワーク、ホーム機器ネットワーク、又は事務機器ネットワークに置き換えて適用することが可能である。

[0131] 上記のＦＡシステムには、例えば、各種物品の搬送システム、検査システム、ロボットを用いた組立システムなどが含まれる。また、これらＦＡシステムを構成する産業機器に搭載される制御機器には、例えば、プログラマブルコントローラ、モーション位置制御コントローラ、フィールドネットワーク機器、無線機器、センサ、アクチュエータ、ロボット、ＨＭＩ機器、及びデータ収集機器のうちの少なくとも１つが含まれてもよい。そして、ＦＡシステムに装備されるセキュリティ装置が上記した産業機器から取得する機器情報には、上記産業機器の運用フェーズである、立ち上げ中、通常稼動中、一時停止中、停止中、及びリプログラミング中のうちの少なくとも１つの運用フェーズに関する情報が含まれてもよい。また、ＦＡシステムにおいて各種の制御装置を接続する通信路は、有線でもよいし、無線でもよい。また、機器ネットワークにおける通信プロトコルはＣＡＮプロトコルに限定されない。前記通信プロトコルは、例えば、ＦＡシステムに用いられるＣＡＮＯｐｅｎ、又は他の派生的なプロトコルなどであってもよい。

産業上の利用可能性

[0132] 本発明は、車載機器、又は産業機器などの１以上の機器が通信路を介して接続された機器ネットワークに発生した攻撃に対するインシデント対応を実行するセキュリティ装置関連の産業分野において広く利用することができる。

[0133] ［付記］

本発明の実施の形態は、以下の付記の様にも記載され得るが、これらに限定されない。

（付記１）

１以上の機器（４、５、６、７、８）が通信路（３）を介して接続された機器ネットワーク（２）に含まれるセキュリティ装置（１０）であって、

前記機器ネットワーク（２）に発生した異常に基づいて特定又は推定され

た攻撃の情報（以下、攻撃情報という）を取得する攻撃情報取得部（２２）と、

前記機器の状態に関する情報（以下、機器情報という）を取得する機器情報取得部（２３）と、

前記攻撃の種類ごとに、インシデント対応と該対応による機能制限のレベルとが紐付けられた情報（以下、対応情報という）が記憶される対応情報記憶部（３１）と、

取得した前記攻撃情報と前記対応情報とに基づいて、前記攻撃情報に含まれる前記攻撃に対して実施すべき前記インシデント対応を決定する対応決定部（２４）と、

決定された前記インシデント対応を実施する対応実施部（２５）とを備え、

前記対応決定部（２４）が、

取得した前記攻撃情報に、一の通信路又は一の機器に対する２以上の前記攻撃が含まれている場合、これら攻撃の前記機能制限のレベルと、取得した前記機器情報とを考慮して、前記２以上の前記攻撃に対する前記インシデント対応の実施条件を決定するものであり、

前記対応実施部（２５）が、

決定された前記実施条件に基づいて、前記２以上の前記攻撃に対する前記インシデント対応を実施するものであることを特徴とするセキュリティ装置（１０）。

[0134] （付記２）

１以上の機器（４、５、６、７、８）が通信路（３）を介して接続された機器ネットワーク（２）に含まれる少なくとも１以上のコンピュータ（１２）が実行するインシデント対応処理方法であって、

前記機器ネットワーク（２）に発生した異常に基づいて特定又は推定された攻撃の情報（以下、攻撃情報という）を取得する攻撃情報取得ステップ（Ｓ１１）と、

前記機器の状態に関する情報（以下、機器情報という）を取得する機器情報取得ステップ（Ｓ１２）と、

取得した前記攻撃情報、及び前記攻撃の種類ごとに、インシデント対応と該対応による機能制限のレベルとを紐付けて記憶された情報（以下、対応情報という）に基づいて、前記攻撃情報に含まれる前記攻撃に対して実施すべき前記インシデント対応を決定する対応決定ステップ（Ｓ１４－Ｓ１５、Ｓ１７－Ｓ１９）と、

決定された前記インシデント対応を実施する対応実施ステップ（Ｓ１６、Ｓ２０）とを含み、

前記対応決定ステップが、

取得した前記攻撃情報に、一の通信路又は一の機器に対する２以上の前記攻撃が含まれている場合、これら攻撃の前記機能制限のレベルと、取得した前記機器情報とを考慮して、前記２以上の前記攻撃に対する前記インシデント対応の実施条件を決定するステップ（Ｓ１８）を含み、

