(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7月30日(30.07.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/153122 A1

(51) 国際特許分類:
B60R 16/02 (2006.01)　*G06F 21/55* (2013.01)

(21) 国際出願番号：　PCT/JP2020/000285

(22) 国際出願日：　2020年1月8日(08.01.2020)

(25) 国際出願の言語：　日本語

(26) 国際公開の言語：　日本語

(30) 優先権データ：
特願 2019-007916　2019年1月21日(21.01.2019)　JP

(71) 出願人: エヌ・ティ・ティ・コミュニケーションズ株式会社(**NTT COMMUNICATIONS CORPORATION**) [JP/JP]; 〒1008019 東京都千代田区大手町二丁目３番１号 Tokyo (JP).

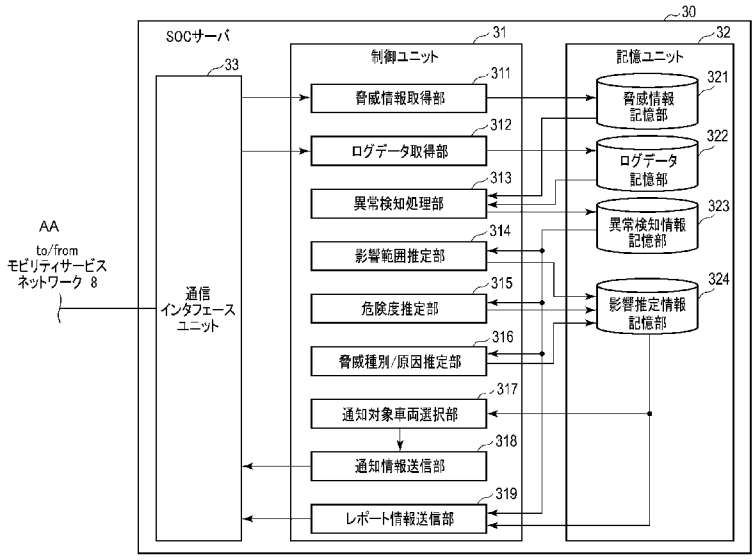
(72) 発明者: 上野 哲(**UENO, Satoshi**); 〒1008019 東京都千代田区大手町二丁目３番１号 エヌ・ティ・ティ・コミュニケーションズ株式会社内 Tokyo (JP). 小田 春樹(**ODA, Haruki**); 〒1008019 東京都千代田区大手町二丁目３番１号 エヌ・ティ・ティ・コミュニケーションズ株式会社内 Tokyo (JP). 若杉 厚司(**WAKASUGI, Atsushi**); 〒1008019 東京都千代田区大手町二丁目３番１号 エヌ・ティ・ティ・コミュニケーションズ株式会社内 Tokyo (JP).

(74) 代理人: 蔵田 昌俊, 外(**KURATA, Masatoshi** et al.); 〒1050014 東京都港区芝三丁目２３番１号 セレスティン芝三井ビルディング１１階 鈴榮特許綜合事務所内 Tokyo (JP).

WO 2020/153122 A1

(54) **Title:** VEHICLE SECURITY MONITORING DEVICE, METHOD, AND PROGRAM

(54) 発明の名称： 車両セキュリティ監視装置、方法及びプログラム



30 SOC server
31 Control unit
32 Storage unit
33 Communication interface unit
311 Threat information acquisition section
312 Log data acquisition section
313 Abnormality detection processing section
314 Influence range estimation section
315 Danger level estimation section
316 Threat type/cause estimation section
317 Notification target vehicle selection section
318 Notification information transmission section
319 Report information transmission section
321 Threat information storage section
322 Log data storage section
323 Abnormality detection information storage section
324 Influence estimation information storage section
AA to/from mobility service network 8

(57) **Abstract:** One aspect of this invention is a vehicle security monitoring device capable of communicating with an on-vehicle network having a function for transmitting log data relating to the operating state of an on-vehicle device. The vehicle security monitoring device acquires the log data, detects an abnormal state in the on-vehicle network on the basis of the acquired log data, estimates the range of influence of the detected abnormal state, and manages information indicating the estimated range of influence.

［続葉有］

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, 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, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, 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: この発明の一つの態様は、車載装置の動作状態に関するログデータを送信する機能を有する車載ネットワークとの間で通信が可能な車両セキュリティ監視装置にあって、前記ログデータを取得し、取得された前記ログデータに基づいて前記車載ネットワークにおける異常状態を検知する。そして、検知された前記異常状態が及ぼす影響の範囲を推定し、推定された前記影響の範囲を表す情報を管理する。

明　細　書

発明の名称 ： 車両セキュリティ監視装置、方法及びプログラム

技術分野

[0001] この発明の一態様は、例えば車両内に構築される車載ネットワークのセキュリティの状態を監視するための車両セキュリティ監視装置、方法およびプログラムに関する。

背景技術

[0002] 近年の自動車等の車両には、ナビゲーションシステムを構成する車載制御装置をはじめ、エンジンやブレーキ等の各種車載機器を電子的に制御する車載制御装置、車両の各種状態を表示するメータ等の機器を制御する車載制御装置などの多くの車載制御装置が搭載されている。そして、車両内では、それら各車載制御装置が通信線により電気的に接続されて車載ネットワークが形成されており、この車載ネットワークを介して各車載制御装置間で各種データの送受信が行われている。

[0003] 車載ネットワークは、当該ネットワークに接続される各車載制御装置が車両に搭載されるエンジンやブレーキ等の各種車載機器の制御を担っていることから、極めて高いセキュリティが要求される。しかし、こうした車載ネットワークは、外部のネットワークとは隔離されているのが一般的である。このため、例えばコントロール・エリア・ネットワーク（ＣＡＮ）等をはじめとする車載ネットワークは、同車載ネットワークで送受信されるデータが正規の車載制御装置から送信される正規のデータであることを前提に設計されている。

[0004] 一方で、最近このような車載ネットワークと外部のネットワークとの各種データの授受や、車両に設けられたデータ・リンク・コネクタ（ＤＬＣ）に接続された外部機器との各種データの授受を可能とするシステムの開発が進められている。この種のシステムを搭載した車両は一般にコネクテッドカーと呼ばれ、例えばナビゲーションシステムの地図データの更新や自動運転等

の高度なサービスを実現するために用いられている。

[0005] しかしながら、コネクテッドカーでは、車載ネットワークが外部のネットワークに接続可能となるため、外部のネットワークからマルウェアやウィルス等を用いたサイバー攻撃の脅威が指摘されている。サイバー攻撃を受けると、例えば不正な制御命令が実行されて車両が誤動作したり、車載制御装置のソフトウェアまたは制御データが改ざんされるおそれがある。

[0006] そこで、車載制御装置のソフトウェアまたは制御データ等の車内システムの改ざんや、それによる故障を検知する技術が種々検討されている（例えば特許文献１を参照）。

先行技術文献

特許文献

[0007] 特許文献1：日本国特開２０１８－０８１３４９号公報

発明の概要

発明が解決しようとする課題

[0008] ところが、従来検討されている技術は、車両ごとにサイバー攻撃によるシステム改ざんや故障を検知し、当該システム改ざんや故障が検知された車両のみに障害の発生等を通知するものが一般的である。

[0009] この発明は上記事情に着目してなされたもので、その一側面では、車載ネットワークから送信されるログデータに基づいてさらに効果的なセキュリティ対策の実行を可能にする技術を提供しようとするものである。

課題を解決するための手段

[0010] 上記課題を解決するためにこの発明に係る車両セキュリティ監視装置の一つの態様は、車載装置の動作状態に関するログデータを送信する機能を有する車載ネットワークとの間で通信が可能な車両セキュリティ監視装置にあって、前記ログデータを取得するログデータ取得部と、前記取得されたログデータに基づいて前記車載ネットワークにおける異常状態を検知する異常状態検知部と、前記検知された異常状態が及ぼす影響の範囲を推定する第１の推

