(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
2018年7月26日(26.07.2018)

WIPO | PCT

(10) 国際公開番号
WO 2018/134981 A1

(51) 国際特許分類:
G06F 21/55 (2013.01)

(21) 国際出願番号： PCT/JP2017/002013

(22) 国際出願日： 2017年1月20日(20.01.2017)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

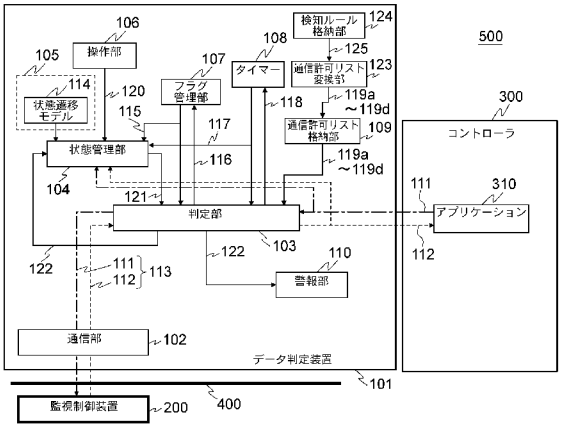
(71) 出願人: 三菱電機株式会社(**MITSUBISHI ELECTRIC CORPORATION**) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目7番3号 Tokyo (JP).

(72) 発明者: 山口 晃由(**YAMAGUCHI, Teruyoshi**); 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP). 中井 綱人(**NAKAI, Tsunato**); 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP). 清水 孝一(**SHIMIZU, Koichi**); 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP). 小林 信博(**KOBAYASHI, Nobuhiro**); 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP).

(74) 代理人: 曾我 道治, 外(**SOGA, Michiharu** et al.); 〒1000005 東京都千代田区丸の内三丁目1番1号 国際ビルディング 8階 曾我特許事務所 Tokyo (JP).

(54) **Title:** DATA DETERMINATION DEVICE, DATA DETERMINATION METHOD, AND DATA DETERMINATION PROGRAM

(54) 発明の名称： データ判定装置、データ判定方法、および、データ判定プログラム



101 Data determination device
102 Communication unit
103 Determination unit
104 State management unit
106 Operation unit
107 Flag management unit
108 Timer
109 Communication permission list storage unit
110 Alarm unit
114 State transition model
123 Communication permission list conversion unit
124 Detection rule storage unit
200 Monitoring control device
300 Controller
310 Application

(57) **Abstract:** A communication permission list conversion unit 123 assigns at least one flag to a request communication and a response communication for which a correspondence relationship is described by a detection rule, and causes a communication permission list to describe and associate the content of a flag operation for specifying a value to be set for the flag, with a flag condition for determining whether the flag has been set to the value to be set for the flag. If a determination unit 103 determines that communication data of the request communication is normal, the determination unit 103 sets the flag to the value to be set for the flag. Then when the determination unit 103 determines whether or not communication data of the response communication corresponding to the request communication is normal, the determination unit 103 determines whether the flag has been set to the value to be set for the flag, and if so, the determination

WO 2018/134981 A1

[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, 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:

一　国際調査報告（条約第21条(3)）

unit 103 determines that the communication data of the response communication is normal, and resets the flag.

(57) 要約：通信許可リスト変換部１２３は、検知ルールに対応関係が記述された要求通信及び応答通信に対して１以上のフラグを割り当て、当該フラグに対して設定すべき値を指定したフラグ操作の内容と、当該フラグに当該設定すべき値が設定されているかを判定するためのフラグ条件とを対応させて通信許可リストに記述する。判定部１０３は、要求通信の通信データが正常であると判定した後に、当該フラグに設定すべき値をセットし、要求通信に対する応答通信の通信データが正常であるか否かを判定する場合に、当該フラグに設定すべき値が設定されているか否かを判定し、設定されていた場合に、応答通信の通信データを正常であると判定して、当該フラグをリセットする。

明　細　書

発明の名称 ：

データ判定装置、データ判定方法、および、データ判定プログラム

技術分野

[0001] 本発明は、データ判定装置、データ判定方法、および、データ判定プログラムに関し、特に、ネットワークへの不正な侵入を検知するためのデータ判定装置、データ判定方法、および、データ判定プログラムに関する。

背景技術

[0002] 近年、産業制御システムにおいて、当該システムがネットワークに接続されるケースが増大している。そのため、システムがサイバー攻撃の標的になるケースが増加している。従って、産業制御システムにおいては、サイバー攻撃によるネットワークへの侵入を検知するために、以下のような侵入検知システムが用いられている。

[0003] 従来の侵入検知システムでは、産業制御システムのネットワーク通信が固定的であることを利用して、送信先アドレスと送信元アドレスとのペアを設定およびプロトコルを設定することで、許可される通信を定義する。そして、侵入検知システムは、許可された通信以外を異常と判定することによって、未知の攻撃に対しても、その侵入を検知するホワイトリスト型の対策を取っている（例えば、特許文献１，２参照）。

[0004] また、許可する通信シーケンスを定義して、各々の通信シーケンスにおいて、未接続、通信中、異常処理等の通信の状態を管理する方式が提案されている（例えば、特許文献２参照）。

[0005] さらに、通信のトランザクションをステートマシンで記述し、通信の順序をホワイトリストとして記述できる方法が提案されている（例えば、非特許文献１参照）。

[0006] また、検知ルールの増加に伴い、いかに検索を高速化するかが課題となっている。パケットデータのマッチングを行うＤＰＩ（Ｄｅｅｐ　Ｐａｃｋｅ

ｔ　Ｉｎｓｐｅｃｔｉｏｎ）では、Ｂｌｏｏｍ　Ｆｉｌｔｅｒを用いる手法（例えば、非特許文献２参照）、および、マルチコアプロセッサを用いる手法（例えば、非特許文献３，４参照）が提案されている。

先行技術文献

特許文献

[0007] 特許文献1：特許第４６８８４２０号公報

特許文献2：特開２００１－０３４５５３号公報

非特許文献

[0008] 非特許文献1：Niv Goldenberg, Avishai Wool, “Accurate Modeling of Modbus/TCP for Intrusion Detection in SCADA Systems”, International Journal of Critical Infrastructure Protection, Volume 6, Issue 2, June 2013.

非特許文献2：Sarang Dharmapurikar, Praveen Krishnamurthy, Todd Sproull, John Lockwood, “Deep Packet Inspection Using Parallel Bloom Filters.”, In Proc. 11th Symp. High Performance Interconnects (HOTI’03), pages 44-51, Stanford, California, 2003.

非特許文献3：Marco Danelutto, Luca Deri, Daniele De Sensi, Massimo Torquati, “Deep Packet Inspection on Commodity Hardware using FastFlow”, Advances in Parallel Computing, Volume 25, Pages 92-99, January 2014.

非特許文献4：Cheng-Hung Lin, Sheng-Yu Tsai, Chen-Hsiung Liu, Shih-Chieh Chang, Jyuo-Min Shyu, “Accelerating String Matching Using Multi-Threaded Algorithm on GPU”, Global Telecommunications Conference (GLOBECOM 2010), Pages: 1-5, December 2010, IEEE.

発明の概要

発明が解決しようとする課題

[0009] 特許文献１，２などに記載の従来のホワイトリストは、パケット単体がル

ールにマッチするかを判定するものが多い。しかしながら、近年、産業制御システムをターゲットにした、例えばStuxnetのように、単一パケットの判定によっては検知できない攻撃も存在する。これらの攻撃を検知するためには、通信が行われた時のシステムまたは装置の状態、および、要求と応答との対応関係などを検知対象に含める必要がある。しかしながら、特許文献１では、そのような対策はとられていない。

[0010] 特許文献２に記載の従来の技術においては、送信元及び送信先の通信状態を監視し、それらの通信状態が、あらかじめ規定された通信シーケンスに従った通信状態であるか否かを判定し、判定結果に従って、アクセス制御を行う。しかしながら、この場合、第三者が、乗っ取ったサーバから通信シーケンスに従った通信を行った場合には、当該通信がサイバー攻撃であることを検知することができないので、その結果、プログラムを不正に書き換える攻撃データなども通信可能となってしまうという課題がある。

[0011] 一方、非特許文献１等に記載の従来の技術においては、要求と応答との対応関係も検知対象に含められているので、サイバー攻撃をより高度に検知することを可能にできる。しかし、非特許文献１では、複数台の機器の通信を１台の検知装置で検知する場合、全装置間の通信の組み合わせをステートマシンで記述しなければならず、組み合わせ爆発を起こす。

[0012] また、検索の高速化において、非特許文献２に記載の従来の技術では、False Positive の可能性があるため、ホワイトリスト型で使用すると、攻撃を見逃す可能性がある。

[0013] また、非特許文献３に記載の従来の技術は、判定処理の並列化によって高速化することを目的としており、判定対象自体を削減することはできない。また、並列プログラミングを実行できるプロセッサ上でしか動作しないという課題がある。

[0014] 本発明は、かかる課題を解決するためになされたものであり、組み合わせ爆発を抑え、高速かつ高精度に、第三者によってサーバが乗っ取られて当該サーバからサイバー攻撃された場合においても、通信データが不正なもので

あることを検知することが可能な、データ判定装置、データ判定方法、および、データ判定プログラムを提供することを目的とする。

課題を解決するための手段

[0015] 本発明は、自装置に対して設定されるフラグの現在値を格納するフラグ管理部と、複数の運用状態間を遷移する自装置の現在の運用状態を格納するとともに、外部からの入力信号、および、前記フラグ管理部が格納する前記フラグの現在値のうちのいずれか１以上に応じて、前記運用状態間の遷移が定義されている状態遷移モデルに従って、前記自装置の運用状態を遷移させる状態管理部と、要求通信を構成する通信データと前記要求通信に対する応答通信を構成する通信データとの対応関係を記述した検知ルールを、前記運用状態ごとに通信が許可された通信データを予め登録する通信許可リストに変換する、通信許可リスト変換部と、前記状態管理部が格納する前記自装置の前記現在の運用状態と、前記通信許可リストと、前記フラグ管理部が格納する前記フラグの現在値とのいずれか１以上を用いて、前記自装置に入力された通信データが、前記通信許可リストに登録された前記現在の運用状態における通信データであるか否かを判定することで、前記自装置に入力された前記通信データが正常か異常かを判定する判定部とを備え、前記通信許可リスト変換部は、前記検知ルールを前記通信許可リストに変換するときに、前記検知ルールに対応関係が記述された前記要求通信及び前記応答通信に対してフラグを割り当て、当該フラグに対する設定値を指定したフラグ操作の内容と、前記フラグに前記設定値が設定されているかを判定するためのフラグ条件とを対応させて、前記通信許可リストに記述し、前記判定部は、前記要求通信の通信データが正常であると判定した後に、前記フラグ操作の内容に従って、前記フラグに前記設定値をセットし、前記要求通信に対する前記応答通信の通信データが正常であるか否かを判定する場合に、前記フラグ条件に基づいて前記フラグに前記設定値が設定されているか否かを判定し、前記設定値が設定されていた場合に、前記応答通信の通信データを正常であると判定して、前記フラグをリセットする、データ判定装置である。