前記対応実施ステップが、

決定された前記実施条件に基づいて、前記２以上の前記攻撃に対する前記インシデント対応を実施するステップ（Ｓ２０）を含むことを特徴とするインシデント対応処理方法。

符号の説明

[0135] １　車両

２　車載ネットワーク（機器ネットワーク）

３　バス

４　ＯＢＤII

５　走行系ＥＣＵ群

６　運転支援系ＥＣＵ群

７　ボディ系ＥＣＵ群

８　情報系ＥＣＵ群

１０　ゲートウェイＥＣＵ（セキュリティ装置）

１１　ゲートウェイ機能部

１２　セキュリティ制御部

２１　攻撃特定推定部

２２　攻撃情報取得部

２３　機器情報取得部

２４　対応決定部

２５　対応実施部

３１　対応情報記憶部

３２　実施条件記憶部

請求の範囲

[請求項1] １以上の機器が通信路を介して接続された機器ネットワークに含まれるセキュリティ装置であって、

前記機器ネットワークに発生した異常に基づいて特定又は推定された攻撃の情報（以下、攻撃情報という）を取得する攻撃情報取得部と、

前記機器の状態に関する情報（以下、機器情報という）を取得する機器情報取得部と、

前記攻撃の種類ごとに、インシデント対応と該対応による機能制限のレベルとが紐付けられた情報（以下、対応情報という）が記憶される対応情報記憶部と、

取得した前記攻撃情報と前記対応情報とに基づいて、前記攻撃情報に含まれる前記攻撃に対して実施すべき前記インシデント対応を決定する対応決定部と、

決定された前記インシデント対応を実施する対応実施部とを備え、

前記対応決定部が、

取得した前記攻撃情報に、一の前記通信路又は一の前記機器に対する２以上の前記攻撃が含まれている場合、これら攻撃の前記機能制限のレベルと、取得した前記機器情報とを考慮して、前記２以上の前記攻撃に対する前記インシデント対応の実施条件を決定するものであり、

前記対応実施部が、

決定された前記実施条件に基づいて、前記２以上の前記攻撃に対する前記インシデント対応を実施するものであることを特徴とするセキュリティ装置。

[請求項2] 前記攻撃の対象に含まれる前記通信路の種別と、前記機器情報と、前記実施条件との関係を示すテーブル情報が記憶される実施条件記憶部を備え、

前記対応決定部が、

取得した前記攻撃情報に、前記２以上の前記攻撃が含まれている場合、前記テーブル情報に基づいて、前記攻撃の対象となった前記一の前記通信路と、取得した前記機器情報とに対応する前記実施条件を決定するものであることを特徴とする請求項１記載のセキュリティ装置。

[請求項3] 前記実施条件には、前記機能制限のレベルの降順又は昇順に実施する条件が含まれていることを特徴とする請求項１又は請求項２記載のセキュリティ装置。

[請求項4] 前記実施条件には、前記機能制限のレベルが高い方又は低い方の前記攻撃に対する前記インシデント対応を実施する条件が含まれていることを特徴とする請求項１又は請求項２記載のセキュリティ装置。

[請求項5] 前記機器が、車両に搭載される制御装置であり、

前記機器ネットワークが、車載ネットワークであることを特徴とする請求項１又は請求項２記載のセキュリティ装置。

[請求項6] 前記制御装置には、

前記車両の走行系制御装置、運転支援系制御装置、ボディ系制御装置、情報系制御装置、及び診断用コネクタ装置のうちの少なくとも１つが含まれ、

前記機器情報には、手動運転中、運転支援中、リプログラミング中、及び駐車中のうちの少なくとも１つの車両状態に関する情報が含まれていることを特徴とする請求項５記載のセキュリティ装置。

[請求項7] 前記機器が、ＦＡ（Factory Automation）システムを構成する産業機器に搭載される制御機器であり、

前記機器ネットワークが、前記ＦＡシステムを構成する産業機器ネットワークであることを特徴とする請求項１又は請求項２記載のセキュリティ装置。

[請求項8] 前記制御機器には、

前記産業機器のプログラマブルコントローラ、フィールドネットワーク機器、無線機器、センサ、アクチュエータ、ロボット、ＨＭＩ（Human Machine Interface）機器、及びデータ収集機器のうちの少なくとも１つが含まれ、

前記機器情報には、前記産業機器の運用フェーズである、立ち上げ中、通常稼動中、一時停止中、停止中、及びリプログラミング中のうちの少なくとも１つの前記運用フェーズに関する情報が含まれていることを特徴とする請求項７記載のセキュリティ装置。

[請求項9] １以上の機器が通信路を介して接続された機器ネットワークに含まれる少なくとも１以上のコンピュータが実行するインシデント対応処理方法であって、

前記機器ネットワークに発生した異常に基づいて特定又は推定された攻撃の情報（以下、攻撃情報という）を取得する攻撃情報取得ステップと、

前記機器の状態に関する情報（以下、機器情報という）を取得する機器情報取得ステップと、

取得した前記攻撃情報、及び前記攻撃の種類ごとに、インシデント対応と該対応による機能制限のレベルとを紐付けて記憶された情報（以下、対応情報という）に基づいて、前記攻撃情報に含まれる前記攻撃に対して実施すべき前記インシデント対応を決定する対応決定ステップと、

決定された前記インシデント対応を実施する対応実施ステップとを含み、

前記対応決定ステップが、

取得した前記攻撃情報に、一の前記通信路又は一の前記機器に対する２以上の前記攻撃が含まれている場合、これら攻撃の前記機能制限のレベルと、取得した前記機器情報とを考慮して、前記２以上の前記攻撃に対する前記インシデント対応の実施条件を決定するステップを