定部と、前記推定された影響の範囲を表す情報を管理する推定情報管理部とを具備するようにしたものである。

発明の効果

[0011] この発明の第１の態様によれば、車両の車載ネットワークから送信されたログデータをもとに異常状態が検知され、当該異常状態が及ぼす影響の範囲が推定される。このため、異常状態が検知された車両のみならず、当該異常状態が影響を及ぼす範囲まで対策の対象を拡げることが可能となる。この結果、例えばサイバー攻撃により車両の車載ネットワークのプログラムが改ざんされた場合には、当該車両または車載ネットワークと関連する他の車両または車載ネットワークについても一括して対応処置を講じることが可能となる。

[0012] すなわち、この発明の各態様によれば、車載ネットワークから送信されるログデータに基づいてさらに効果的なセキュリティ対策の実行を可能にした技術を提供することができる。

図面の簡単な説明

[0013] [図1]図１は、この発明の一実施形態に係る車両セキュリティ監視装置を含む車両情報通信システムの全体構成を示すブロック図である。

[図2]図２は、この発明の一実施形態に係る車両セキュリティ監視装置として動作するＳＯＣサーバのハードウェア構成を示すブロック図である。

[図3]図３は、この発明の一実施形態に係る車両セキュリティ監視装置として動作するＳＯＣサーバのソフトウェア構成を示すブロック図である。

[図4]図４は、図２および図３に示したＳＯＣサーバによる制御手順と制御内容を示すフローチャートである。

[図5]図５は、脅威情報として定義される脅威の種別（インシデントの攻撃種別）と危険度の尺度（インシデントの危険度）との組み合わせの一例を示す図である。

[図6]図６は、分析レポートの一例を示す図である。

発明を実施するための形態

[0014] 以下、図面を参照してこの発明に係わる実施形態を説明する。

［一実施形態］

（構成）

（１）システム

図１は、この発明の一実施形態に係る車両セキュリティ監視装置を備えたシステムの全体構成を示す図である。

一実施形態に係る車両セキュリティ管理システムは、例えば中核としてモビリティサービスネットワーク８を有する。モビリティサービスネットワーク８には、モビリティサービスサーバ２０、セキュリティ・オペレーション・センタ（Security Operation Center：ＳＯＣ）サーバ３０、およびＰＳＩＲＴ（Product Security Incident Response Team）サーバ４０が接続されている。

[0015] またモビリティサービスネットワーク８は、車両１に搭載された車載ネットワーク２との間で、移動通信ネットワーク７を介して通信が可能となっている。さらにモビリティサービスネットワーク８は、インターネット９を介して外部サーバ５０との間でも通信が可能となっている。

[0016] なお、移動通信ネットワーク７とモビリティサービスネットワーク８との間、およびモビリティサービスネットワーク８とインターネット９との間は、それぞれネットワーク間接続装置としての例えばゲートウェイ８１，８２を介して接続される。また、移動通信ネットワーク７としては、例えばセルラ移動通信ネットワークや無線ＬＡＮ（Local Area Network）が用いられる。

[0017] 車載ネットワーク２は、例えばＣＡＮ（Control Area Network）と呼称され、複数の車載電子制御装置（Electric Control Unit：ＥＣＵ）を有している。ＥＣＵは、それぞれがプロセッサにプログラムを実行させることにより所定の制御機能を果たすように構成される。例えば、ＥＣＵはエンジンやトランスミッション、操舵角、アクセル、ブレーキ等を制御する装置、ウィンカーやライト、ワイパーを制御する装置、ドアロックおよび窓の開閉を制御

する装置、空調を制御する装置等として用いられる。

[0018] また、車両１には、速度センサや温度センサ、振動センサ等の車両の動作状態に係る各種車両センサの計測データをはじめ、ドライバの状態を監視する車内センサ、車外の状況を監視する車外センサ等の多くのセンサが設けられている。ＥＣＵは、これらのセンサから出力されるセンシングデータを取り込む装置としても用いられる。ＥＣＵは、さらに自動運転制御装置やドライバの状態を監視する装置としても用いられる。

[0019] また車載ネットワーク２には、通信制御ユニット（ＴＣＵ）３およびナビゲーション装置４が接続されている。ＴＣＵ３は、車載ネットワーク２と移動通信ネットワーク７との間でデータの送受信を行うために用いられる。例えば、ＴＣＵ３はドライバの通話データを送受信したり、Ｗｅｂサイトからナビゲーションデータを受信したり、上記ＥＣＵの動作状態を表すログデータをＳＯＣサーバ３０へ送信するために用いられる。

[0020] ナビゲーション装置４は、ＵＳＢポートおよび無線インタフェースを有している。そして、ＵＳＢポートを介してＵＳＢメモリ５との間でデータの書き込みおよび読み出しを行うと共に、無線インタフェースを介してスマートフォン等の携帯端末６との間のデータの送受信や外部との間のデータの送受信を行う機能を有している。なお、無線インタフェースとしては、例えばBluetooth（登録商標）又はWiFi（登録商標）を使用するものが用いられる。

[0021] なお、車載ネットワーク２は、外部インタフェースポート（ＯＢＤ－２）を有している。このＯＢＤ－２には、試験装置やパーソナルコンピュータが接続可能である。試験装置やパーソナルコンピュータは、例えばＥＣＵの試験を行ったり、ＥＣＵに対し更新プログラムや制御データをインストールするために使用される。

[0022] 外部サーバ５０は、例えばＡｕｔｏ－ＩＳＡＣ（Automotive Information Sharing and Analysis Center）が運用管理する。外部サーバ５０は、例えば、コネクテッドカー関連のサイバー脅威や潜在的な脆弱性に関する脅威情報を蓄積するデータベースを備える。そして、当該データベースに蓄積された

情報をＳＯＣサーバ３０に提供する。

[0023] ＰＳＩＲＴサーバ４０は、例えば、車両メーカ又は車載装置の開発ライフサイクルを通じて必要な安全管理、サポート、インシデント対応を実施するための組織（ＰＳＩＲＴ）が運用する。ＰＳＩＲＴサーバ４０は、例えば、当該メーカ固有のサイバー脅威情報を記憶する脅威情報データベースを備える。そして、ＳＯＣサーバ３０からの要求に応じて脅威情報をＳＯＣサーバ３０へ送信する。またＰＳＩＲＴサーバ４０は、例えば、メーカ別に決定された対応方針等がＰＳＩＲＴの管理者により入力された場合に、当該対応方針等を含むリコール指示を該当車両に向けて送信する機能を有する。上記対応方針等は、ＳＯＣサーバ３０から提供されるセキュリティに対する分析レポートをもとに入力される。なお、脅威情報は、例えば脅威の種別と危険度の尺度との組み合わせにより定義される。分析レポートも、例えば上記脅威の種別と危険度の尺度との組み合わせを用いて記述される。

[0024] （２）ＳＯＣサーバ

図２および図３は、それぞれ上記ＳＯＣサーバ３０のハードウェア構成およびソフトウェア構成を示すブロック図である。

ＳＯＣサーバ３０は、例えば車両セキュリティ監視装置として動作するもので、クラウドサーバやＷｅｂサーバにより構成される。ＳＯＣサーバ３０は、制御ユニット３１と、記憶ユニット３２と、通信Ｉ/Ｆ（通信Ｉ/Ｆ）３３とを備える。これらはバス３４を介して相互に接続される。

[0025] 通信Ｉ／Ｆ３３は、モビリティサービスネットワーク８およびインターネット９で使用される通信プロトコルに従い、車載ネットワーク２、外部サーバ５０およびＰＳＩＲＴサーバ４０との間で、それぞれ各種データの伝送を行う。

[0026] 記憶ユニット３２は、例えば、ＨＤＤ（Hard Disk Drive）またはSolid State Drive（ＳＳＤ）等の随時書込みおよび読出しが可能な不揮発性メモリと、ＲＯＭ（Read Only Memory）およびＲＡＭ（Random Access Memory）とを組み合わせて構成される記憶媒体を備えたもので、プログラム記憶領域とデ

ータ記憶領域とを有する。なお、記憶媒体の構成は上記構成に限るものではない。プログラム記憶領域には、ＯＳ（Operating System）等のミドルウェアに加えて、この発明の一実施形態に係る各種制御処理を実行するために必要なプログラムが格納されている。