発明の効果

[0016] 本発明に係るデータ判定装置においては、通信許可リストに正常な通信を定義する際に、要求通信と応答通信との対応関係を記述するようにしたので、組み合わせ爆発を起こさずに、すべての通信データを記述することができる。また、要求通信と応答通信との対応関係をフラグのセット／リセットで判定できるようにし、要求通信と応答通信との対応関係も考慮して通信データが正常か異常かを判定するようにしたので、第三者によってサーバが乗っ取られて当該サーバからサイバー攻撃された場合においても、通信データが不正であることを検知することができる。また、要求通信と応答通信との対応関係を定義することにより、増大する検知ルールの検索を高速に行うことができる。

図面の簡単な説明

[0017] [図1]本発明の実施の形態１に係るデータ判定装置の構成を示したブロック図である。

[図2]本発明の実施の形態１に係るデータ判定装置の変形例の構成を示したブロック図である。

[図3]本発明の実施の形態１に係るデータ判定装置における状態遷移モデル記憶部に記憶された状態遷移モデルの一例を示した図である。

[図4]本発明の実施の形態１に係るデータ判定装置における検知ルール格納部に格納された検知ルールリストの一例を示す図である。

[図5]本発明の実施の形態１に係るデータ判定装置における通信許可リスト格納部に格納された通信許可リストの一例を示す図である。

[図6]本発明の実施の形態１に係るデータ判定装置における通信許可リスト格納部に格納された通信許可リストの一例を示す図である。

[図7]本発明の実施の形態１に係るデータ判定装置における通信許可リスト格納部に格納された通信許可リストの一例を示す図である。

[図8]本発明の実施の形態１に係るデータ判定装置における通信許可リスト格納部に格納された通信許可リストの一例を示す図である。

[図9]本発明の実施の形態１に係るデータ判定装置のハードウェア構成を示したブロック図である。

[図10]本発明の実施の形態１に係るデータ判定装置におけるデータ判定処理の流れを示したフローチャートである。

[図11]本発明の実施の形態１に係るデータ判定装置における判定部の処理の流れを示したフローチャートである。

[図12]本発明の実施の形態１に係るデータ判定装置における通信許可リスト変換部の処理の流れを示したフローチャートである。

[図13]本発明の実施の形態１に係るデータ判定装置から得られる効果を説明する図である。

発明を実施するための形態

[0018] 実施の形態１.

図１および図３～図８を用いて、本発明の実施の形態１に係るデータ判定装置１０１の構成について説明する。ここでは、図１に示すように、本実施の形態１に係るデータ判定装置１０１が、監視制御装置２００およびコントローラ３００に接続されていて、監視制御装置２００とコントローラ３００との間で双方向通信される通信データを判定対象とする場合について説明する。但し、以下では、コントローラ３００から監視制御装置２００へ送信されるデータを送信データ１１１と呼び、コントローラ３００が監視制御装置２００から受信するデータを受信データ１１２と呼ぶこととする。また、データ判定装置１０１、監視制御装置２００、および、コントローラ３００を備えるシステムを、データ判定システム５００と称する。

[0019] 図１に示すように、データ判定装置１０１は、ネットワーク４００に接続されている。データ判定装置１０１は、ネットワーク４００を介して、監視制御装置２００に接続される。また、データ判定装置１０１は、コントローラ３００に接続されている。データ判定装置１０１は、監視制御装置２００とコントローラ３００との間で送信される通信データの仲介を行う。また、データ判定装置１０１は、当該通信データが不正アクセスによるものか否か

の判定も行う。このように、データ判定装置１０１は、ネットワーク４００に侵入する攻撃を検知する侵入検知装置および侵入検知システムを構成している。

[0020] ここでは、コントローラ３００が産業制御システムに備えられている場合を例に挙げる。但し、その場合に限られることはなく、コントローラ３００は、任意のシステムに備えることができる。コントローラ３００は、アプリケーション３１０を備える。アプリケーション３１０は、送信データ１１１を、データ判定装置１０１を介して、監視制御装置２００に送信する。また、アプリケーション３１０は、受信データ１１２を、データ判定装置１０１を介して、監視制御装置２００から受信する。送信データ１１１および受信データ１１２が、本実施の形態１に係るデータ判定装置の判定対象であるため、以下では、受信データ１１２および送信データ１１１を、まとめて、通信判定データ１１３と呼ぶこととする。

[0021] 一方、監視制御装置２００は、コントローラ３００が備えられた産業制御システムを監視制御するサーバである。

[0022] データ判定装置１０１は、監視制御装置２００からネットワーク４００を介して受信した受信データ１１２を、コントローラ３００に送信する。また、データ判定装置１０１は、コントローラ３００のアプリケーション３１０が送信した送信データ１１１を、ネットワーク４００を介して、監視制御装置２００に送信する。データ判定装置１０１は、受信データ１１２及び送信データ１１１を仲介する過程において、ネットワーク４００への攻撃的な侵入を検知するデータ判定処理を行う。

[0023] 図１に示すように、データ判定装置１０１は、状態管理部１０４、タイマー１０８、通信許可リスト格納部１０９、通信許可リスト変換部１２３、検知ルール格納部１２４、判定部１０３、通信部１０２、警報部１１０、操作部１０６、フラグ管理部１０７、および、状態遷移モデル記憶部１０５を有する。但し、タイマー１０８、通信許可リスト格納部１０９、検知ルール格納部１２４、警報部１１０、操作部１０６については、必ずしも設けなくて

もよい。

[0024] 状態遷移モデル記憶部１０５は、自装置が取得した取得情報に応じて、複数の運用状態の各運用状態間を遷移するための状態遷移モデル１１４を記憶する。自装置とは、データ判定装置１０１自身である。また、取得情報とは、データ判定装置１０１の状態を遷移させる要素である。取得情報は、通信により外部から取得される通信データと、自装置に対する入力操作を受け付けたことを示す操作信号１２０と、タイマー１０８から出力されるタイマー現在値１１７と、フラグ管理部１０７から出力されるフラグ現在値１１５とを含む。

[0025] 図３に、状態遷移モデル１１４の一例を示す。図３は一例であり、状態遷移モデル１１４は必ずしも図３の通りでなくてもよい。

図３において、符号３０１～３０８は、データ判定装置１０１の複数の運用状態の例を示す。ここでは、運用状態の例として、停止中３０１、立上げ３０２、制御中３０３、立下げ３０４、保守３０５、立上げ３０６、試運転３０７、立下げ３０８が挙げられている。

また、図３において、１つの運用状態と他の運用状態との間には、運用状態間の状態遷移の例が示されている。例えば、図３の例では、データ判定装置１０１は、電源投入時に停止中３０１に遷移する。また、停止中３０１から「立上げ開始」を実行すると、立上げ３０２に移行する。また、立上げ３０２から「立上げ完了」すると、制御中３０３に移行する。これらの「立上げ開始」、「立上げ完了」などが、各運用状態間の状態遷移の情報である。状態遷移モデル１１４においては、どの運用状態から、どの運用状態に遷移するかが予め定義されている。従って、停止中３０１からは立上げ３０２に遷移することが定義されているため、停止中３０１から他の運用状態３０３～３０７のいずれにも遷移することはない。

また、「立上げ開始」等の状態遷移を指示する状態遷移指令信号は、操作部１０６にユーザによって入力される操作信号１２０、データ判定装置１０１が受信した受信データ１１２または送信データ１１１、フラグ管理部１０

７からのフラグ現在値１１５、タイマー１０８からのタイマー現在値１１７である。

このように、状態遷移モデル１１４には、各運用状態３０１～３０７の情報と、それらの運用状態間の状態遷移の情報とが含まれている。

[0026] 状態管理部１０４は、操作部１０６にユーザによって入力される操作信号１２０、データ判定装置１０１が受信した受信データ１１２または送信データ１１１、フラグ管理部１０７からのフラグ現在値１１５、タイマー１０８からのタイマー現在値１１７のうちの少なくとも１つが入力された場合に、状態遷移モデル１１４に従って、自装置、すなわちデータ判定装置１０１の運用状態を遷移させ、最新の運用状態を保有する。

[0027] 通信許可リスト格納部１０９は、通信許可ルール１４１として、通信許可リスト１１９ａ～１１９ｄを格納する。図５～図８に、通信許可リスト１１９ａ～１１９ｄの例をそれぞれ示す。図５～図８は一例であり、通信許可リスト１１９ａ～１１９ｄは必ずしも図５～図８の通りでなくてもよい。

図５に示す通信許可リスト１１９ａは、ルール番号、送信元情報、送信先情報、コマンド種別、データサイズ、データ設定範囲、タイマー条件、フラグ条件、アクション番号の各項目を有する。

図６に示す通信許可リスト１１９ｂは、運用状態、ルール数、インデックス、ルール番号の各項目を有する。

図７に示す通信許可リスト１１９ｃは、アクション番号、タイマー操作、フラグ操作の各項目を有する。

図８に示す通信許可リスト１１９ｄは、運用状態、送信元情報、送信先情報、インデックス先頭番号、検索個数の各項目を有する。

但し、各通信許可リスト１１９ａ～１１９ｄにおける項目は、これらの例に限定されるものではなく、任意に設定可能である。

また、各通信許可リスト１１９ａ～１１９ｄの詳細については、後述する。

[0028] 検知ルール格納部１２４は、検知ルールリスト１２５を格納する。検知ル

ールリスト１２５は、要求通信とそれに応答する応答通信との対応関係が予め登録されている。検知ルールリスト１２５は、要求通信と応答通信との対応関係に基づいて、通信データが正常か異常かを判定するために、要求通信と応答通信との対応関係を記述している。図４に、検知ルールリスト１２５の例を示す。図４は一例であり、検知ルールリストは必ずしも図４の通りでなくてもよい。

[0029] 図４の例においては、検知ルールリスト１２５が、２４個の検知ルール１２６を包含している。

[0030] 各検知ルール１２６には、固有のルール番号が付されている。各検知ルール１２６は、運用状態、ルール番号、送信元情報、送信先情報、要求通信のルール番号（以下、要求ルール番号とする）、応答通信のルール番号（以下、応答ルール番号とする）、コマンド種別、データサイズの上限値、データ設定範囲、コマンド実行の周期の各項目を有する。各検知ルール１２６は、さらに、タイマー現在値、フラグ現在値などの項目を有していてもよい。これらの項目は任意であり、通信データを特定することができる項目であれば、その他の項目でも構わない。