含み、

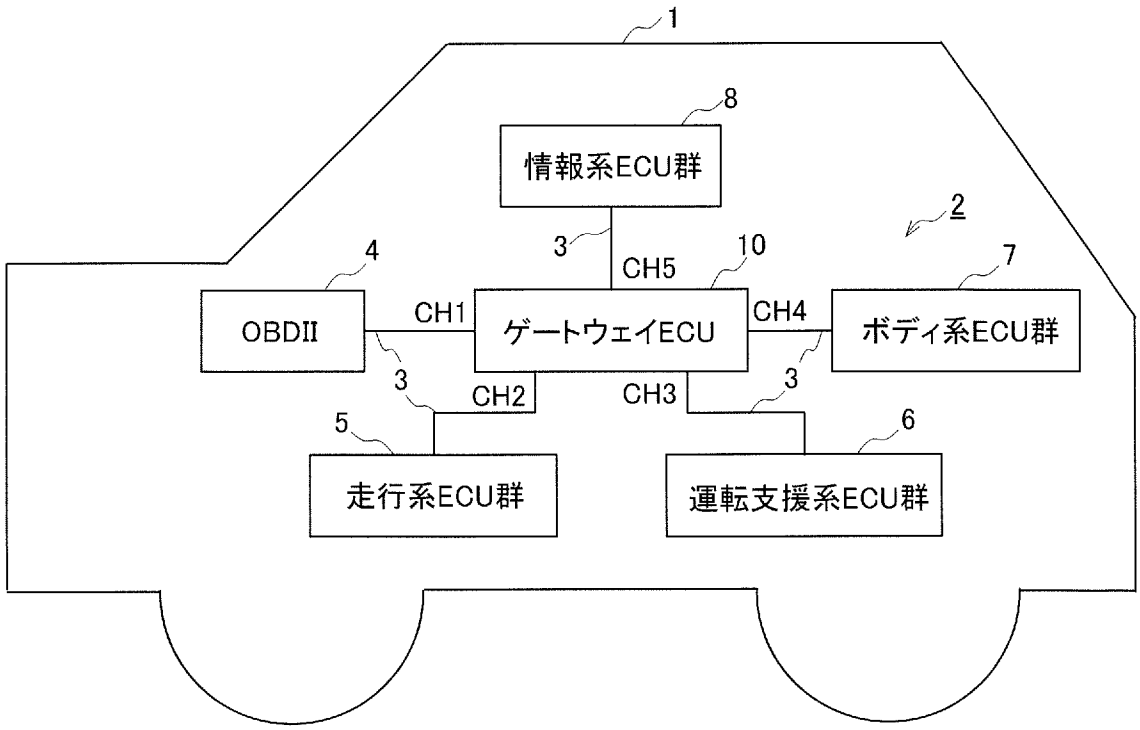
前記対応実施ステップが、

決定された前記実施条件に基づいて、前記２以上の前記攻撃に対する前記インシデント対応を実施するステップを含むことを特徴とするインシデント対応処理方法。

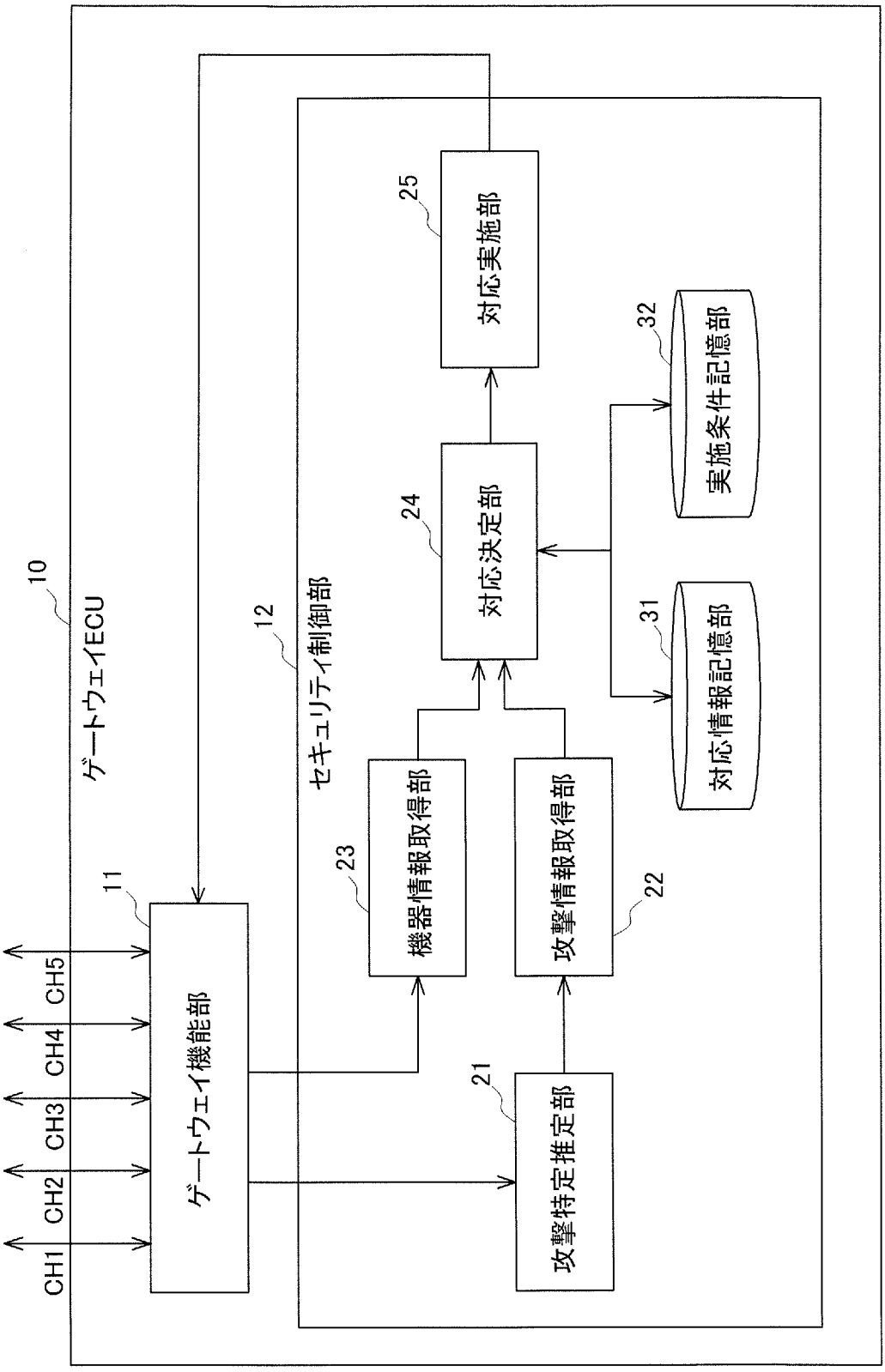
[請求項10] 請求項９記載のインシデント対応処理方法の各ステップを前記機器ネットワークに含まれる少なくとも１以上のコンピュータに実行させるためのプログラム。