[0027] データ記憶領域には、脅威情報記憶部３２１と、ログデータ記憶部３２２と、異常検知情報記憶部３２３と、影響推定情報記憶部３２４が設けられている。

[0028] 脅威情報記憶部３２１は、外部サーバ５０およびＰＳＩＲＴサーバ４０から取得された脅威情報を蓄積するために使用される。ログデータ記憶部３２２は、車載ネットワーク２から送信されたログデータを蓄積するために使用される。異常検知情報記憶部３２３は、制御ユニット３１の異常検知処理により得られた車載ネットワーク２の異常検知情報を記憶するために使用される。影響推定情報記憶部３２４は、制御ユニット３１により得られた、上記異常の影響に関する複数の推定結果を表す情報を記憶するために使用される。

[0029] 制御ユニット３１は、例えば、ＣＰＵ（Central Processing Unit）等のハードウェアプロセッサを備える。制御ユニット３１は、この発明の一実施形態を実現するための制御機能として、脅威情報取得部３１１と、ログデータ取得部３１２と、異常検知処理部３１３と、影響範囲推定部３１４と、危険度推定部３１５と、脅威種別／原因推定部３１６と、通知対象車両選択部３１７と、通知情報送信部３１８と、レポート情報送信部３１９とを有している。これらの制御機能部は、いずれも上記記憶ユニット３２のプログラム記憶領域に格納されたプログラムを上記ハードウェアプロセッサに実行させることにより実現される。

[0030] 脅威情報取得部３１１は、外部サーバ５０およびＰＳＩＲＴサーバ４０から、モビリティサービスネットワーク８を介して、車載ネットワーク２にとっての脅威情報を取得する。そして、取得された脅威情報を脅威情報記憶部３２１に記憶させる処理を行う。脅威情報には、例えば、サイバー攻撃に対

する車載ネットワーク２の脆弱性の種類とその弱さを表す情報や、事故を引き起こす可能性がある異常動作の種類とその重要度を表す情報が含まれる。なお、脅威情報の取得は、モビリティサービスネットワーク８を介さず、インターネット９等の他のネットワークを介して行われてもよい。

[0031] ログデータ取得部３１２は、車載ネットワーク２から送信されるログデータを、移動通信ネットワーク７およびモビリティサービスネットワーク８を介して取得する。そして、取得されたログデータをログデータ記憶部３２２に記憶させる処理を行う。また、ログデータの取得についても、モビリティサービスネットワーク８を介さず、インターネット９等の他のネットワークを介して行われてもよい。

[0032] ログデータには、例えば、車載ネットワーク２内のＥＣＵにおけるプログラムや制御データの変更履歴や、各ＥＣＵによる車載機器および車載装置の動作履歴、外部ネットワークから各種制御データ又はコンテンツデータを受信したときの当該受信データの通信経路を表す情報が含まれる。また、ログデータには、送信元を識別する情報と、ログデータ発生元となるＥＣＵ、車両機器または車載装置の識別番号と、車両１に予め割り当てられたネットワークアドレスと、ログデータの発生日時を表すタイムスタンプおよび車両１の現在位置を表す位置情報がヘッダとして付与される。位置情報は、例えばカーナビゲーションシステムに備えられているＧＰＳ（Global Positioning System）受信機により取得できる。

[0033] 異常検知処理部３１３は、上記ログデータ取得部３１２により取得されたログデータと脅威情報記憶部３２１に記憶された脅威情報との相関を求めることで、ログデータの内容が脅威に相当するものか否かを判定する。そして、脅威に相当すると判定された場合に、その脅威に対応する異常の種類および上記相関の度合いを表す情報を、上記対象となったログデータと共に異常検知情報として異常検知情報記憶部３２３に記憶させる処理を行う。

[0034] 影響範囲推定部３１４は、上記異常検知情報記憶部３２３に記憶された異常検知情報の内容に基づいて異常状態が及ぼす影響の範囲を推定し、その推

定結果を表す情報を影響推定情報記憶部３２４に記憶させる処理を行う。影響範囲の推定対象としては、例えば、車両のメーカ、車種、年式、地域、ＥＣＵ、および車載ネットワーク２内の部位が想定される。

[0035] 危険度推定部３１５は、上記異常検知情報記憶部３２３に記憶された異常検知情報に含まれる異常動作の種類と脅威情報との相関をとることで、異常動作が及ぼす危険の度合い（危険度）を推定する。そして、その推定結果を表す情報を影響推定情報記憶部３２４に記憶させる処理を行う。危険度は、例えば、異常動作が車両又はドライバに及ぼす危険の度合いを示すもので、例えば“Information”、“Medium”、“Serious”、“Critical”の４段階で判定できる。

[0036] 脅威種別／原因推定部３１６は、上記異常状態が検知されたログデータに付与されている情報もとに、異常状態（インシデント）の攻撃種別を推定する。また脅威種別／原因推定部３１６は、マルウェアやウィルス等によるサイバー攻撃を受けた場合に、このとき受信した伝送データの通信経路情報から送信経路および送信元を推定する。そして、これらの推定結果をもとに異常状態の脅威種別又は発生要因もしくはその両方を表す情報を生成し、影響推定情報記憶部３２４に記憶させる処理を行う。

[0037] 通知対象車両選択部３１７は、上記影響推定情報記憶部３２４に記憶された影響範囲、危険度および脅威種別又は発生要因もしくはその両方の推定結果を表す情報に基づいて、異常対応の対象となる車両群を選択する。そして、選択された車両群に対し異常対応通知情報を送信する処理を行う。異常対応の対象となる車両群としては、例えば、メーカ、車種、形式のいずれかに該当する車両、或いは特定地域で使用されている車両等が挙げられる。

[0038] 通知情報送信部３１８は、上記通知対象車両選択部３１７により選択された車両群を宛先として、上記異常対応通知情報を通信Ｉ／Ｆ３３からモビリティサービスネットワーク８へ送信する処理を行う。

[0039] レポート情報送信部３１９は、上記影響推定情報記憶部３２４に記憶された影響範囲、危険度および脅威種別又は発生要因それぞれの推定結果を表す

情報と、異常検知情報記憶部３２３に記憶された異常検知情報とを含む車両セキュリティ用の分析レポートを作成する。そして、作成された分析レポートの情報を通信Ｉ／Ｆ３３からＰＳＩＲＴサーバ４０へ送信する処理を行う。

[0040] （動作）

次に、以上のように構成されたＳＯＣサーバ３０の動作例を、車載ネットワーク２の動作例と共に説明する。図４はその制御手順と制御内容の一例を示すフローチャートである。

[0041] （１）脅威情報の取得

ＳＯＣサーバ３０は、脅威情報取得部３１１の制御の下、ステップＳ２０において、外部サーバ５０およびＰＳＩＲＴサーバ４０から、定期的又は任意のタイミングで、コネクテッドカー関連のサイバー脅威や潜在的な脆弱性を定義した情報を取得する。具体的には、脅威種別と危険度の尺度とで定義される情報を取得する。そして、取得された情報を脅威情報として脅威情報記憶部３２１に記憶させる。なお、上記脅威情報の取得処理は、ＳＯＣサーバ３０から外部サーバ５０等にアクセスして取得する方式でも、外部サーバ５０等が定期的又は不定期にプッシュ方式で送信する脅威情報をＳＯＣサーバ３０が受信する方式であってもよい。

[0042] （２）ログデータの取得

各車両１の車載ネットワーク２は、各ＥＣＵおよび車両機器または装置が自身の動作状態等を常時又は定期的に監視している。そして、その監視結果に基づいて動作履歴を表すログデータを生成している。また、外部ネットワークから送信された伝送データを車載ネットワーク２が受信した場合にも、当該伝送データの受信履歴を表すログデータを生成している。

[0043] また車載ネットワーク２は、上記生成されたログデータをステップＳ１０により収集して内部メモリに一旦記憶する。そして車載ネットワーク２は、上記記憶されたログデータを、ステップＳ１１で一定期間が経過するごとに読み出す。そして、読み出されたログデータを、ステップＳ１２においてＴ

ＣＵ３からＳＯＣサーバ３０に向け送信する。なお、上記ログデータは、一定時間分まとめずに、生成されるごとにリアルタイムで送信されるようにしてもよい。

[0044] これに対しＳＯＣサーバ３０は、ログデータ取得部３１２の制御の下、ステップＳ２１によりログデータの受信を監視している。この状態で、通信Ｉ／Ｆ３１によりログデータが受信されると、ログデータ取得部３１２がステップＳ２２により、上記受信されたログデータを取り込んでログデータ記憶部３２２に記憶させる。ログデータ取得部３１２は、ログデータが受信されるごとに上記処理を繰り返す。