[0031] 図４に示すように、検知ルール１２６においては、運用状態が停止中３０１の場合は、ルール番号１～４のみを許可し、それ以外のルールを許可しない。同様に、運用状態が立上げ３０２の場合は、ルール番号５～８のみを許可し、それ以外のルールを許可しない。運用状態が制御中３０３、立下げ３０４、保守３０５の場合も同様である。このように、検知ルールリスト１２５においては、運用状態ごとに、通信が許可される通信データについて、要求通信と応答通信の対応関係が登録されている。

[0032] また、検知ルールリスト１２５において、要求通信と応答通信の対応関係は、要求ルール番号と応答ルール番号の対で表現する。但し、１つの要求ルール番号に対して、複数の応答ルール番号を設定してもよい。また、逆に、１つの応答ルール番号に対して、複数の要求ルール番号を設定してもよい。

[0033] 具体的に、要求通信と応答通信の対応関係について説明すると、図４の検

知ルールリスト１２５において、停止中３０１のルール番号「１」の検知ルール１２６は、送信元「192.168.0.10」から送信先「192.168.0.50」への「装置状態取得」の要求通信である。当該要求通信に対する応答ルール番号は「２」である。すなわち、当該要求通信に対する応答通信は、停止中３０１のルール番号「２」の検知ルール１２６である。当該応答通信は、送信元「192.168.0.50」から、「装置状態取得」を要求してきた送信先「192.168.0.10」に、装置状態の情報を送信する応答通信である。ここで、ルール番号「１」の検知ルール１２６において、コマンド実行の周期として「１±０．１」が設定されている。従って、「１±０．１」秒の周期で、「装置状態取得」の要求通信が、送信元「192.168.0.10」から送信先「192.168.0.50」へ繰り返し送信されることがわかる。このように、各検知ルール１２６において、自身が要求通信であれば、それに対応する応答通信のルール番号が「応答ルール番号」として登録されており、逆に、自身が応答通信であれば、それに対応する要求通信のルール番号が「要求ルール番号」として登録されている。このように、検知ルールリスト１２５においては、要求通信および応答通信の対応関係が、運用状態ごとに、すべて登録されている。

[0034] さらに具体的な例を挙げると、検知ルールリスト１２５の立上げ３０２のルール番号「５」の要求通信とルール番号「６」の応答通信とが対になっている。これらの検知ルールのコマンドは「装置起動」である。また、ルール番号「７」の要求通信とルール番号「８」の応答通信とが対、ルール番号「９」の要求通信とルール番号「１０」の応答通信とが対、ルール番号「１１」の要求通信とルール番号「１２」の応答通信とが対、・・・のように、要求通信と応答通信との対応関係が定められている。

[0035] このように、検知ルールリスト１２５においては、要求通信と応答通信との対応関係がルール番号で記述されている。すなわち、検知ルールリスト１２５は、要求通信である通信データと、それに対する応答通信である通信データとの対応関係を検知するために、当該対応関係を記述している。

[0036] 通信許可リスト変換部１２３は、検知ルールリスト１２５から、図５～図

８に示す通信許可リスト１１９ａ～１１９ｄを生成する。

[0037] 通信許可リスト変換部１２３は、まず、検知ルールに対応関係が記述された要求通信及び応答通信に対して１以上のフラグを割り当てる。そうして、通信許可リスト１１９ａ，１１９ｃにおいて、要求通信および応答通信ごとに当該フラグに設定すべき値を指定するフラグ操作の内容と、当該フラグに当該値が設定されているかを判定するためのフラグ条件とを対応させて記述する。図５の通信許可リスト１１９ａには、通信データごとに、ルール番号と、アクション番号と、フラグ条件との対応関係が記述されている。また、図７の通信許可リスト１１９ｃには、アクション番号とフラグ操作との対応関係が記述されている。従って、通信許可リスト１１９ａ，１１９ｃを併せて参照することで、それらのアクション番号が共通であるため、フラグ操作の内容とフラグ条件との対応関係が分かる。本実施の形態では、通信許可リスト１１９ａ，１１９ｃを分けているが、これらをまとめて１つの通信許可リストとしてもよい。

さらに、通信許可リスト変換部１２３は、通信許可リストの各通信データを、運用状態、送信元、送信先の優先順、または、運用状態、送信先、送信元の優先順でソートし、ソート後の順位を運用状態ごとにインデックスとして各通信データに付与した通信許可リスト１１９ｂを生成する。

また、通信許可リスト変換部１２３は、運用状態、送信元情報、および、送信先情報に基づいて、参照すべきソート後の通信許可リストの検索範囲を指定する先頭ポインタを示すインデックス先頭番号と、検索範囲の含まれる検索個数とを示す、通信許可リスト１１９ｄを生成する。

[0038] 以下、図４～図８を用いて、本実施の形態に係る通信許可リスト変換部１２３の動作について説明する。

図４に示す検知ルールリスト１２５が与えられると、通信許可リスト変換部１２３は、要求ルール番号と応答ルール番号との対応関係をフラグのＯＮ／ＯＦＦで表現する。

例えば、検知ルールリスト１２５で、ルール番号１の要求通信の応答ルー

ル番号が「２」の場合、通信許可リスト変換部１２３は、ルール番号「１」とルール番号「２」とが対応していると認識する。そのため、ルール番号「１」とルール番号「２」に対して、フラグＦ１を割り当てる。通信許可リスト変換部１２３は、通信許可リスト１１９ａのルール番号「１」のルールが成立した時に、要求通信のアクションとして、図７の通信許可リスト１１９ｃにおいて、アクション番号「１」の「フラグ操作」として、フラグＦ１を「１」に設定するように「Ｆ１＝１」と記述する。これが、フラグのＯＮである。次に、通信許可リスト変換部１２３は、図５の通信許可リスト１１９ａにおいて、ルール番号「２」の通信データにおいて、フラグＦ１が１にセットされたときに当該通信の許可が有効になるように、フラグ条件として、「Ｆ１＝＝１」を記述する。これにより、ルール番号「２」の通信データが判定対象であったとすると、運用状態が「停止中３０１」のときに、送信元情報が「192.168.0.50」で、送信先情報が「192.168.0.10」で、コマンド種別が「装置状態取得」で、且つ、フラグ管理部１０７のフラグ現在値１１５において、フラグＦ１が「１」に設定されているときにのみ、当該通信データの通信許可が有効になる。すなわち、フラグＦ１が「１」に設定されていない状態で、ルール番号「２」の通信データが送信されていた場合には、当該通信データは不正アクセスによるもので、通信を不許可とすべきものである、と判定することができる。

また、通信許可リスト変換部１２３は、通信許可リスト１１９ａのルール番号「２」のルールが成立した時に、応答通信のアクションとして、図７の通信許可リスト１１９ｃにおいて、アクション番号「２」の「フラグ操作」として、フラグＦ１を「０」に設定するように「Ｆ１＝０」と記述する。これが、フラグのＯＦＦである。

このように、通信許可リスト変換部１２３は、通信許可リスト１１９ａ～１１９ｄにおいて、要求ルール番号と応答ルール番号との対応関係をフラグのＯＮ／ＯＦＦで表現している。

[0039] これにより、後述する判定部１０３は、要求通信である通信データの判定

を行う際に、当該通信データが正常であると判定した場合に、当該要求通信のアクションとして、通信許可リストに記述されたフラグ操作の内容に従って、フラグ管理部１０７のフラグの現在値をセットする。ここでは、例えば、フラグＦ１に１を設定して、フラグＦ１をＯＮにする。

判定部１０３は、当該要求通信に対応する応答通信の通信データの判定を行う際に、通信許可リストに記述されたフラグ条件に基づいて、フラグＦ１の現在値が、要求通信のアクションとして更新されたフラグＦ１の値である「１」と一致しているかを判定することで、当該応答通信が先の要求通信に正しく対応しているものかを判定して、当該応答通信が正常であるか否かを判定する。

判定部１０３は、応答通信が正常であると判定した場合には、当該応答通信のアクションとして、通信許可リストに記述されたフラグ操作の内容に従って、フラグ管理部１０７のフラグの現在値をリセットする。すなわち、ここでは、例えば、フラグＦ１に０を設定する。

このように、本実施の形態１においては、判定部１０３が、フラグのＯＮ／ＯＦＦによって、要求通信と応答通信との対応関係を確認することができる。

[0040] また、通信許可リスト変換部１２３は、運用状態ごとに、各運用状態で適用するルール数とルール番号とを示す図６の通信許可リスト１１９ｂを生成する。通信許可リスト変換部１２３は、図６の通信許可リスト１１９ｂを生成する際に、運用状態、送信元情報および送信先情報の優先度に基づいて、運用状態、送信先、送信元の優先順で、通信データをソートする。図６の通信許可リスト１１９ｂでは、図１の通信許可リスト１１９ａの各通信データが、運用状態、送信元、送信先の優先順でソートされ、ソート後の順位が運用状態ごとに、インデックスとして各通信データに付与されている。すなわち、例えば、停止中３０１においては、ルール番号１，３，２，４の順に通信データがソートされ、それぞれに対し、インデックス番号０，１，２，３が付与されている。

[0041] また、通信許可リスト変換部１２３は、送信元情報及び送信先情報から、参照すべき通信許可リスト１１９ｂのインデックス先頭番号と検索個数とを割り出すための、図８の通信許可リスト１１９ｄを生成する。図８の通信許可リスト１１９ｄにおいては、停止中３０１において、送信元情報が「192.168.0.50」で、送信先情報が「192.168.0.10」のときには、インデックス先頭番号が「２」で、検索個数が「２」である。そのため、判定部１０３が、インデックス先頭番号「２」、および、検索個数「２」に基づいて、図６の通信許可リスト１１９ｂを参照すると、ソート後の通信許可リストにおいて、「２」から始めるインデックスが検索範囲の先頭ポインタとなり、当該先頭ポインタを含む検索個数２個が検索範囲であることがわかる。判定部１０３は、このようにして、検索範囲を特定して、当該検索範囲に該当する通信許可リストの通信データと判定対象となる通信データとを比較することで、判定対象となる通信データが正常か異常かを判定する。

[0042] さらに、通信許可リスト変換部１２３は、図５の通信許可リスト１１９ａに記載の通信許可ルール１４１の参照頻度に従って、図６の通信許可リスト１１９ｂのルール番号を並べなおしてもよい。この際、送信元情報及び送信先情報の対応関係を保つように並べ替えを実施する。例えば、保守３０５のルールにおいて、ルール番号１９と２１とは同一送信元・同一送信先のルールであるため、並べ替えてもよいが、ルール番号２１と２３とは送信元・送信先が異なるため、並べ替えてはならない。

[0043] なお、本実施の形態においては、このように、通信許可リスト変換部１２３が、４つの通信許可リスト１１９ａ～１１９ｄを生成すると説明したが、その場合に限らず、このうちの通信許可リスト１１９ａ，１１９ｃのみを生成するようにしてもよい。但し、通信許可リスト１１９ｂ，１１９ｄを生成した場合には、検索範囲を絞ることが可能になるため、判定部１０３の判定処理の処理時間を短縮することができる。