[請求項11] 請求項９記載のインシデント対応処理方法の各ステップを前記機器ネットワークに含まれる少なくとも１以上のコンピュータに実行させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

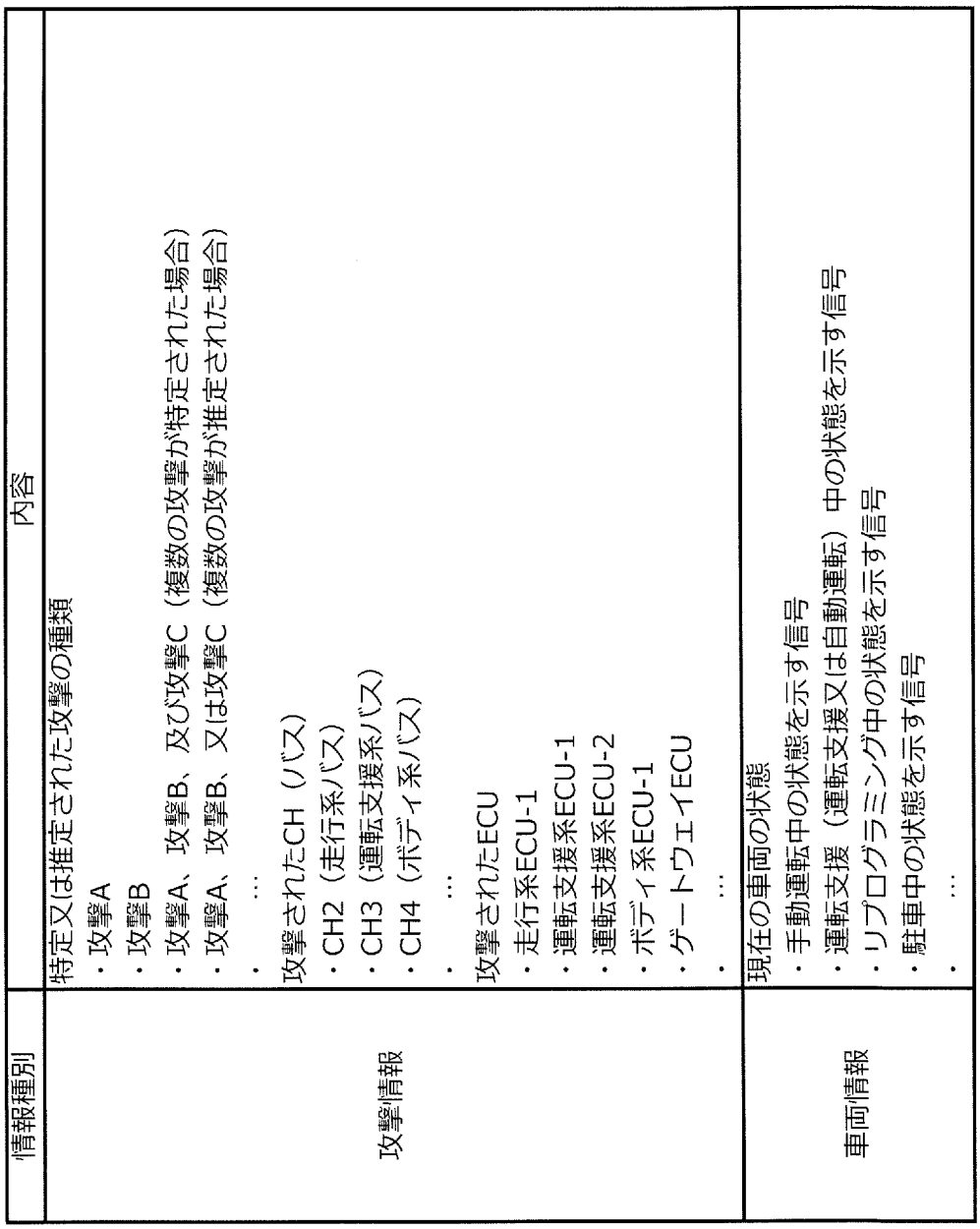
[図1]


1
8
情報系ECU群
2
3
CH5
10
4
7
OBDII
CH1
ゲートウェイECU
CH4
ボディ系ECU群
3
CH2
CH3
3
5
6
走行系ECU群
運転支援系ECU群

[図2]