[0045] （３）異常検知処理

ＳＯＣサーバ３０は、新たなログデータが取得されるごとに、異常検知処理部３１３の制御の下、ステップＳ２２において、上記新たに取得されたログデータをログデータ記憶部３２２から読み込む。そして、当該ログデータに含まれる動作内容等を表す情報と、脅威情報記憶部３２１に記憶された複数の脅威情報との相関値をそれぞれ演算する。そして、相関値が閾値以上となるログデータを異常検知情報として異常検知情報記憶部３２３に記憶させる。

[0046] 例えば、サイバー攻撃によるプログラムまたは制御データの改ざんやプログラムのバグ等による不自然な挙動を定義する脅威情報として、「晴天時のワイパーの連続動作」、「ヘッドライトの連続的な点滅」、「エンジンの異常な高回転動作」といった検知ロジックが定義されている。異常検知処理部３１３は、車載ネットワーク２から送られたログデータの内容が上記検知ロジックのいずれかと一致すると、上記ログデータを異常状態を含むログデータとして抽出し、これを異常検知情報として異常検知情報記憶部３２３に記憶させる。

[0047] （４）異常状態が及ぼす影響範囲の推定

ＳＯＣサーバ３０は、異常状態を含むログデータが検出されたことをステップＳ２４で判定すると、先ず影響範囲推定部３１４の制御の下、ステップ

Ｓ２５により上記異常動作が及ぼす影響の範囲を推定する。

[0048] 例えば、異常状態が「晴天時のワイパーの連続動作」、「ヘッドライトの連続的な点滅」、「エンジンの異常な高回転動作」だったとし、当該異常状態が一定の期間中に複数台の車両から通知されたとする。この場合影響範囲推定部３１４は、検知された上記複数台の車両の車両識別番号又は車台番号をログデータから抽出して、例えば車両のメーカ名、車種、年式の共通性を判定する。そして、その判定結果をもとに、上記異常動作の影響範囲が特定の「メーカ」であるか、特定の「車種」であるか、或いは特定の「年式」であるのかを推定し、その推定結果を対象ログデータと共に影響推定情報記憶部３２４に記憶させる。なお、上記車両メーカ以外に、車両の販売者や、車載ネットワーク２のメーカまたは販売者を影響範囲として推定するようにしてもよい。

[0049] また、例えば、異常状態が「寒冷地仕様の車載装置」で発生した場合には、影響範囲を「寒冷地域」と推定する。そして、その推定結果を対象ログデータと共に影響推定情報記憶部３２４に記憶させる。

[0050] さらに、例えば、動作異常を示すログデータを発生したＥＣＵ、車載機器または装置と同一のバス上に接続されている他のＥＣＵ、車載機器または装置を、上記異常動作が及ぼす影響の範囲として推定する。そして、その推定結果を対象ログデータと共に影響推定情報記憶部３２４に記憶させる。

[0051] （５）異常状態が及ぼす危険の度合い

次にＳＯＣサーバ３０は、危険度推定部３１５の制御の下、ステップＳ２６において、上記異常動作が及ぼす危険の度合い（危険度）を推定する。この危険度の推定は、異常検知情報に含まれる異常動作の種類と、当該異常動作と脅威情報との相関値に基づいて、推定される。

[0052] 例えば、異常状態の種類が、エンジンやトランスミッション等のパワーユニットに係るものの場合や、マルウェアやウィルス等のサイバー攻撃による車載ネットワーク２の乗っ取りが疑われるものの場合には、車両１又はドライバに及ぼす危険の度合いが高いと推定される。一方、異常状態の種類が空

調装置に関するものの場合には、車両１又はドライバに及ぼす危険の度合いは低いと推定される。具体的には、インシデントの危険度は、図５に例示したように“Information”、“Medium”、“Serious”、“Critical”の４段階で判定される。

[0053] そして危険度推定部３１５は、以上のように推定された上記危険度の推定結果を表す情報を、推定の対象となったログデータと共に、影響推定情報記憶部３２４に記憶させる。

[0054] （６）異常状態の脅威種別／発生要因の推定

続いてＳＯＣサーバ３０は、脅威種別／原因推定部３１６の制御の下、ステップＳ２７において、異常状態の脅威種別又は発生要因もしくはその両方を推定する処理を行う。例えば、異常状態が検知されたログデータに付与されているログ発生元を示す情報もとに、異常状態の発生場所がＥＣＵ、車載機器、車載装置のいずれであるかを推定する。また、例えばマルウェアやウィルス等によるサイバー攻撃を受けた場合には、当該サイバー攻撃に係る伝送データの通信経路情報を解析することにより攻撃元とその通信経路を表す情報、例えば地域、ＩＤ、ドメインを推定する。そして、これらの推定結果をもとに、異常状態の脅威種別（インシデントの攻撃種別）又は発生要因もしくはその両方を表す情報を生成し、影響推定情報記憶部３２４に記憶させる。インシデントの攻撃種別としては、例えば図４に例示したように、「不正アクセス」、「ＤｏＳ攻撃」、「マルウェア」、「不自然な通信」、「調査行為」および「その他」の６種類が定義される。

[0055] なお、脅威種別／原因推定部３１６の処理内容としては、異常発生場所又はサイバー攻撃元を推定するだけでなく、ログデータの内容を解析して異常状態の脅威種別又は発生要因を推定するようにしてもよい。例えば、振動センサにより検出された波形の特徴や温度センサにより検出された温度変化の特徴を抽出し、抽出された特徴データを学習モデルに入力することで、異常状態の脅威種別又は発生要因もしくはその両方を推定する。

[0056] （７）通知対象車両の選択と対応情報の通知

上記影響範囲、危険度および脅威種別／原因の各推定処理が終了すると、ＳＯＣサーバ３０は、通知対象車両選択部３１７の制御の下、ステップＳ２８において、上記影響推定情報記憶部３２４に記憶された影響範囲、危険度および脅威種別又は発生要因の各推定結果を表す情報に基づいて、対応情報の通知対象車両を選択する。

[0057] 例えば、影響範囲の推定結果が「メーカ」、「車種」、「年式」の場合には、ＰＳＩＲＴサーバ４０又は外部サーバ５０から、メーカ別、車種別、年式別の車両所有者の登録情報を取得し、取得した登録情報をもとに「メーカ」、「車種」、「年式」に該当する車両の所有者を抽出する。そして、通知情報送信部３１８の制御の下、ステップＳ２９において、上記危険度および脅威種別又は発生要因もしくはその両方の推定結果に基づいて異常に対する対応指示を生成する。そして、生成された上記対応指示を含む通知情報を、上記抽出された所有者のリストをもとに、当該各所有者の車両に向けてそれぞれ送信する。

[0058] また通知情報送信部３１８は、影響範囲の推定結果が「地域」の場合には、当該地域に存在する車両をログデータに付与されている車両の位置情報をもとに抽出する。そして、上記危険度および脅威種別又は発生要因もしくはその両方の推定結果に基づいて異常状態に対する対応指示を生成し、当該対応指示を含む通知情報を、上記地域内に存在する車両に向け送信する。

[0059] さらに通知情報送信部３１８は、危険度に応じて、対応指示を送信する際の優先順位を設定する。例えば、同一時間帯に複数の車載ネットワーク２においてそれぞれ異常状態が検知された場合に、それぞれの異常状態が及ぼす危険度が高いものから順に優先度を設定し、当該優先度に従い対応指示を含む通知情報を送信する。この結果、例えば、パワーユニットの異常や、車載ネットワーク２の乗っ取りが疑われる異常が発生した車両に対しては、空調機やパワーウィンドウの異常、ナビゲーションシステムの異常が発生した車両に比べて、高い優先度で対応指示を含む通知情報が送信される。上記対応指示を含む通知情報は、モビリティサービスネットワーク８および移動通信