[0044] 図１の説明に戻る。通信部１０２は、ネットワーク４００を介して、監視制御装置２００に接続されている。通信部１０２は、監視制御装置２００か

らネットワーク４００を介して受信データ１１２を受信し、受信した受信データ１１２を判定部１０３に出力する。また、通信部１０２は、判定部１０３から送信データ１１１を受信し、受信した送信データ１１１をネットワーク４００を介して監視制御装置２００に送信する。通信部１０２は、ネットワーク入出力部を構成している。

[0045] 状態管理部１０４は、データ判定装置１０１の運用状態を、状態遷移モデル１１４に基づいて管理する。状態遷移モデル１１４は予め設定され、データ判定装置１０１の記憶領域に記憶される。記憶領域は、例えば後述する図９のメモリ９０３または補助記憶装置９０２から構成される。状態管理部１０４は、操作部１０６からの操作信号１２０、コントローラ３００からの送信データ１１１、監視制御装置２００からの受信データ１１２、および、タイマー１０８からのタイマー現在値のうちの少なくともいずれか１つが入力された場合に、状態遷移モデル１１４に従って、自装置の運用状態を遷移させる。

[0046] また、状態管理部１０４は、判定部１０３によって通信判定データ１１３が通信許可ルール１４１に該当すると判定された場合、すなわち、判定部１０３によって通信判定データ１１３が正常であると判定された場合に、状態遷移モデル１１４に基づいて、自装置の運用状態を遷移させる。また、状態管理部１０４は、判定部１０３により通信判定データ１１３が通信許可ルール１４１に該当しないと判定された場合、すなわち、判定部１０３によって通信判定データ１１３が異常であると判定された場合に、自装置の運用状態を異常状態に遷移させてもよい。なお、状態管理部１０４は、通信判定データ１１３が正常と判定された場合に、運用状態を遷移するのみでもよい。以上のように、状態管理部１０４は、自装置であるデータ判定装置１０１の現在の運用状態１２１を保有する。

[0047] 操作部１０６は、ユーザが操作するボタン、タッチパネル、キーボード、マウスなどから構成される。操作部１０６は、ユーザからの操作入力があったときに、自装置に対する操作を受け付けたことを示す操作信号１２０を出

力する。

[0048] タイマー１０８は、自装置の運用状態が継続する時間を計測する。運用状態ごとに、当該運用状態が継続される時間が予め設定されている。運用状態が遷移したときに、タイマー１０８には、その運用状態の継続時間が設定される。タイマー１０８は、設定された継続時間の値から一定周期(例えば1ms)で一定値を減算していき、値が０になった場合に減算を終了し、タイムアップ信号として、値が「０」のタイマー現在値１１７を出力する。また、タイマー１０８は、判定部１０３および状態管理部１０４からの要求に応じて、現在のタイマー１０８の値を、タイマー現在値１１７として出力する。なお、すべての運用状態に対して継続時間を予め設定しておく必要はなく、特定の運用状態に対してのみ継続時間を設定するようにしてもよい。

[0049] フラグ管理部１０７は、判定部１０３から入力されるフラグ設定値１１６を保持し、判定部１０３および状態管理部１０４に対してフラグ現在値１１５を出力する。

[0050] 判定部１０３は、通信判定データ１１３として、受信データ１１２を通信部１０２から取得するとともに、送信データ１１１をアプリケーション３１０から取得する。また、判定部１０３は、状態管理部１０４が保有する自装置の運用状態を現在の運用状態１２１として取得する。また、判定部１０３は、タイマー１０８からタイマー現在値１１７を取得し、さらに、フラグ管理部１０７からフラグ現在値１１５を取得する。判定部１０３は、現在の運用状態１２１、タイマー現在値１１７、フラグ現在値１１５、および、通信許可リスト格納部１０９が格納する通信許可リスト１１９ａ～１１９ｄを用いて、通信判定データ１１３が、現在の運用状態１２１において、通信許可ルール１４１に該当するか否かを判定する。

[0051] 判定部１０３は、まず、受信データ１１２または送信データ１１１から、送信元情報および送信先情報を抽出する。次に、判定部１０３は、抽出した送信元情報および送信先情報と状態管理部１０４から取得した現在の運用状態１２１とを用いて、図８の通信許可リスト１１９ｄから、インデックス先

頭番号と検索個数とを割り出す。割り出したインデックス先頭番号と検索個数とに基づいて、判定部１０３は、図６の通信許可リスト１１９ｂに基づいて、参照すべき検索範囲を特定し、当該検索範囲に該当するルール番号を抽出する。例えば、運用状態が停止中３０１の状態で、送信元情報が192.168.0.50で、送信先情報が192.168.0.10の通信判定データ１１３を判定する場合、判定部１０３は、図８の通信許可リスト１１９ｄから、インデックス先頭番号「２」を抽出するとともに、検索個数「２」を抽出する。そうして、判定部１０３は、図６の通信許可リスト１１９ｂの中から、運用状態が停止中３０１で、インデックス番号が「２」から始まるルールのルール番号が「２」であることを抽出し、さらに、検索個数「２」の情報に基づいて、ルール番号「２］とその隣のルール番号「４」とを抽出する。こうして、判定部１０３は、通信判定データ１１３が、図５の通信許可リスト１１９ａのルール番号「２」または「４」のいずれかの通信許可ルール１４１に該当するか否かを判定する。

[0052] 判定部１０３は、このようにして、通信判定データ１１３が通信許可ルール１４１に該当するか否かを判定する。判定部１０３は、通信判定データ１１３が通信許可ルール１４１に該当すると判定した場合、通信判定データ１１３が正常であると判定するとともに、該当したルール番号の通信許可ルール１４１に記載されたアクション番号に対応するアクションを実行する。例えば、通信判定データ１１３がルール番号９の通信許可ルール１４１が該当した場合、図５の通信許可リスト１１９ａのルール番号９の通信許可ルール１４１から、アクション番号「９」を抽出する。そうして、判定部１０３は、図７の通信許可リスト１１９ｃのアクション番号９に記載のアクションを実行する。すなわち、判定部１０３は、図７の通信許可リスト１１９ｃのアクション番号９の「タイマー操作」の内容に基づいて、タイマー１０８のタイマー値Ｔ２に「０」を代入し、アクション番号９の「フラグ操作」の内容に基づいて、フラグ管理部１０７のフラグＦ５に「１」をセットする。

[0053] 一方、判定部１０３は、通信判定データ１１３が通信許可ルール１４１に

該当しないと判定した場合、通信判定データ１１３が異常であると判定し、コントローラ３００と監視制御装置２００との間の通信を遮断する。また、判定部１０３は、警報部１１０に対して、通信判定データ１１３が異常であることを示す判定結果１２２を出力する。

[0054] 警報部１１０は、判定部１０３から、通信判定データ１１３が異常であることを示す判定結果１２２が入力された場合に、ユーザに対して異常を通知するための警報を出力する。すなわち、警報部１１０は、判定結果１２２が異常の場合に、警報を発する。警報部１１０が発する警報は、視覚的な警報でもよく、あるいは、聴覚的な警報であってもよい。視覚的な警報の場合には、警報部１１０を例えばランプから構成しておき、当該ランプの点灯または点滅動作を「警報」としてもよい。また、警報が聴覚的な警報の場合には、警報部１１０をブザーまたはスピーカから構成しておき、ブザー音の発声または音声メッセージの発声を「警報」としてもよい。また、「警報」として、警報部１１０が、例えばネットワーク４００を経由して、別のサーバに警報信号を送信するようにしてもよい。また、警報部１１０を、後述する図９のディスプレイ９０８から構成し、判定部１０３の判定結果１２２を表示画面に表示するようにしてもよい。この場合、判定結果１２２が正常であった場合には、表示画面において「判定結果１２２が正常」の旨を示す表示を行う。一方、判定結果１２２が異常であった場合には、表示画面において「判定結果１２２が異常」の旨を示す表示を行うとともに、警報を発生させる。

[0055] 次に、図２を用いて、図１のデータ判定装置１０１の変形例について説明する。図２は、図１のデータ判定装置１０１とは異なる動作を行うデータ判定装置１０１ａの構成について示している。

[0056] 図１に示すデータ判定装置１０１では、判定部１０３が通信判定データ１１３を判定した後に、受信データ１１２あるいは送信データ１１１を通信する構成を示した。

一方、図２に示すデータ判定装置１０１ａにおいては、アプリケーション

３１０と監視制御装置２００とが、データ判定装置１０１ａを介さずに、送信データ１１１および受信データ１１２の通信を直接行っている。当該通信は、ネットワーク４００を用いて行ってもよく、あるいは、専用の回線を用いて行ってもよい。このとき、データ判定装置１０１ａは、通信部１０２を用いて、監視制御装置２００とアプリケーション３１０との通信をキャプチャして通信判定データ１１３を取得し、取得した通信判定データ１１３の判定を行う。しかしながら、図２のデータ判定装置１０１ａでは、判定部１０３による判定結果１２２が異常の場合においても、判定部１０３がアプリケーション３１０と監視制御装置２００との間の通信を遮断することはできない。一方、警報部１１０により発せられた警報により、ユーザに異常を通知することはできるので、異常の通知を受けたユーザが、第三者による不正な攻撃に対する何らかの対処を行うことができる。

なお、図２のデータ判定装置１０１ａの他の構成および動作は、図１のデータ判定装置１０１と同じであるため、ここでは、その説明を省略する。

[0057] 次に、図９を用いて、本実施の形態に係るデータ判定装置１０１のハードウェア構成の一例について説明する。

[0058] 図９に示すように、データ判定装置１０１は、例えばコンピュータから構成される。

データ判定装置１０１を構成するコンピュータは、プロセッサ９０１、補助記憶装置９０２、メモリ９０３、通信装置９０４、入力インタフェース９０５、ディスプレイインタフェース９０６といったハードウェアを備える。

プロセッサ９０１は、信号線９１０を介して、他のハードウェア９０２～９０６と接続され、これら他のハードウェア９０２～９０６を制御する。

入力インタフェース９０５は、入力装置９０７に接続されている。

ディスプレイインタフェース９０６は、ディスプレイ９０８に接続されている。

[0059] データ判定装置１０１における入力部である通信部１０２および操作部１０６は、入力装置９０７および入力インタフェース９０５である。また、デ

ータ判定装置１０１の出力部は、ディスプレイ９０８およびディスプレイインタフェース９０６である。また、図９では、図示を省略しているが、データ判定装置１０１には、警報部１１０を構成するハードウェアも設けられている。

[0060] プロセッサ９０１は、プロセッシングを行うＩＣ（Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）から構成される。プロセッサ９０１は、例えば、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）、ＤＳＰ（Ｄｉｇｉｔａｌ Ｓｉｇｎａｌ Ｐｒｏｃｅｓｓｏｒ）、ＧＰＵ（Ｇｒａｐｈｉｃｓ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）である。