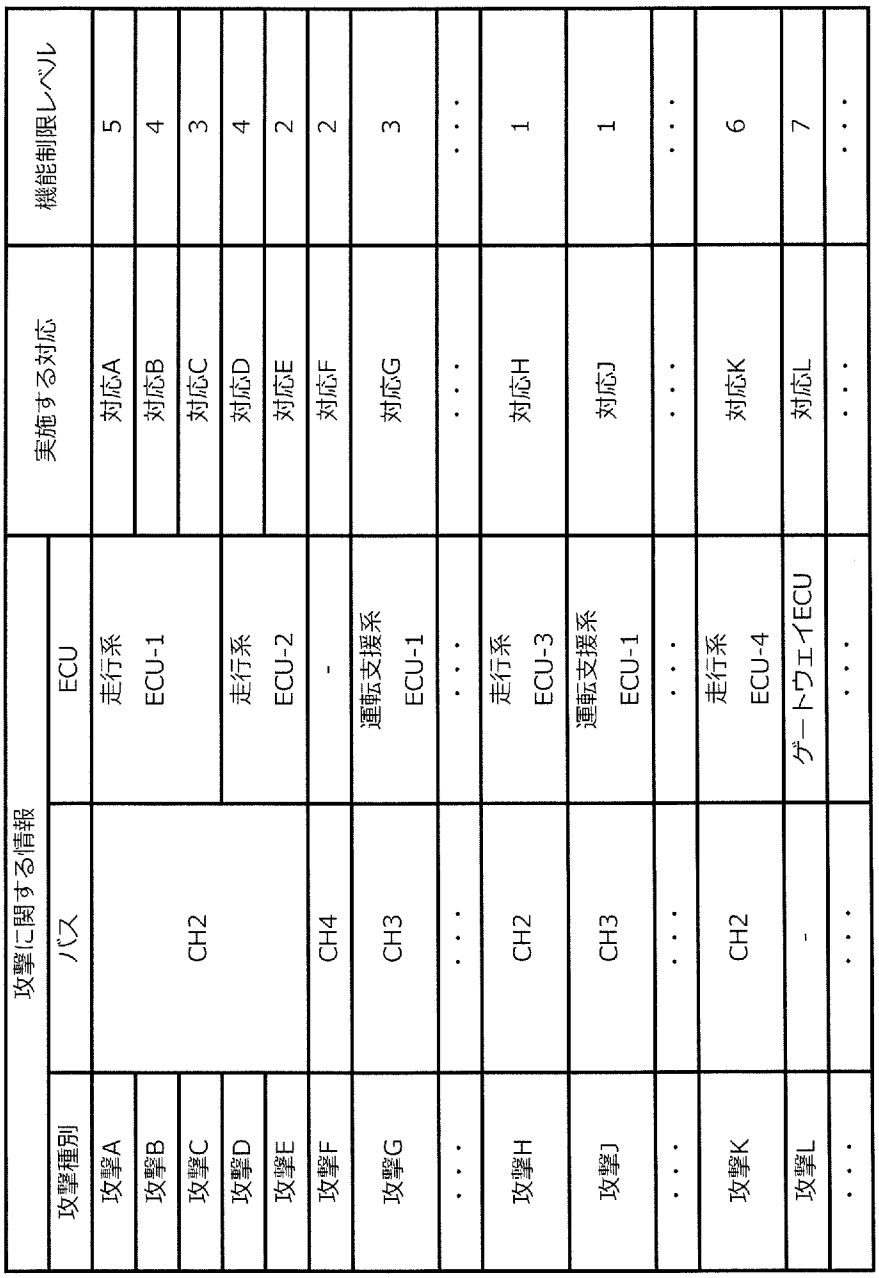

10
ゲートウェイECU
12
セキュリティ制御部
11
ゲートウェイ機能部
CH1
CH2
CH3
CH4
CH5
21
攻撃特定推定部
22
攻撃情報取得部
23
機器情報取得部
24
対応決定部
25
対応実施部
31
対応情報記憶部
32
実施条件記憶部

[図3]