ネットワーク７を介して、通知対象の各車両にそれぞれ伝送される。

[0060] 上記通知情報を受信した車両の車載ネットワーク２は、図４に示すステップＳ１３により上記通知情報の受信を検出すると、ステップＳ１４において、上記通知情報に含まれる対応指示に応じて車載ネットワーク２の復旧処理を実行する。例えば、対応指示に応じて動作異常が検知されたＥＣＵのプログラムや制御データを修復したり、車載機器または装置の動作状態をリセットする。

[0061] （８）分析レポートの作成および送信

さらにＳＯＣサーバ３０は、レポート情報送信部３１９の制御の下、ステップＳ３０において、上記影響推定情報記憶部３２４に記憶された影響範囲、危険度および脅威種別又は発生要因もしくはその両方それぞれの推定結果を表す情報と、異常検知情報記憶部３２３に記憶された異常検知情報とを含む分析レポートを作成する。そして、作成した分析レポートを該当するメーカのＰＳＩＲＴサーバ４０に向け送信する。

[0062] 分析レポートには、例えば、推定された脅威種別（インシデントの攻撃種別）又は発生要因もしくはその両方、インシデントの危険度および推奨される対応内容を表すメッセージが記載される。図５は、脅威種別（インシデントの攻撃種別）と危険度の尺度（インシデントの危険度）との組み合わせの一例を示したもので、この例では１２通りの組み合わせが定義されている。図６は分析レポートの一例を示すもので、“Severity”の欄にインシデントの危険度が記載され、“Category”の欄にインシデントの攻撃種別が記載される。また、“Recommendation/Action”の欄には、攻撃に対し推奨される対応メッセージが記載される。

[0063] メーカは、上記分析レポートに基づいて、例えば該当車両に対する恒久的な回復手段を検討してその対策指示を該当車両に送信したり、場合によってはリコールを検討することができる。また、以後開発する車両に搭載する車載ネットワーク２の設計にも反映することができる。

[0064] （効果）

以上詳述したように一実施形態では、ＳＯＣサーバ３０において、車載ネットワーク２から送信されるログデータを取得し、取得されたログデータと脅威情報との相関を求めることで異常動作を表すログデータを検知する。そして、上記異常の検知情報に基づいて上記異常が及ぼす影響の範囲、危険の度合いおよび異常の脅威種別又は発生要因もしくはその両方をそれぞれ推定し、これらの推定結果に基づいて対応指示の通知対象となる車両を選択して、選択した車両に対し対応指示を送信するようにしている。

[0065] 従って、車両の車載ネットワーク２から送信されたログデータをもとに、当該ログデータにより表される異常状態が及ぼす影響の範囲が推定され、当該影響範囲に対応する車両群が選択されて対応指示が通知される。このため、異常状態が検知された車両のみならず、例えば同一メーカ、車種、年式の他の車両に対しても同時に対応指示を通知することができる。この結果、例えばサイバー攻撃により特定のメーカ、車種又は年式の車両のＥＣＵのプログラム又は制御データが改ざんされた場合には、該当する車両のプログラム又は制御データを遠隔より一括して修復することが可能となる。

[0066] また、異常状態が及ぼす影響の範囲をもとに対応指示の通知先となる車両が選択され、これらの車両に対してのみ通知指示が通知される。このため、対応が必要な車両に対しもれなく対応指示を通知することができ、一方他の無関係な車両には対応指示が通知されないので、他車両に対しては悪影響が及ばないようにすることができる。

[0067] さらに、対応指示を送信する際に、異常状態が及ぼす危険の度合いおよび異常の脅威種別又は発生要因もしくはその両方の推定結果に基づいてそれらに適した対応指示を生成して送信することができる。このため、車載ネットワーク２内のＥＣＵ、車載機器または装置のプログラムや動作状態を、より的確に復旧させることが可能となる。

[0068] さらに、異常状態が及ぼす危険の度合いに基づいて対応指示の通知先に対し優先度が設定される。このため、例えばパワーユニットの異常やサイバー攻撃による車載ネットワーク２の乗っ取り等のように、車両の走行自体に影

響する重要度の高い異常が検知された車載ネットワーク２に対しては、それよりも重要度の低い異常が検知された車載ネットワーク２より優先的に対策指示を通知することが可能となる。

[0069] ［その他の実施形態］

（１）ログデータから異常を検知する手法として、例えば、異常の影響範囲、危険度および脅威種別又は発生要因もしくはその両方を推定するために、ニューラルネットワーク等を用いた学習モデルを使用してもよい。この場合ＳＯＣサーバ３０は、ログデータから異常動作の特徴を表す複数のパラメータを抽出し、これらのパラメータを学習モデルに入力することにより、異常動作が及ぼす影響範囲、危険度および異常の脅威種別又は発生要因もしくはその両方の推定結果を得る。異常動作の特徴を表すパラメータとしては、例えば振動、温度、回転数、速度、照度、周囲の天候等が考えられる。

[0070] （２）一実施形態では、車両セキュリティ監視装置の全機能をＳＯＣサーバ３０に設けた場合を例にとって説明した。しかし、それに限定されるものではなく、例えば、車両セキュリティ監視装置の機能を、ＳＯＣサーバ３０とＰＳＩＲＴサーバ４０又は外部サーバ５０に分散して設けるようにしてもよい。

[0071] （３）その他、検知対象となる異常の種類とその検知手法、異常状態の影響範囲、危険度および脅威種別又は発生要因もしくはその両方のそれぞれの推定手法、車両セキュリティ監視装置のおよび車載ネットワークの構成、車両セキュリティ監視処理による処理手順と処理内容等についても、この発明の要旨を逸脱しない範囲で種々に変形することが可能である。

[0072] （４）前記一実施形態では地上を走行する乗用車や貨物車、二輪車等の一般車両を対象として説明した。しかしこの発明は、車両として、バスやタクシー等の乗り合い用の営業車両、工事用車両、農業用車両、救急車両等の特殊用途車両等を対象としてもよく、さらには航空機やヘリコプター、ドローン等の飛行体、水上を走行する漁船や客船、貨物船、タンカー等の船舶、路面電車やモノレール等の軌道上を走行する鉄道等車両への適用も可能である

。

[0073] （５）各実施形態は可能な限り適宜組み合わせて実施してもよく、その場合組み合わせた効果が得られる。更に、上記実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適当な組み合わせにより種々の発明が抽出され得る。例えば、実施形態に示される全構成要件からいくつかの構成要件が削除されても、発明が解決しようとする課題の欄で述べた課題が解決でき、発明の効果の欄で述べられている効果が得られる場合には、この構成要件が削除された構成が発明として抽出され得る。

符号の説明

[0074] １…車両

２…車載ネットワーク

３…通信制御ユニット（ＴＣＵ）

４…ナビゲーション装置

５…ＵＳＢメモリ

６…携帯端末

７…移動通信ネットワーク

８…モビリティサービスネットワーク

８１，８２…ゲートウェイ

９…インターネット

２０…モビリティサービスサーバ

３０…ＳＯＣサーバ

３１…制御ユニット

３２…記憶ユニット

３３…通信Ｉ／Ｆ

３１１…脅威情報取得部

３１２…ログデータ取得部

３１３…異常検知処理部

３１４…影響範囲推定部

３１５…危険度推定部

３１６…脅威種別／原因推定部

３１７…通知対象車両選択部

３１８…通知情報送信部

３１９…レポート情報送信部

３２１…脅威情報記憶部

３２２…ログデータ記憶部

３２３…異常検知情報記憶部

３２４…影響推定情報記憶部

４０…ＰＳＩＲＴサーバ

５０…外部サーバ

請求の範囲

[請求項1] 車載装置の動作状態に関するログデータを送信する機能を有する車載ネットワークとの間で通信が可能な車両セキュリティ監視装置であって、

前記ログデータを取得するログデータ取得部と、

前記取得されたログデータに基づいて前記車載ネットワークにおける異常状態を検知する異常状態検知部と、

前記検知された異常状態が及ぼす影響の範囲を推定する第１の推定部と、

前記推定された影響の範囲を表す情報を管理する推定情報管理部とを具備する車両セキュリティ監視装置。

[請求項2] 前記検知された異常状態が及ぼす危険の度合いを推定する第２の推定部を、さらに具備し、

前記推定情報管理部は、前記推定された影響危険の度合いを表す情報をさらに管理する、請求項１に記載の車両セキュリティ監視装置。

[請求項3] 前記検知された異常状態の脅威種別および発生要因の少なくとも一方を推定する第３の推定部を、さらに具備し、

前記推定情報管理部は、前記推定された脅威種別および発生要因の少なくとも一方を表す情報をさらに管理する、請求項１または２に記載の車両セキュリティ監視装置。

[請求項4] 前記推定情報管理部により管理される前記影響の範囲を表す情報に基づいて当該影響の範囲に関係する対応策の通知対象を選択し、当該選択された通知対象に対し前記対応策を表す情報を含む通知情報を送信する第１の送信制御部を、さらに具備する請求項１に記載の車両セキュリティ監視装置。