[0061] 補助記憶装置９０２は、例えば、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）、フラッシュメモリ、ＨＤＤ（Ｈａｒｄ Ｄｉｓｋ Ｄｒｉｖｅ）から構成される。

[0062] メモリ９０３は、例えば、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）から構成される。

[0063] 通信装置９０４は、データを受信するレシーバー９０４１及びデータを送信するトランスミッター９０４２を含む。通信装置９０４は、例えば、通信チップ又はＮＩＣ（Ｎｅｔｗｏｒｋ Ｉｎｔｅｒｆａｃｅ Ｃａｒｄ）から構成される。

[0064] 入力インタフェース９０５は、入力装置９０７のケーブル９１１が接続されるポートである。入力インタフェース９０５は、例えば、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ Ｓｅｒｉａｌ Ｂｕｓ）端子から構成される。

[0065] ディスプレイインタフェース９０６は、ディスプレイ９０８のケーブル９１２が接続されるポートである。ディスプレイインタフェース９０６は、例えば、ＵＳＢ端子又はＨＤＭＩ（登録商標）（Ｈｉｇｈ Ｄｅｆｉｎｉｔｉｏｎ Ｍｕｌｔｉｍｅｄｉａ Ｉｎｔｅｒｆａｃｅ）端子から構成される。

[0066] 入力装置９０７は、例えば、マウス、キーボード又はタッチパネルから構成される。

[0067] ディスプレイ９０８は、例えば、ＬＣＤ（Ｌｉｑｕｉｄ Ｃｒｙｓｔａｌ

Ｄｉｓｐｌａｙ）から構成される。

[0068] 補助記憶装置９０２には、図１に示す状態管理部１０４、判定部１０３、警報部１１０、フラグ管理部１０７、タイマー１０８、通信許可リスト変換部１２３（以下、状態管理部１０４、判定部１０３、警報部１１０、フラグ管理部１０７、タイマー１０８、通信許可リスト変換部１２３をまとめて「部」と表記する）の機能を実現するプログラムが記憶されている。上述したデータ判定装置１０１が備える「部」の機能を実現するプログラムは、データ判定プログラムとも称される。「部」の機能を実現するプログラムは、１つのプログラムであってもよいし、複数のプログラムから構成されていてもよい。当該プログラムは、メモリ９０３にロードされ、プロセッサ９０１に読み込まれ、プロセッサ９０１によって実行される。

[0069] 更に、補助記憶装置９０２には、ＯＳ（Ｏｐｅｒａｔｉｎｇ Ｓｙｓｔｅｍ）も記憶されている。そして、ＯＳの少なくとも一部がメモリ９０３にロードされ、プロセッサ９０１はＯＳを実行しながら、「部」の機能を実現するプログラムを実行する。

[0070] 図９では、１つのプロセッサ９０１が図示されているが、データ判定装置１０１が複数のプロセッサ９０１を備えていてもよい。そして、複数のプロセッサ９０１が「部」の機能を実現するプログラムを連携して実行してもよい。

[0071] また、「部」の処理の結果を示す情報、データ、信号値、変数値などが、メモリ９０３、補助記憶装置９０２、又は、プロセッサ９０１内のレジスタ又はキャッシュメモリにファイルとして記憶される。

[0072] また、「部」を「サーキットリー」で提供してもよい。

[0073] また、「部」を「回路」又は「工程」又は「手順」又は「処理」に読み替えてもよい。また、「処理」を「回路」又は「工程」又は「手順」又は「部」に読み替えてもよい。

[0074] 「回路」及び「サーキットリー」は、プロセッサ９０１だけでなく、ロジックＩＣ又はＧＡ（Ｇａｔｅ Ａｒｒａｙ）又はＡＳＩＣ（Ａｐｐｌｉｃａ

ｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）又はＦＰＧＡ（Ｆｉｅｌｄ－Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）といった他の種類の処理回路をも包含する概念である。

[0075] なお、プログラムプロダクトと称されるものは、「部」として説明している機能を実現するプログラムが記録された記憶媒体、記憶装置などであり、見た目の形式に関わらず、コンピュータ読み取り可能なプログラムをロードしているものである。

[0076] 次に、図１０を用いて、本実施の形態に係るデータ判定装置１０１のデータ判定方法であるデータ判定処理Ｓ１００について説明する。

[0077] 上述したように、データ判定装置１０１は、状態遷移モデル１１４を記憶する状態遷移モデル記憶部１０５と、通信許可ルール１４１を通信許可リスト１１９ａ～１１９ｄとして格納する通信許可リスト格納部１０９とを備える。

[0078] 図１０に示すように、まず、ステップＳ１０１の状態管理処理において、状態管理部１０４は、状態遷移モデル１１４に基づいて、自装置の運用状態を保有する状態管理処理Ｓ１０１を実行する。すなわち、状態管理部１０４は、操作信号１２０、受信データ１１２、送信データ１１１、フラグ管理部１０７からのフラグ現在値１１５、タイマー１０８からのタイマー現在値１１７のいずれか１以上に基づいて、状態遷移モデル１１４に従って自装置の運用状態を遷移させ、最新の運用状態を保有する。

[0079] 次に、ステップＳ１１０の通信処理において、通信部１０２および判定部１０３は、通信判定データ１１３を取得する。具体的には、通信部１０２が受信データ１１２を取得し、判定部１０３が送信データ１１１を取得する。

[0080] 次に、ステップＳ１２０の判定処理において、判定部１０３は、ステップＳ１１０の通信処理により取得された受信データ１１２を通信部１０２から取得するとともに、ステップＳ１０１の状態管理処理により保有された自装置の運用状態を現在の運用状態１２１として状態管理部１０４から取得する。また、判定部１０３は、タイマー１０８よりタイマー現在値１１７を取得

し、フラグ管理部１０７よりフラグ現在値１１５を取得する。判定部１０３は、現在の運用状態１２１と、タイマー現在値１１７と、フラグ現在値１１５と、通信許可リスト格納部１０９に格納されている通信許可リスト１１９ａ～１１９ｄとを用いて、通信判定データ１１３が現在の運用状態１２１において通信許可ルール１４１に該当するか否かを判定する。判定部１０３は、判定結果１２２を出力する。

[0081] 次に、ステップＳ１３０の分岐処理において、判定結果１２２が正常か否かを判定する。判定結果１２２が正常、すなわち、通信判定データ１１３が通信許可ルール１４１に該当する場合、ステップＳ１４０の正常処理に進む。一方、判定結果１２２が異常、すなわち、通信判定データ１１３が通信許可ルール１４１に該当しない場合、ステップＳ１５０の異常処理に進む。

[0082] ステップＳ１４０の正常処理において、状態管理部１０４は、取得した通信判定データ１１３、タイマー現在値１１７、フラグ現在値１１５、操作信号１２０のいずれか１以上を用いて、状態遷移モデル１１４に従って、自装置の運用状態を遷移させる。

[0083] 一方、ステップＳ１５０の異常処理において、状態管理部１０４は、自装置の運用状態を異常状態に遷移させる。また、警報部１１０は、判定部１０３からの判定結果１２２に基づいて警報を通知する。

[0084] 次に、図１１を用いて、図１０のステップＳ１２０の判定部１０３による判定処理について説明する。

[0085] まず、ステップＳ１２１において、判定部１０３は、受信データ１１２あるいは送信データ１１１を通信判定データ１１３として取得し、取得した通信判定データ１１３を解析する。判定部１０３は、当該解析により、通信判定データ１１３の中から、判定に必要な要素を抽出する。抽出される要素は、図５の通信許可リスト１１９ａに記載されている項目であり、すなわち、送信元情報、送信先情報、コマンド種別等である。

[0086] 次に、ステップＳ１２２において、判定部１０３は、状態管理部１０４から現在の運用状態１２１を取得する。また、判定部１０３は、通信許可リス

ト格納部１０９から通信許可リスト１１９ａ～１１９ｄを取得する。

[0087] ステップＳ１２３において、判定部１０３は、ステップＳ１２２で取得した現在の運用状態１２１と通信許可リスト１１９ａ～１１９ｄとに基づいて、通信判定データ１１３が現在の運用状態１２１において許可されている通信データであるか、すなわち、通信許可ルール１４１に該当するか否かを判定する。判定の結果、通信判定データ１１３が通信許可ルール１４１に該当すれば、ステップＳ１２４に進む。一方、通信判定データ１１３が通信許可ルール１４１に該当しない、すなわち、通信判定データ１１３が許可されていない通信であれば、ステップＳ１２５に進む。

[0088] ステップＳ１２４において、判定部１０３は、「正常」を示す判定結果１２２を出力する。また、該当する通信許可ルール１４１に記載されたアクション番号に対応するアクションを実行する。判定部１０３は、当該アクション番号に基づいて、図７の通信許可リスト１１９ｃを参照して、例えば、フラグ管理部１０７に所定のフラグをセットする、あるいは、タイマー１０８に所定の値をセットする。

[0089] 一方、ステップＳ１２５においては、判定部１０３は、「異常」を示す判定結果１２２を警報部１１０に出力するとともに、通信判定データ１１３の通信を遮断する。あるいは、判定部１０３は、「異常」を示す判定結果１２２を出力するだけで、通信判定データ１１３の通信を遮断しなくてもよい。

[0090] 次に、図１２を用いて、本発明における通信許可リスト変換部１２３の動作について説明する。

[0091] まず、ステップＳ２０１において、通信許可リスト変換部１２３は、検知ルール格納部１２４から、図４の検知ルールリスト１２５を取得する。通信許可リスト変換部１２３は、検知ルールリスト１２５から、各ルールごとの要求と応答との対応関係を解析する。解析結果は以下の３通りとなる。

[0092] Ａ） 要求と応答とが１：１対応

Ｂ） 要求と応答とが０：ｍ対応（ｍ≧１）

Ｃ） 要求と応答とが１：ｎ対応（ｎ≧２）

[0093] Ａ）は、１つの要求通信に対して、１つの応答通信が対応する関係である。例えば、ＴＣＰを用いたＲｅａｄ通信及びＷｒｉｔｅ通信が該当する。

[0094] Ｂ）は、要求通信に対応して複数の応答通信が存在するが、応答通信間に依存関係がない関係である。例えば、ブロードキャストによるキープアライブ通信などが該当する。

[0095] Ｃ）は、１つの要求通信に対して、複数の応答通信の候補があり、どれか１つが成立すれば、他は無効になる関係である。例えば、ＵＤＰを用いたコネクション型の通信が該当する。

[0096] ステップＳ２０１の解析において、解析結果がＡ）の場合はステップＳ２０２に進み、解析結果がＢ）の場合はステップＳ２０５に進み、解析結果がＣ）の場合はステップＳ２０８に進む。以下に、それぞれの場合について説明する。