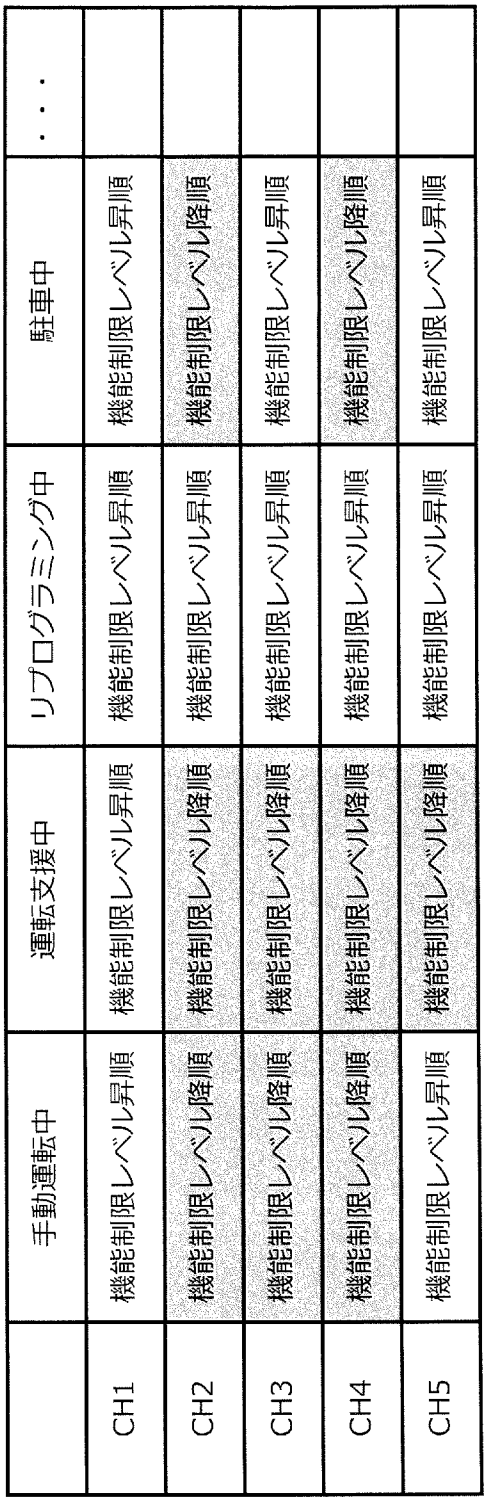
情報種別	内容
攻撃情報	特定又は推定された攻撃の種類 ・攻撃A ・攻撃B ・攻撃A、攻撃B、及び攻撃C（複数の攻撃が特定された場合） ・攻撃A、攻撃B、又は攻撃C（複数の攻撃が推定された場合） ・　… 攻撃されたCH（バス） ・CH2（走行系バス） ・CH3（運転支援系バス） ・CH4（ボディ系バス） ・　… 攻撃されたECU ・走行系ECU-1 ・運転支援系ECU-1 ・運転支援系ECU-2 ・ボディ系ECU-1 ・ゲートウェイECU ・　…
車両情報	現在の車両の状態 ・手動運転中の状態を示す信号 ・運転支援（運転支援又は自動運転）中の状態を示す信号 ・リプログラミング中の状態を示す信号 ・駐車中の状態を示す信号 ・　…

[図4]



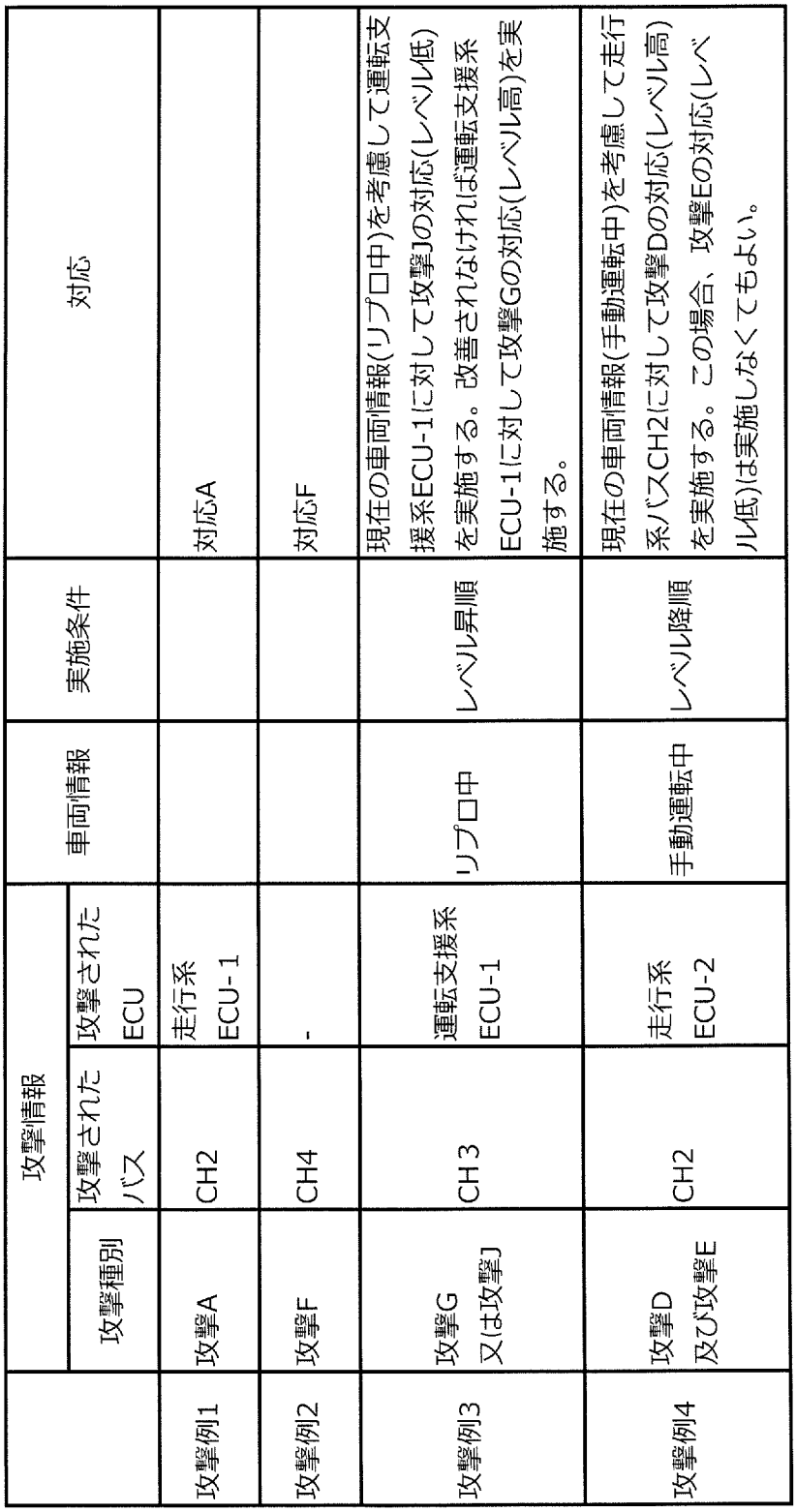
攻撃に関する情報			実施する対応	機能制限レベル
攻撃種別	バス	ECU		
攻撃A	CH2	走行系 ECU-1	対応A	5
攻撃B			対応B	4
攻撃C			対応C	3
攻撃D		走行系 ECU-2	対応D	4
攻撃E			対応E	2
攻撃F	CH4	-	対応F	2
攻撃G	CH3	運転支援系 ECU-1	対応G	3
・・・	・・・	・・・	・・・	・・・
攻撃H	CH2	走行系 ECU-3	対応H	1
攻撃J	CH3	運転支援系 ECU-1	対応J	1
・・・	・・・	・・・	・・・	・・・
攻撃K	CH2	走行系 ECU-4	対応K	6
攻撃L	-	ゲートウェイECU	対応L	7
・・・	・・・	・・・	・・・	・・・