[請求項5] 前記推定情報管理部により管理される前記危険の度合いを表す情報に基づいて対応策の通知対象に対する優先度を設定し、当該優先度に従い通知対象に対し対応策を表す情報を含む通知情報を送信する第２

の送信制御部を、さらに具備する請求項２に記載の車両セキュリティ監視装置。

[請求項6] 前記異常検知部により検知された異常状態と、前記推定情報管理部により管理される前記影響の範囲、前記危険の度合い、前記脅威種別および発生要因の少なくとも一方を表す各情報とに基づいて、前記異常状態に対する対応内容を含む対応指示情報を生成し、生成された対応指示情報を通知対象に送信する第３の送信制御部とを、さらに具備する請求項３に記載の車両セキュリティ監視装置。

[請求項7] 前記推定情報管理部は、脅威種別と危険度の尺度との組み合わせを定義した情報を記憶し、

前記第３の送信制御部は、前記記憶された脅威種別と危険度の尺度との組み合わせを定義した情報を参照して、前記前記異常状態に対する対応内容と対応指示の通知対象を決定する、請求項６に記載の車両セキュリティ監視装置。

[請求項8] 前記第１の送信制御部は、前記影響の範囲に関係する対応策の通知対象として、前記車載ネットワークまたは当該システムを搭載する車両の製造者または販売者、車種、年式、使用地域の少なくとも１つに該当する車両またはその車載ネットワークを選択し、当該選択された車両またはその車載ネットワークに対し前記対応策を表す情報を含む通知情報を送信する、請求項４に記載の車両セキュリティ監視装置。

[請求項9] 車載装置の動作状態に関するログデータを送信する機能を有する車載ネットワークとの間で通信が可能な車両セキュリティ監視装置が実行する車両セキュリティ監視方法であって、

前記ログデータを取得する過程と、

前記取得されたログデータに基づいて前記車載ネットワークにおける異常状態を検知する過程と、

前記検知された異常状態が及ぼす影響の範囲を推定する過程と、

前記推定された影響の範囲を表す情報を管理する過程と

を具備する車両セキュリティ監視方法。

[請求項10] 前記検知された異常状態が及ぼす危険の度合いを推定する過程を、さらに具備し、

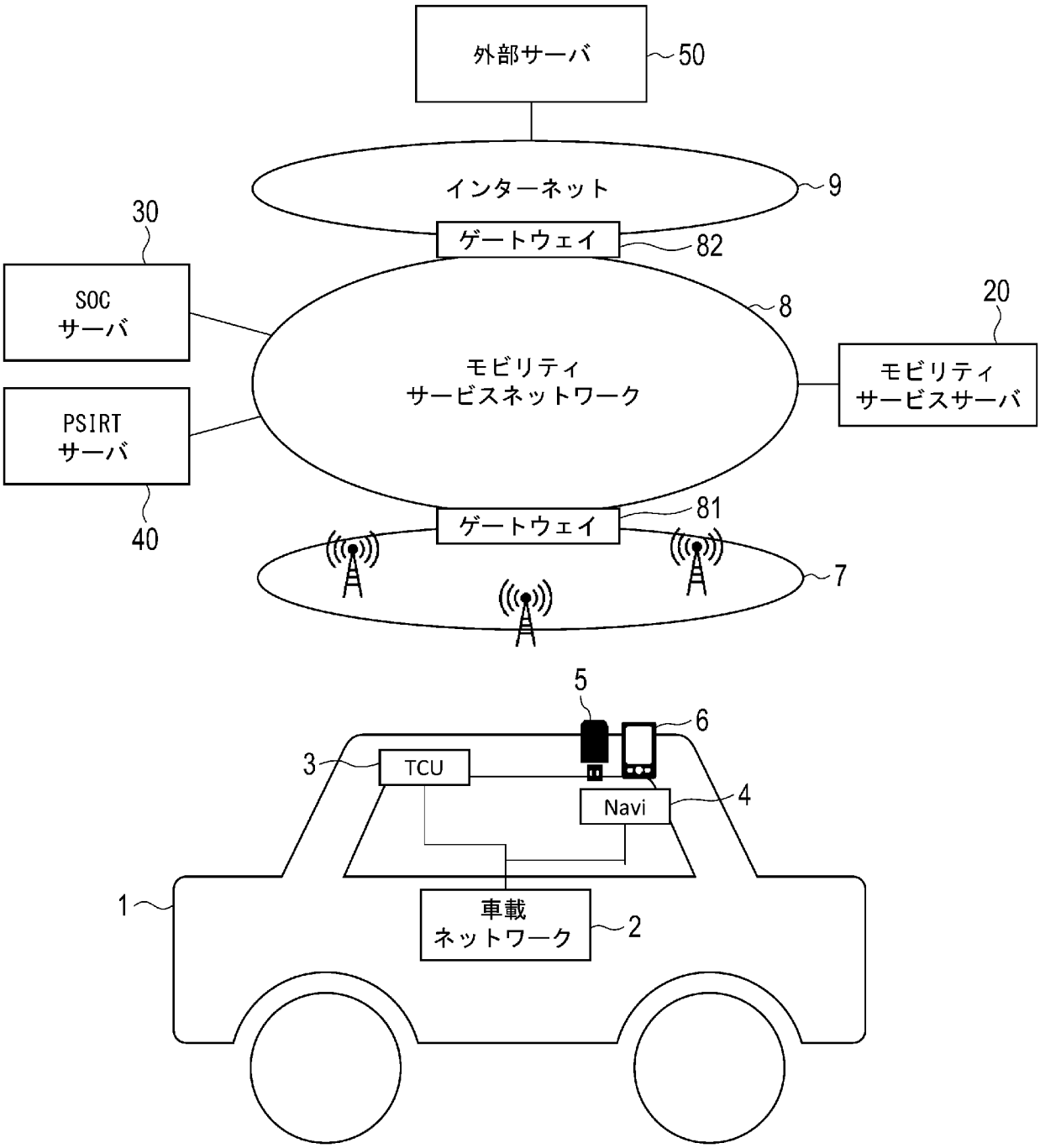
前記推定情報を管理する過程は、前記推定された危険の度合いを表す情報をさらに管理する、請求項９に記載の車両セキュリティ監視方法。