[0097] 解析結果がＡ）の場合、まず、ステップＳ２０２において、図４の検知ルールリスト１２５の要求ルールのルール番号ごとに１つのフラグを定義し、当該ルール番号のアクション番号に対応する図７の通信許可リスト１１９ｃのアクションのフラグ操作に、当該フラグの設定操作を追記する。次に、ステップＳ２０３において、図５の通信許可リスト１１９ａの応答ルールに、ステップＳ２０２で割り当てたフラグがセットされているかを判定するフラグ条件を追記する。次に、ステップＳ２０４において、応答ルールのアクション番号に対応する通信許可リスト１１９ｃのフラグ操作にステップＳ２０２で割り当てたフラグのリセット操作を追記する。

[0098] 解析結果がＢ）の場合、まず、ステップＳ２０５において、図４の検知ルールリスト１２５の要求ルールのルール番号ごとにｍ個のフラグを定義し、当該ルール番号のアクション番号に対応する図７の通信許可リスト１１９ｃのアクションのフラグ操作に、当該フラグの設定操作を追記する。次に、ステップＳ２０６において、図５の通信許可リスト１１９ａの応答ルールに、ステップＳ２０５で割り当てたｍ個のフラグを１つずつ割り当て、当該フラグがセットされているかを判定するフラグ条件を追記する。次に、ステップ

Ｓ２０７において、応答ルールのアクション番号に対応する通信許可リスト１１９ｃのフラグ操作にステップＳ２０６で割り当てたフラグのリセット操作を追記する。

[0099] 解析結果がＣ）の場合、まず、ステップＳ２０８において、図４の検知ルールリスト１２５の要求ルールのルール番号ごとに１つのフラグを定義し、当該ルール番号のアクション番号に対応する図７の通信許可リスト１１９ｃのアクションのフラグ操作に、当該フラグの設定操作を追記する。次に、ステップＳ２０９において、図５の通信許可リスト１１９ａの全ての応答ルールに、ステップＳ２０８で割り当てたフラグがセットされているかを判定するフラグ条件を追記する。次に、ステップＳ２１０において、応答ルールのアクション番号に対応する通信許可リスト１１９ｃのフラグ操作にステップＳ２０８で割り当てたフラグのリセット操作を追記する。

[0100] 以上で、本実施の形態に係るデータ判定装置１０１のデータ判定方法及びデータ判定処理Ｓ１００についての説明を終わる。

[0101] 以上のように、本実施の形態に係るデータ判定装置１０１は、以下の構成を有する。

（Ａ）自装置に対して設定されるフラグの現在値を格納するフラグ管理部１０７。

（Ｂ）複数の運用状態間を遷移する自装置の現在の運用状態１２１を格納するとともに、外部からの入力信号としての例えば通知データ、および、フラグ管理部１０７が格納するフラグの現在値１１５のうちのいずれか１以上に応じて、運用状態間の遷移が定義されている状態遷移モデル１１４に従って、自装置の運用状態を遷移させる状態管理部１０４。

（Ｃ）要求通信を構成する通信データと要求通信に対する応答通信を構成する通信データとの対応関係を記述した検知ルール１２５を、運用状態ごとに通信が許可された通信データを予め登録する通信許可リスト１１９ａ，１１９ｃに変換する、通信許可リスト変換部１２３。

（Ｄ）状態管理部１０４が格納する自装置の現在の運用状態１２１と、通

信許可リスト１１９ａ，１１９ｃと、フラグ管理部１０７が格納するフラグの現在値１１５とのいずれか１以上を用いて、自装置に入力された通信データ１１３が、通信許可リスト１１９ａ，１１９ｃに登録された現在の運用状態１２１における通信データであるか否かを判定することで、自装置に入力された通信データ１１３が正常か異常かを判定する判定部１０３。

[0102] 通信許可リスト変換部１２３は、検知ルールを通信許可リスト１１９ａ，１１９ｃに変換するときに、検知ルールに対応関係が記述された要求通信及び応答通信に対して１以上のフラグを割り当て、当該フラグに対して設定すべき値を指定したフラグ操作の内容と、前記フラグに当該値が設定されているかを判定するためのフラグ条件との対応関係を、前記通信許可リストに記述する。

[0103] 判定部１０３は、要求通信である通信データの判定を行い、当該通信データが正常であると判定した場合に、当該要求通信のアクションとして、通信許可リストに記述されたフラグ操作の内容に基づいて、フラグ管理部１０７のフラグの現在値を更新する。ここでは、例えば、フラグＦ１に１を設定する。

判定部１０３は、当該要求通信に対応する応答通信の通信データの判定を行う際に、通信許可リストに記述されたフラグ条件に基づいて、フラグＦ１の現在値が、要求通信のアクションとして更新されたフラグＦ１の値である「１」と一致しているかを判定することで、当該応答通信が先の要求通信に正しく対応しているものかを判定して、当該応答通信が正常であるか否かを判定する。

判定部１０３は、応答通信が正常であると判定した場合には、当該応答通信のアクションとして、通信許可リストに記述されたフラグ操作の内容に従って、フラグ管理部１０７のフラグの現在値をリセットする。すなわち、ここでは、例えば、フラグＦ１に０を設定する。

このように、判定部１０３は、データの判定の際に、フラグの現在値のＯＮ／ＯＦＦによって、要求と応答との対応関係を確認し、要求と応答との対

応関係が取れない場合に、通信データが不正な攻撃よるものであると判定するようにしたので、攻撃の検知を、より高度に行うことができる。

また、判定部１０３は、通信データが異常であると判定した場合、当該通信データの通信を遮断する。

[0104] 以上の構成により、本実施の形態に係るデータ判定装置においては、通信許可リストに正常な通信を定義する際に、要求通信と応答通信との対応関係を記述するようにしたので、組み合わせ爆発を起こさずに、すべての通信データを記述することができる。また、要求通信と応答通信との対応関係をフラグのセット／リセットで判定できるようにし、要求通信と応答通信との対応関係も考慮して通信データが正常か異常かを判定するようにしたので、第三者によってサーバが乗っ取られて当該サーバからサイバー攻撃された場合においても、通信データが不正であることを検知することができる。また、要求通信と応答通信との対応関係を定義することにより、増大する検知ルールの検索を高速に行うことができる。

[0105] また、通信許可リスト変換部１２３は、さらに、通信許可リスト１１９ｂ，１１９ｄを生成してもよい。

すなわち、通信許可リスト変換部１２３は、通信許可リストの通信データを、運用状態、送信元、送信先の優先順、または、運用状態、送信先、送信元の優先順でソートし、ソート後の順位をインデックスとして各前記通信データに付与した、通信許可リスト１１９ｂを生成する。

また、通信許可リスト変換部１２３は、運用状態、送信元の情報、および、送信先の情報に基づいて参照すべきソート後の通信許可リスト１１９ｂの検索範囲を指定する先頭ポインタを示すインデックス先頭番号と検索個数とを示す通信許可リスト１１９ｄを生成する。

このとき、判定部１０３は、状態管理部１０４から自装置の現在の運用状態１２１を取得するとともに、判定対象となる通信データ１１３から送信元の情報および送信先の情報を取得して、現在の運用状態１２１、送信元の情報、および、送信先の情報に基づいて、通信許可リスト１１９ｄから、イン

デックス先頭番号と検索個数とを抽出して、抽出したインデックス先頭番号と検索個数とに基づいてソート後の通信許可リスト１１９ｂおける参照すべき検索範囲を特定して、当該検索範囲に該当する通信許可リスト１１９ａの通信データと判定対象となる通信データ１１３とを比較することで、判定対象となる通信データ１１３が正常か異常かを判定する。

[0106] また、必要に応じて、本実施の形態に係るデータ判定装置１０１は、さらに、以下の構成を有していてもよい。

（Ｅ）複数の運用状態間を遷移する自装置の現在の運用状態の継続時間を計測するタイマー１０８。

（Ｆ）通信許可リスト１１９ａ～１１９ｄを格納する通信許可リスト格納部１０９。

（Ｇ）判定部１０３が通信データが異常であると判定した場合に、警報を発する警報部１１０。

（Ｈ）検知ルールを格納する検知ルール格納部１２４。

[0107] 本実施の形態１によれば、上述したように、判定部１０３が、フラグの現在値のＯＮ／ＯＦＦによって、要求と応答との対応関係を確認し、要求と応答との対応関係が取れない場合に、通信データが不正な攻撃よるものであると検知することができる。その一例を、図１３を用いて説明する。図１３は、BACnet通信を例に説明している。図１３における装置１および装置２は、コントローラ３００および監視制御装置２００に相当する。図３においては、データ判定装置１０１の図示は省略されている。

[0108] 図１３において、（Ａ）が正常時のシーケンスであり、（Ｂ）が攻撃時のシーケンスであるとする。（Ａ）、（Ｂ）において、通信データＴ１の要求と通信データＴ２の応答とが対応しており、通信データＴ３、Ｔ５，Ｔ７の要求と通信データＴ４，Ｔ６の応答とが対応している。各対応に対してフラグが割り当てられている。

[0109] （Ａ）では、装置１からの“Confirmed Request”要求に対して、装置２が“Complex Ack”もしくは“Abort”を返すものとする。

[0110] すなわち、図１３の（Ａ）では、通信データＴ１の“Confirmed Request”要求に対して、通信データＴ２の“Abort”が返され、通信データＴ３の“Confirmed Request”要求に対して、通信データＴ４の“Complex Ack”が返されている。

[0111] また、通信データＴ４のように、装置２が装置１に対して“Complex Ack”を応答した場合は、装置１は“Segment Ack”を返し、このやりとりを２回行って、通信を終了するものとする。すなわち、装置２が通信データＴ４の“Complex Ack”を応答した場合は、装置１は、通信データＴ５の“Segment Ack”を返す。これが１回目のやりとりである。その後、装置２が、再び、通信データＴ６の“Complex Ack”を応答し、装置１が、通信データＴ７の“Segment Ack”を返す。これが２回目のやりとりである。こうして、通信を終了する。

[0112] 以上が、正常時のシーケンス（Ａ）である。このとき、データ判定装置１０１の判定部１０３は、フラグの値に基づいて、要求と応答との対応関係が成立しているかを判定している。

[0113] これに対し、（Ｂ）においては、装置２に不正プログラムがインストールされた場合を示している。（Ｂ）における符号Ｔ３～Ｔ６は、（Ａ）における符号Ｔ３～Ｔ６に対応している。（Ｂ）においては、装置２の不正プログラムにより、装置２から装置１への２回目の“Complex Ack”の送信の前に、装置２から“Abort”を流すという攻撃が行われたものとする。この場合、データ判定装置１０１の判定部１０３は、装置２から装置１への送信が“Complex Ack”でなく、フラグの値が一致しないことから、要求通信と応答通信の対応関係が成立していないと判定して、通信が異常であると判断し、これ以上の通信を行わない。仮に、装置２上の正規のプログラムが、その後に、“Complex Ack”を流しても、通信を完結することはできない。