[図5]



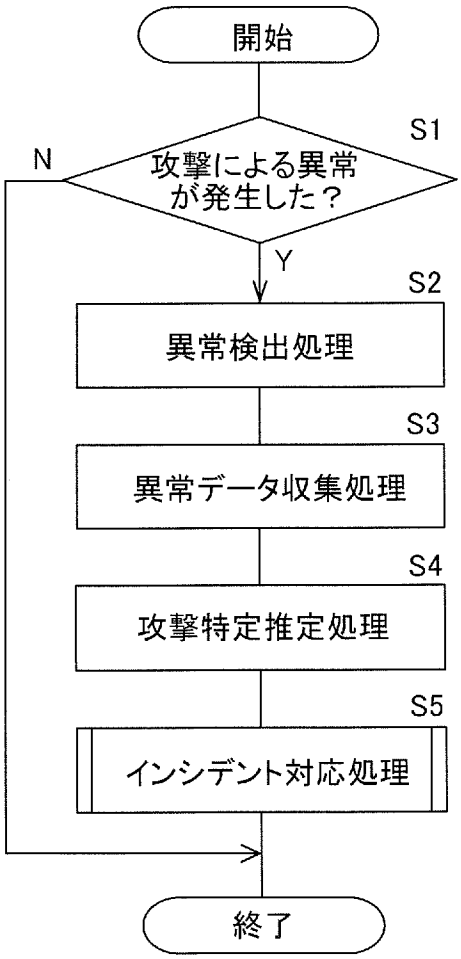
	手動運転中	運転支援中	リプログラミング中	駐車中	・・・
CH1	機能制限レベル昇順	機能制限レベル昇順	機能制限レベル昇順	機能制限レベル昇順	
CH2	機能制限レベル降順	機能制限レベル降順	機能制限レベル昇順	機能制限レベル降順	
CH3	機能制限レベル降順	機能制限レベル降順	機能制限レベル昇順	機能制限レベル昇順	
CH4	機能制限レベル降順	機能制限レベル降順	機能制限レベル昇順	機能制限レベル降順	
CH5	機能制限レベル昇順	機能制限レベル降順	機能制限レベル昇順	機能制限レベル昇順	

[図6]