[請求項11] 前記検知された異常状態の脅威種別および発生要因の少なくとも一方を推定する過程を、さらに具備し、

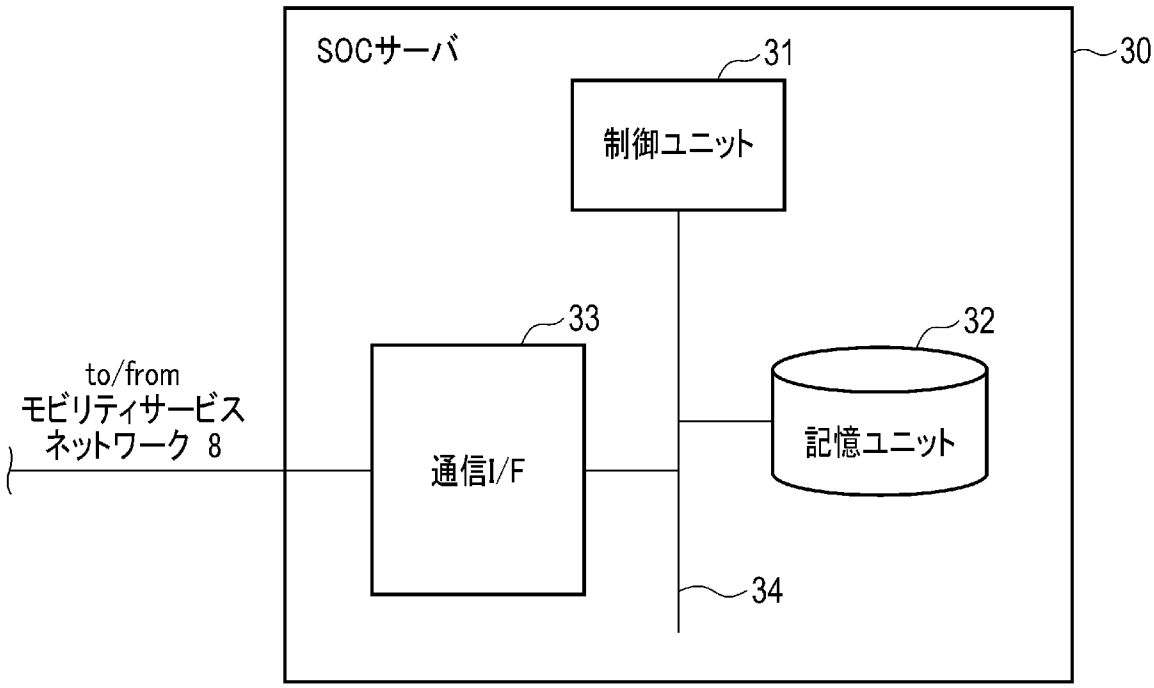
前記推定情報を管理する過程は、前記推定された脅威種別および発生要因の少なくとも一方を表す情報をさらに管理する、請求項９または１０に記載の車両セキュリティ監視方法。

[請求項12] 請求項１乃至８のいずれかに記載の車両セキュリティ監視装置が具備する前記各部による処理を、前記車両セキュリティ監視装置が備えるハードウェアプロセッサに実行させるプログラム。

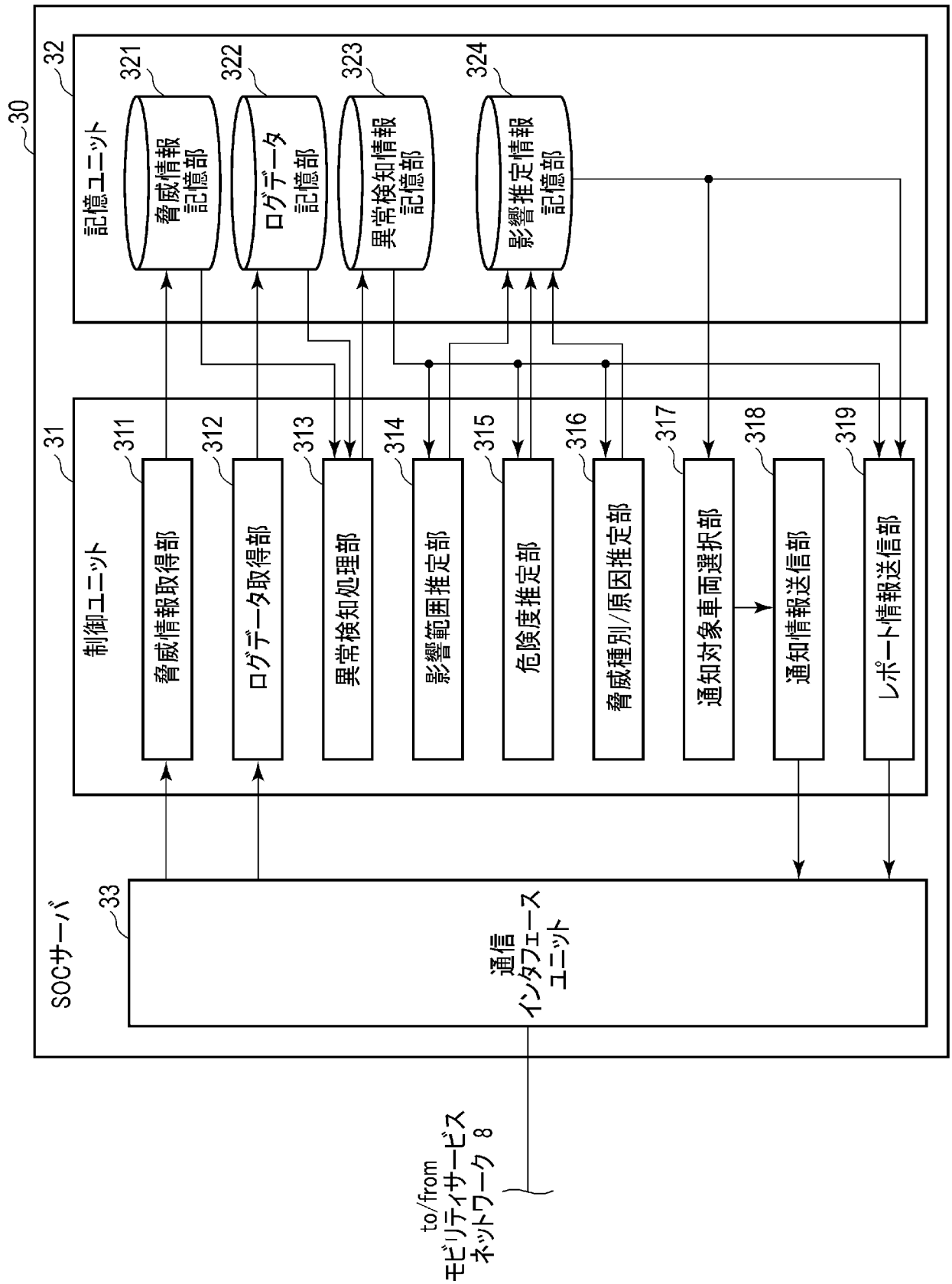
[図1]


外部サーバ
50
インターネット
9
30
ゲートウェイ
82
SOC
サーバ
8
20
モビリティ
サービスネットワーク
モビリティ
サービスサーバ
PSIRT
サーバ
40
ゲートウェイ
81
7
5
6
3
TCU
Navi
4
1
車載
ネットワーク
2

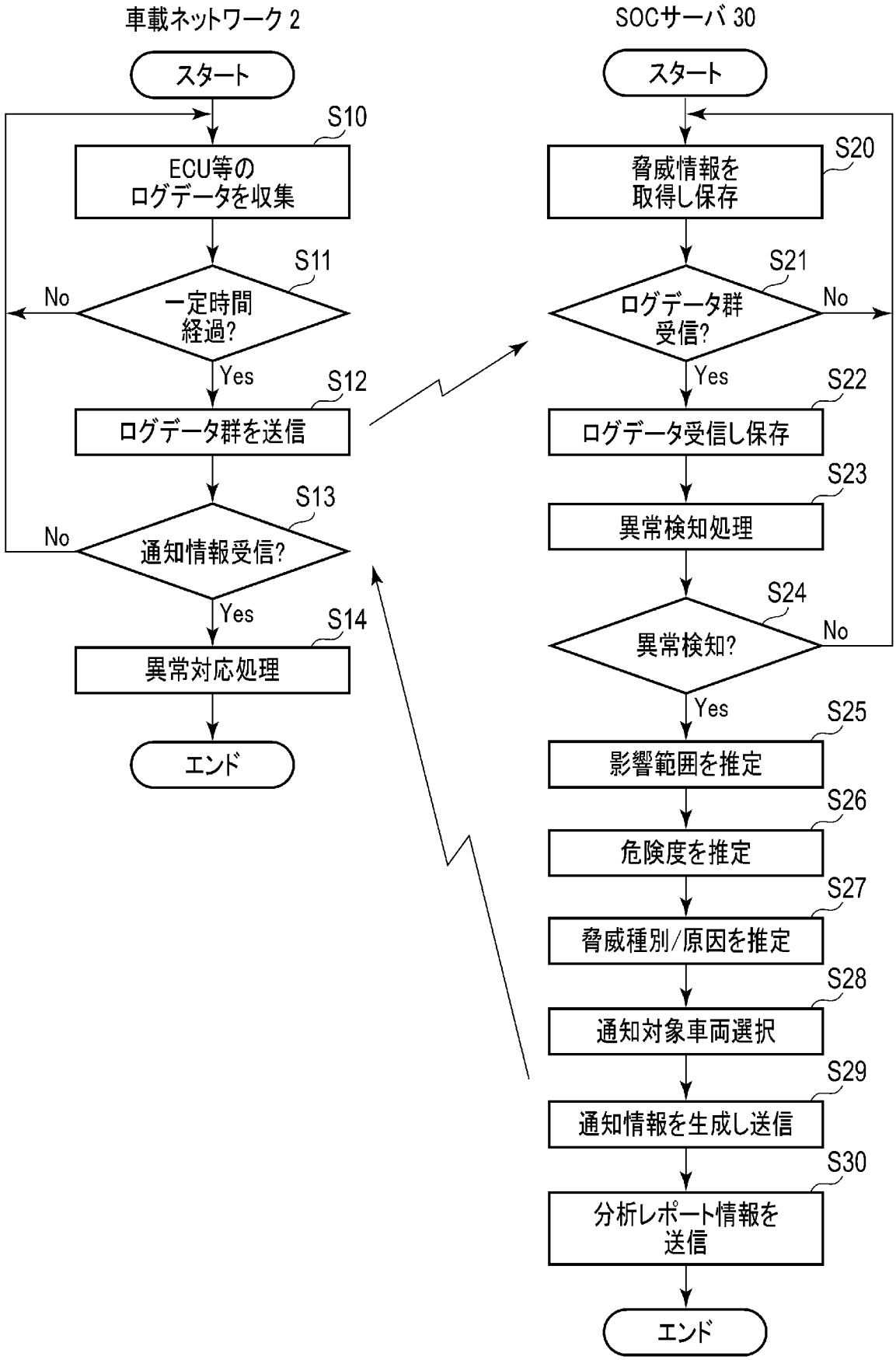
[図2]