なお、装置２からの“Abort”自体は正常な通信であるため、従来のデータ判定装置であれば、このようなケースを見逃す可能性があったが、本実施の形態１によるデータ判定装置では、要求通信と応答通信の対応関係をデータ

判定に用いているため、このような、装置２が第三者に乗っ取られたようなケースにおいても、第三者からの攻撃を検知することができる。

[0114] さらに、本実施の形態１に係るデータ判定装置によれば、検知ルールが増大しても、送信元・送信先でインデックスを作成し、検索範囲を絞りこんでいるため、通信許可リストと判定対象データとのマッチングを高速に行うことができる。

[0115] さらに、本実施の形態１に係るデータ判定装置によれば、頻度による再ソート以外はすべて事前計算で実行できるため、判定処理に影響を与えずに実現できる。

符号の説明

[0116] １０１　データ判定装置、１０２　通信部、１０３　判定部、１０４　状態管理部、１０５　状態遷移モデル記憶部、１０６　操作部、１０７　フラグ管理部、１０８　タイマー、１０９　通信許可リスト格納部、１１０　警報部、１１１　送信データ、１１２　受信データ、１１３　通信判定データ、１１４　状態遷移モデル、１１５　フラグ現在値、１１６　フラグ設定値、１１７　タイマー現在値、１１８　タイマー設定値、１１９ａ，１１９ｂ，１１９ｃ，１１９ｄ　通信許可リスト、２００　監視制御装置、３００　コントローラ、３１０　アプリケーション。

請求の範囲

[請求項1] 自装置に対して設定されるフラグの現在値を格納するフラグ管理部と、

複数の運用状態間を遷移する自装置の現在の運用状態を格納するとともに、外部からの入力信号、および、前記フラグ管理部が格納する前記フラグの現在値のうちのいずれか１以上に応じて、前記運用状態間の遷移が定義されている状態遷移モデルに従って、前記自装置の運用状態を遷移させる状態管理部と、

要求通信を構成する通信データと前記要求通信に対する応答通信を構成する通信データとの対応関係を記述した検知ルールを、前記運用状態ごとに通信が許可された通信データを予め登録する通信許可リストに変換する、通信許可リスト変換部と、

前記状態管理部が格納する前記自装置の前記現在の運用状態と、前記通信許可リストと、前記フラグ管理部が格納する前記フラグの現在値とのいずれか１以上を用いて、前記自装置に入力された通信データが、前記通信許可リストに登録された前記現在の運用状態における通信データであるか否かを判定することで、前記自装置に入力された前記通信データが正常か異常かを判定する判定部と

を備え、

前記通信許可リスト変換部は、前記検知ルールを前記通信許可リストに変換するときに、前記検知ルールに対応関係が記述された前記要求通信及び前記応答通信に対してフラグを割り当て、当該フラグに対する設定値を指定したフラグ操作の内容と、前記フラグに前記設定値が設定されているかを判定するためのフラグ条件とを対応させて、前記通信許可リストに記述し、

前記判定部は、前記要求通信の通信データが正常であると判定した後に、前記フラグ操作の内容に従って、前記フラグに前記設定値をセットし、前記要求通信に対する前記応答通信の通信データが正常であ

るか否かを判定する場合に、前記フラグ条件に基づいて前記フラグに前記設定値が設定されているか否かを判定し、前記設定値が設定されていた場合に、前記応答通信の通信データを正常であると判定して、前記フラグをリセットする、

データ判定装置。

[請求項2] 前記判定部が前記要求通信の通信データまたは前記応答通信の通信データが異常であると判定した場合に、警報を発する警報部を備えた、

請求項１に記載のデータ判定装置。

[請求項3] 前記自装置の前記現在の運用状態が継続している継続時間を計測するタイマーを備え、

前記状態管理部は、外部からの入力信号、前記タイマーのタイマー現在値、および、前記フラグ管理部が格納する前記フラグの現在値のうちのいずれか１以上に応じて、前記状態遷移モデルに従って、前記自装置の運用状態を遷移させ、

前記判定部は、前記状態管理部が格納する前記自装置の前記現在の運用状態と、前記通信許可リストと、前記タイマーからの前記タイマー現在値と、前記フラグ管理部が格納する前記フラグの現在値とのいずれか１以上を用いて、前記自装置に入力された通信データが、前記通信許可リストに登録された前記現在の運用状態における通信データであるか否かを判定する、

請求項１または２に記載のデータ判定装置。

[請求項4] 前記通信許可リスト変換部は、

前記通信許可リストの前記通信データを、運用状態、送信元、送信先の優先順、または、運用状態、送信先、送信元の優先順でソートし、前記ソート後の順位をインデックスとして各前記通信データに付与するとともに、

前記運用状態、前記送信元の情報、および、前記送信先の情報に基

づいて参照すべき前記ソート後の前記通信許可リストの検索範囲を指定する先頭ポインタを示すインデックス先頭番号と検索個数とを示すリストを作成し、

前記判定部は、

前記状態管理部から前記自装置の前記現在の運用状態を取得するとともに、判定対象となる前記通信データから送信元の情報および送信先の情報を取得して、前記現在の運用状態、前記送信元の情報、および、前記送信先の情報に基づいて、前記リストから、前記インデックス先頭番号と前記検索個数とを抽出して、前記インデックス先頭番号と前記検索個数とに基づいて前記ソート後の前記通信許可リストおける参照すべき検索範囲を特定して、前記検索範囲に該当する前記通信許可リストの前記通信データと前記判定対象となる前記通信データとを比較することで、前記判定対象となる前記通信データが正常か異常かを判定する、

請求項１から３までのいずれか１項に記載のデータ判定装置。

[請求項5] 前記状態遷移モデルは、さらに前記判定部が出力する判定結果に応じて前記運用状態が遷移することを定義する、

請求項１から４までのいずれか１項に記載のデータ判定装置。

[請求項6] 前記判定部が前記通信データが異常であると判定した場合に、前記通信データの通信を遮断する遮断部

を備えた請求項１から５までのいずれか１項に記載のデータ判定装置。

[請求項7] 自装置に対して設定されるフラグの現在値を格納するフラグ管理ステップと、

外部からの入力信号、および、前記フラグ管理ステップで格納された前記フラグの現在値のうちのいずれか１以上に応じて、前記自装置の複数の運用状態間の遷移が定義されている状態遷移モデルに従って、前記自装置の運用状態を遷移させ、前記自装置の現在の運用状態を

格納する状態管理ステップと、

要求通信を構成する通信データと前記要求通信に対する応答通信を構成する通信データとの対応関係を記述した検知ルールを、前記運用状態ごとに通信が許可された通信データを予め登録する通信許可リストに変換する、通信許可リスト変換ステップと、

前記状態管理ステップで格納された前記自装置の前記現在の運用状態と、前記通信許可リストと、前記フラグ管理ステップで格納された前記フラグの現在値とのいずれか1以上を用いて、前記自装置に入力された通信データが、前記通信許可リストに登録された前記現在の運用状態における通信データであるか否かを判定することで、前記自装置に入力された前記通信データが正常か異常かを判定する判定ステップと

を備え、

前記通信許可リスト変換ステップは、前記検知ルールを前記通信許可リストに変換するときに、前記検知ルールに対応関係が記述された前記要求通信及び前記応答通信に対してフラグを割り当て、当該フラグに対する設定値を指定したフラグ操作の内容と、前記フラグに前記設定値が設定されているかを判定するためのフラグ条件とを対応させて、前記通信許可リストに記述し、

前記判定ステップは、前記要求通信の通信データが正常であると判定した後に、前記フラグ操作の内容に従って、前記フラグに前記設定値をセットし、前記要求通信に対する前記応答通信の通信データが正常であるか否かを判定する場合に、前記フラグ条件に基づいて前記フラグに前記設定値が設定されているか否かを判定し、前記設定値が設定されていた場合に、前記応答通信の通信データを正常であると判定して、前記フラグをリセットする、

データ判定方法。

[請求項8] データの判定を行うために、コンピュータを、

自装置に対して設定されるフラグの現在値を格納するフラグ管理部と、

複数の運用状態間を遷移する自装置の現在の運用状態を格納するとともに、外部からの入力信号、および、前記フラグ管理部が格納する前記フラグの現在値のうちのいずれか１以上に応じて、前記運用状態間の遷移が定義されている状態遷移モデルに従って、前記自装置の運用状態を遷移させる状態管理部と、

要求通信を構成する通信データと前記要求通信に対する応答通信を構成する通信データとの対応関係を記述した検知ルールを、前記運用状態ごとに通信が許可された通信データを予め登録する通信許可リストに変換する、通信許可リスト変換部と、

前記状態管理部が格納する前記自装置の前記現在の運用状態と、前記通信許可リストと、前記フラグ管理部が格納する前記フラグの現在値とのいずれか１以上を用いて、前記自装置に入力された通信データが、前記通信許可リストに登録された前記現在の運用状態における通信データであるか否かを判定することで、前記自装置に入力された前記通信データが正常か異常かを判定する判定部と