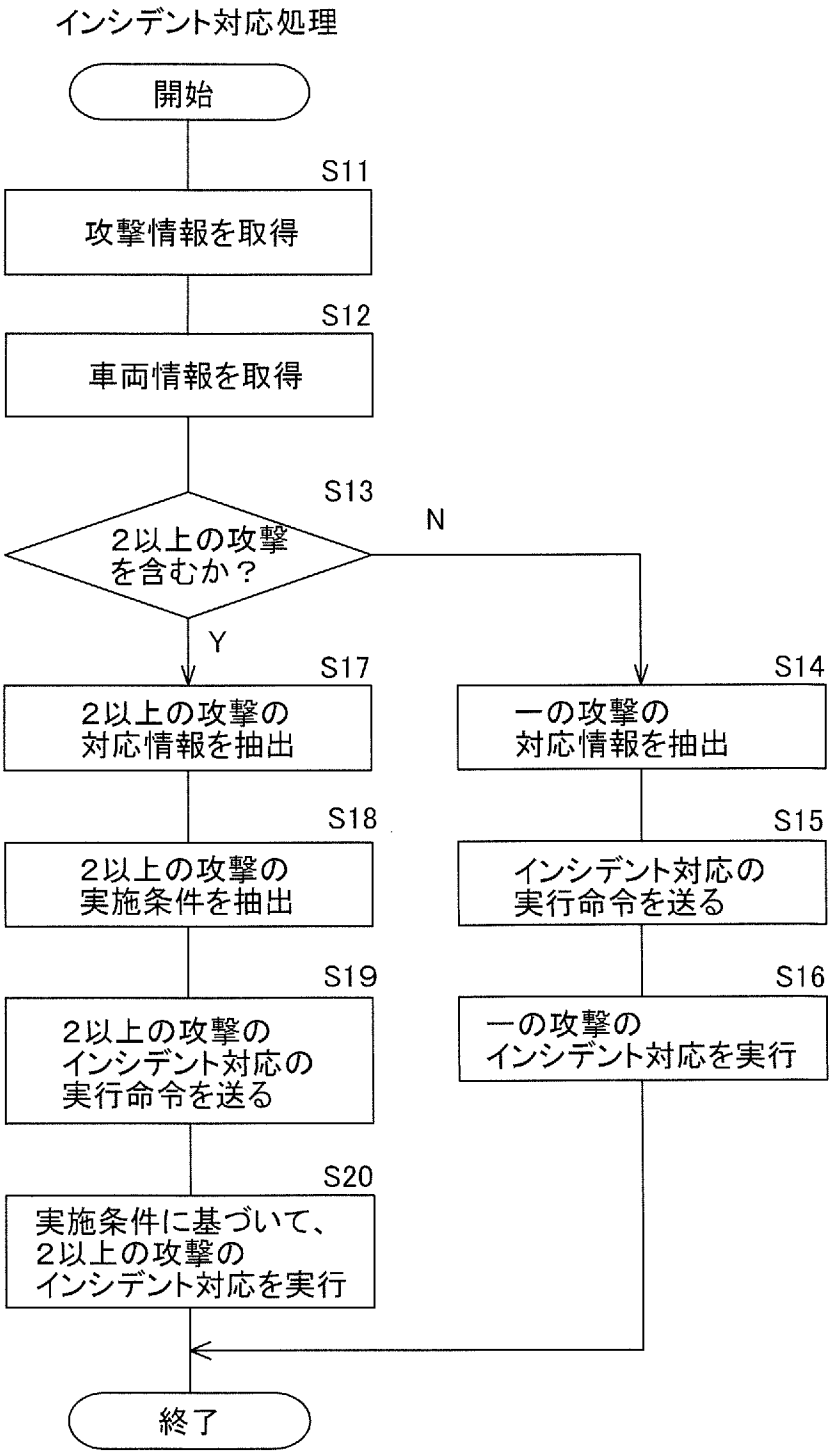


	攻撃情報			車両情報		実施条件	対応
	攻撃種別	攻撃されたバス	攻撃されたECU				
攻撃例1	攻撃A	CH2	走行系ECU-1				対応A
攻撃例2	攻撃F	CH4	-				対応F
攻撃例3	攻撃G又は攻撃J	CH3	運転支援系ECU-1	リプロ中		レベル昇順	現在の車両情報(リプロ中)を考慮して運転支援系ECU-1に対して攻撃Jの対応(レベル低)を実施する。改善されなければ運転支援系ECU-1に対して攻撃Gの対応(レベル高)を実施する。
攻撃例4	攻撃D及び攻撃E	CH2	走行系ECU-2	手動運転中		レベル降順	現在の車両情報(手動運転中)を考慮して走行系バスCH2に対して攻撃Dの対応(レベル高)を実施する。この場合、攻撃Eの対応(レベル低)は実施しなくてもよい。

[図7]


開始
S1
攻撃による異常が発生した？
N
Y
S2
異常検出処理
S3
異常データ収集処理
S4
攻撃特定推定処理
S5
インシデント対応処理
終了

[図8]


インシデント対応処理
開始
S11
攻撃情報を取得
S12
車両情報を取得
S13
2以上の攻撃を含むか？
N
Y
S17
2以上の攻撃の対応情報を抽出
S18
2以上の攻撃の実施条件を抽出
S19
2以上の攻撃のインシデント対応の実行命令を送る
S20
実施条件に基づいて、2以上の攻撃のインシデント対応を実行
S14
一の攻撃の対応情報を抽出
S15
インシデント対応の実行命令を送る
S16
一の攻撃のインシデント対応を実行
終了

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/029627

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. H04L12/46(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. H04L12/46

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.
Y	JP 2018-64293 A (PANASONIC INTELLECTUAL PROPERTY CORPORATION OF AMERICA) 19 April 2018, paragraphs [0015]-[0206] & US 2018/0316680 A1, paragraphs [0041]-[0211] & EP 3484106 A1, paragraphs [0015]-[0186]	1-11
Y	WO 2019/026310 A1 (MITSUBISHI ELECTRIC CORPORATION) 07 February 2019, paragraphs [0012]-[0051] (Family: none)	1-11

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 13.09.2019	Date of mailing of the international search report 15.10.2019
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/029627

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2017/183099 A1 (MITSUBISHI ELECTRIC CORPORATION) 26 October 2017, paragraphs [0036], [0037], fig. 4 & US 2019/0052674 A1, paragraphs [0068], [0069], fig. 4	1-11

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１９／０２９６２７

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L12/46(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.　H04L12/46

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
Y	JP 2018-64293 A（パナソニック　インテレクチュアル　プロパティ　コーポレーション　オブ　アメリカ）2018.04.19, 段落[0015]～[0206] & US 2018/0316680 A1,段落[0041]～[0211] & EP 3484106 A1, 段落[0015]～[0186]	1-11
Y	WO 2019/026310 A1（三菱電機株式会社）2019.02.07, 段落[0012]～[0051]（ファミリーなし）	1-11

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１３．０９．２０１９	１５．１０．２０１９

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｘ　４１８５
大石　博見
電話番号　０３－３５８１－１１０１　内線　３５９６

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
Y	WO 2017/183099 A1（三菱電機株式会社）2017.10.26, 段落[0036], [0037],Fig.4 & US 2019/0052674 A1,段落[0068],[0069],Fig.4	1-11