SOCサーバ
31
30
制御ユニット
33
32
to/from
モビリティサービス
ネットワーク 8
通信I/F
記憶ユニット
34

[図3]


30
SOCサーバ
32
記憶ユニット
321
脅威情報
記憶部
322
ログデータ
記憶部
323
異常検知情報
記憶部
324
影響推定情報
記憶部
31
制御ユニット
311
脅威情報取得部
312
ログデータ取得部
313
異常検知処理部
314
影響範囲推定部
315
危険度推定部
316
脅威種別/原因推定部
317
通知対象車両選択部
318
通知情報送信部
319
レポート情報送信部
33
通信
インタフェース
ユニット
to/from
モビリティサービス
ネットワーク 8

[図4]


車載ネットワーク 2
スタート
S10
ECU等の
ログデータを収集
S11
No
一定時間
経過?
Yes
S12
ログデータ群を送信
S13
No
通知情報受信?
Yes
S14
異常対応処理
エンド
SOCサーバ 30
スタート
S20
脅威情報を
取得し保存
S21
ログデータ群
受信?
No
Yes
S22
ログデータ受信し保存
S23
異常検知処理
S24
異常検知?
No
Yes
S25
影響範囲を推定
S26
危険度を推定
S27
脅威種別/原因を推定
S28
通知対象車両選択
S29
通知情報を生成し送信
S30
分析レポート情報を
送信
エンド

[図5]


インシデントの危険度
インシデントの攻撃種別
Description
Information
Medium
Serious
Critical
不正アクセス
脆弱性を突く攻撃や、認証突破を試みるアクセス
攻撃成功の可能性が高い場合
攻撃成功が明白な場合
DoS攻撃
サービス不能状態に陥れるようなイベント
影響は見られていないがDoS攻撃が発生している場合
サービス不能状態が確認された場合
マルウェア
マルウェアのダウンロードおよび感染後挙動
アドウェア等好まれざるプログラムの挙動が確認された場合
マルウェアのダウンロード成功が確認された場合
マルウェアの感染が確認された場合
不自然な通信
一般的なポリシーに違反するような通信や設定不備が疑われるような通信
不自然な通信が確認された場合
セキュリティ侵害に繋がるような設定不備が発見された場合
調査行為
ネットワークスキャン、脆弱性スキャンなどの調査行為
継続的なスキャン行為が発生している場合
その他
上記に分類されないもの
その他
調査の過程でセキュリティ不備が見つかった場合

[図6]


分析レポート
※Analysts name
不正なサイトへのアクセス(NUCLEAR Exploit Kit)
※Customer
〇〇株式会社
※Device
Reference #
test_device_ids01
277622
Data and Time
2018-07-01 15:06:1
※Severity
Medium
※Category
x300 マルウェア
※Description
Dst側ホストがエクスプロイトキットの設置されたページにアクセスした可能性があります。
Time:2015-06-27 15:41:19
Src:203.xx.yy.zz:8080
Dst:203.zz.yy.zz:49612
Signature:NUCLEAR Exploit Kit Detection
一般的なドライイブバイダウンロードでは、
ユーザがエクスプロイトキットの設置されたページにアクセスした後、
アプリケーションなどの脆弱性を利用されマルウェアのダウンロードが実行されます。
今回取得されたPCAPから、NUCLEAR
ExploitKitで生成したと思われるJavaScriptの一部分が確認できました。
URLログを取得していないため、具体的なアクセス先はSOCでは把握できず、
これ以上の調査はできていません。
現時点のところ、マルウェア感染と思われる通信は確認されていませ
※Recommendation/Actions
下記項目の実施を推奨いたします。
(1)Proxyログ等をご確認いただき、該当ホストのアクセス先が業務上意図されたものかご確認ください。
(2)万が一不審なサイトへアクセスしていた場合、
アンチウイルスソフトを用いて該当ホストのスキャンを実施するとともに、
周辺のNW機器において不審な通信が発生していないかご確認ください。
Severity
各インシデントの危険度
Category
各インシデントの攻撃種別
Recommendation/Action
攻撃に対するお客様への推奨対応

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/000285

A. CLASSIFICATION OF SUBJECT MATTER
B60R 16/02(2006.01)i; G06F 21/55(2013.01)i
FI: G06F21/55; B60R16/02 660Q; B60R16/02 660W
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)
B60R16/02: G06F21/55

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

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2020
Registered utility model specifications of Japan	1996-2020
Published registered utility model applications of Japan	1994-2020

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) 22.06.2017 (2017-06-22) paragraphs [0024], [0041]-[0124], fig. 2-8	1-2, 4-5, 8-10, 12
Y	paragraphs [0024], [0041]-[0124], fig. 2-8	3, 6-8, 11-12
Y	US 2018/0351980 A1 (GALULA, Yaron) 06.12.2018 (2018-12-06) paragraphs [0029]-[0126]	3, 6-8, 11-12

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

☒ See patent family annex.

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

Date of the actual completion of the international search	Date of mailing of the international search report
31 January 2020 (31.01.2020)	10 February 2020 (10.02.2020)

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2020/000285

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2017-111796 A	22 Jun. 2017	US 2018/0295147 A1 paragraphs [0046], [0063]-[0146], fig. 2-8 CN 107925600 A	
US 2018/0351980 A1	06 Dec. 2018	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2020/000285

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

B60R 16/02(2006.01)i; G06F 21/55(2013.01)i
FI: G06F21/55; B60R16/02 660Q; B60R16/02 660W

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））

B60R16/02; G06F21/55

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０２０年
日本国実用新案登録公報	１９９６－２０２０年
日本国登録実用新案公報	１９９４－２０２０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) 22.06.2017 (2017-06-22) 段落[0024],[0041]-[0124],図2-8	1-2,4-5,8-10,12
Y	段落[0024],[0041]-[0124],図2-8	3,6-8,11-12
Y	US 2018/0351980 A1 (GALULA, Yaron) 06.12.2018 (2018-12-06) 段落[0029]-[0126]	3,6-8,11-12

☐ 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抵触するものではなく、発明の原理又は理論の理解のために引用するもの
“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
“Y” 特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
“&” 同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
31.01.2020	10.02.2020

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
上島　拓也 5S 6293
電話番号 03-3581-1101 内線 3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2020/000285

引用文献	公表日	パテントファミリー文献	公表日
JP 2017-111796 A	22.06.2017	US 2018/0295147 A1 段落[0046],[0063]-[0146], 図2-8 CN 107925600 A	
US 2018/0351980 A1	06.12.2018	（ファミリーなし）	