して機能させるためのデータ判定プログラムであって、

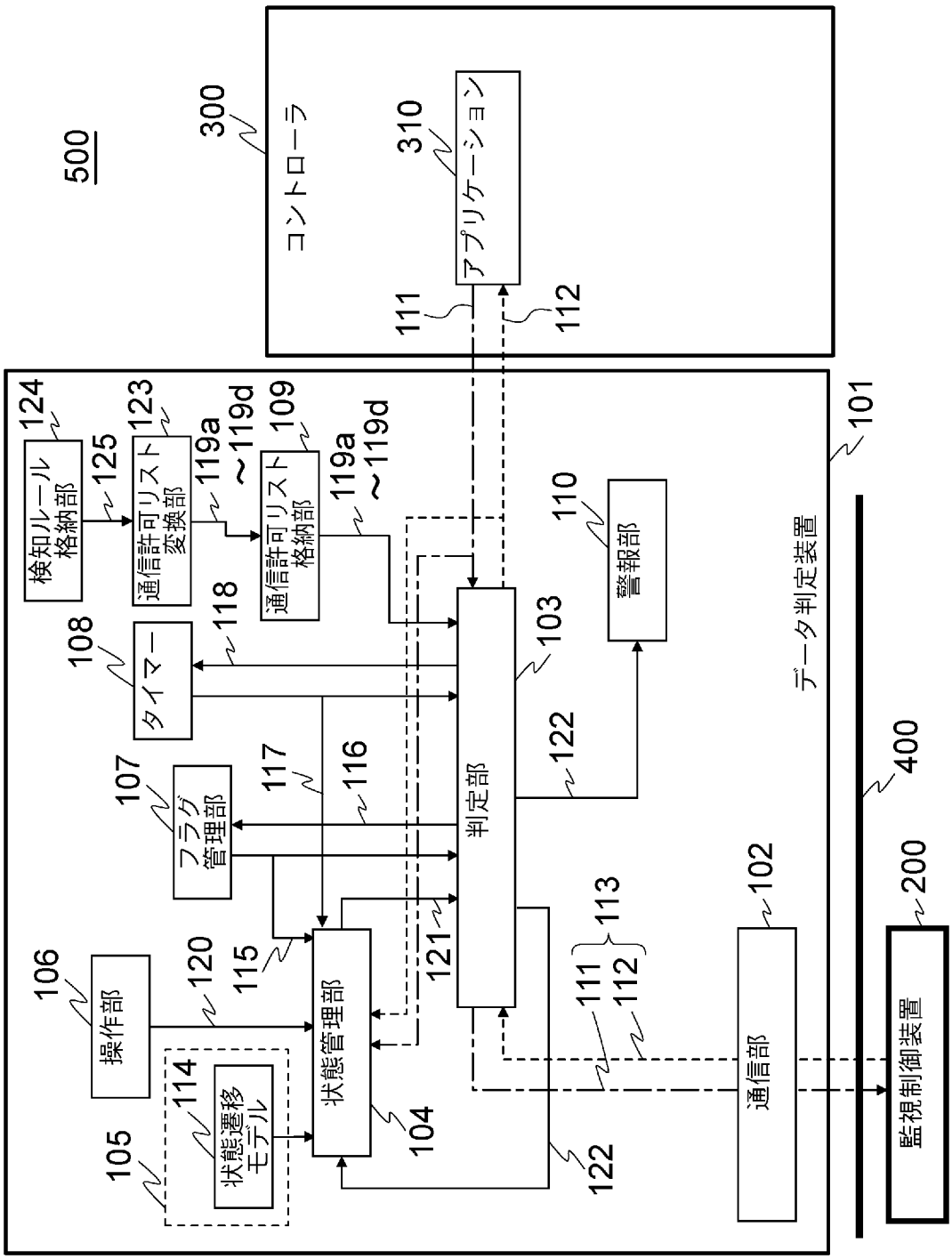
前記通信許可リスト変換部は、前記検知ルールを前記通信許可リストに変換するときに、前記検知ルールに対応関係が記述された前記要求通信及び前記応答通信に対してフラグを割り当て、当該フラグに対する設定値を指定したフラグ操作の内容と、前記フラグに前記設定値が設定されているかを判定するためのフラグ条件とを対応させて、前記通信許可リストに記述し、

前記判定部は、前記要求通信の通信データが正常であると判定した後に、前記フラグ操作の内容に従って、前記フラグに前記設定値をセットし、前記要求通信に対する前記応答通信の通信データが正常であるか否かを判定する場合に、前記フラグ条件に基づいて前記フラグに

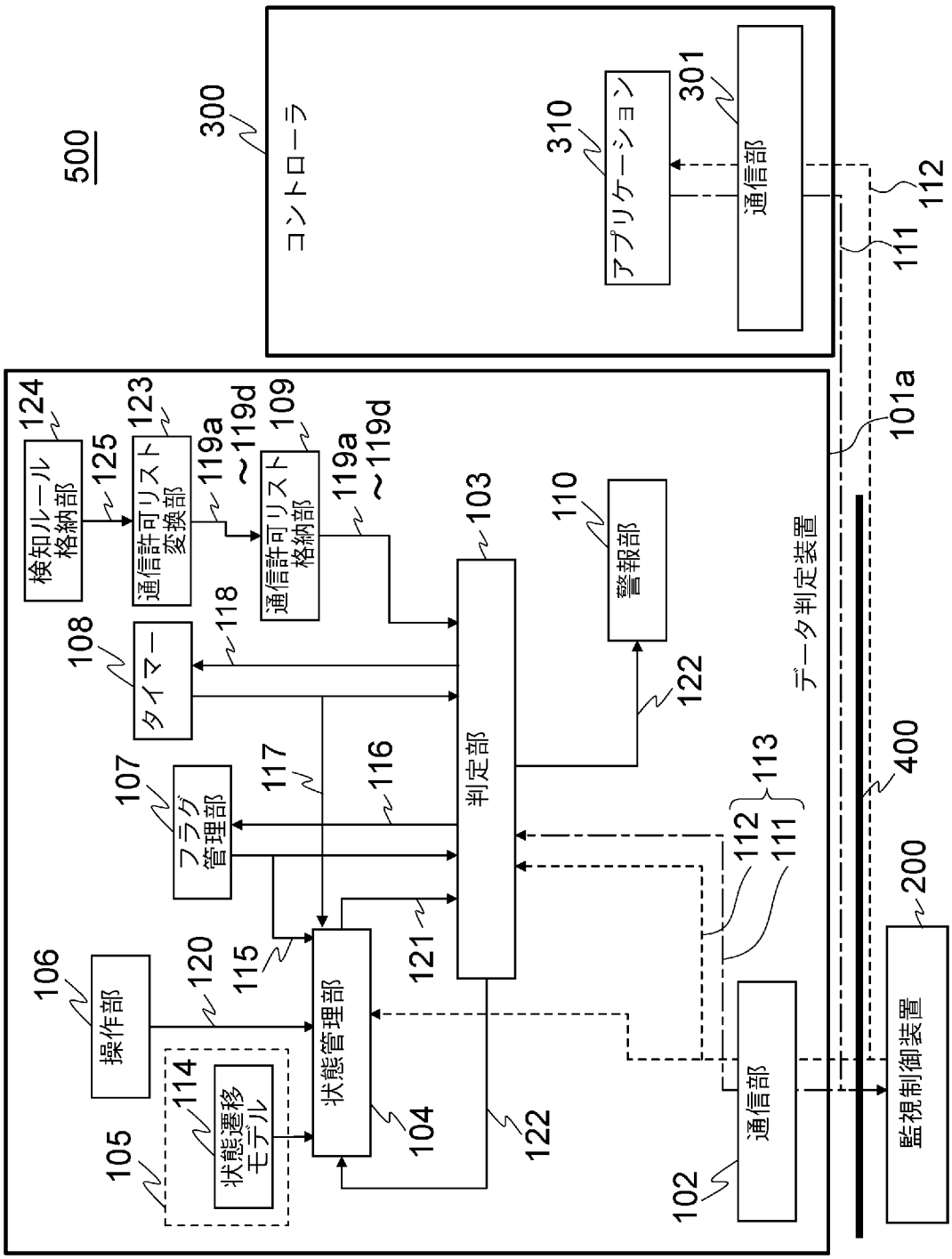
前記設定値が設定されているか否かを判定し、前記設定値が設定されていた場合に、前記応答通信の通信データを正常であると判定して、前記フラグをリセットする、

データ判定プログラム。

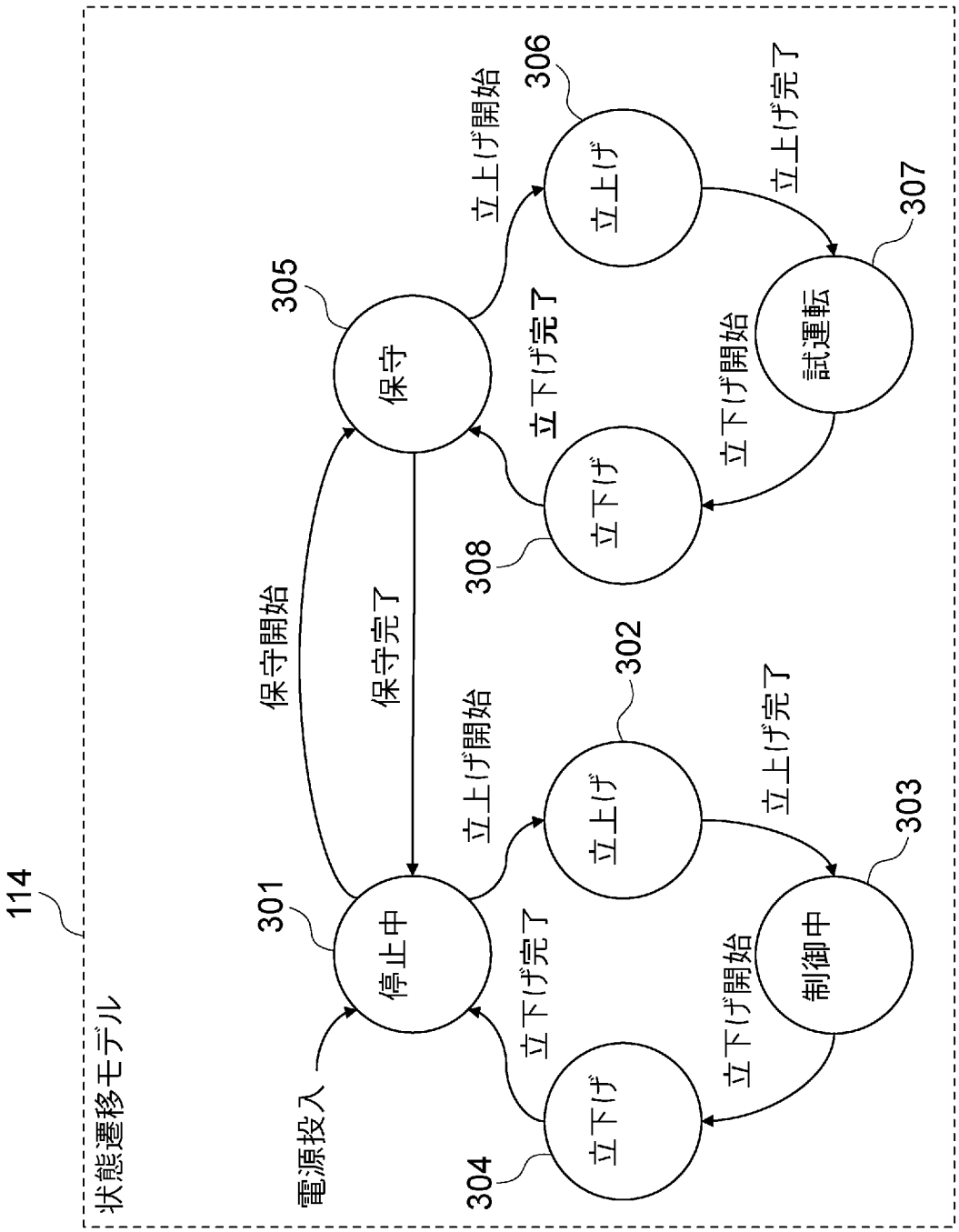
[図1]


500
300
コントローラ
310
アプリケーション
111
112
101
データ判定装置
124
検知ルール格納部
125
123
通信許可リスト変換部
119a ～119d
109
通信許可リスト格納部
119a ～119d
110
警報部
108
タイマー
118
103
判定部
122
107
フラグ管理部
117
116
400
106
操作部
120
115
状態管理部
121
111
112
113
102
200
114
状態遷移モデル
105
104
122
通信部
監視制御装置

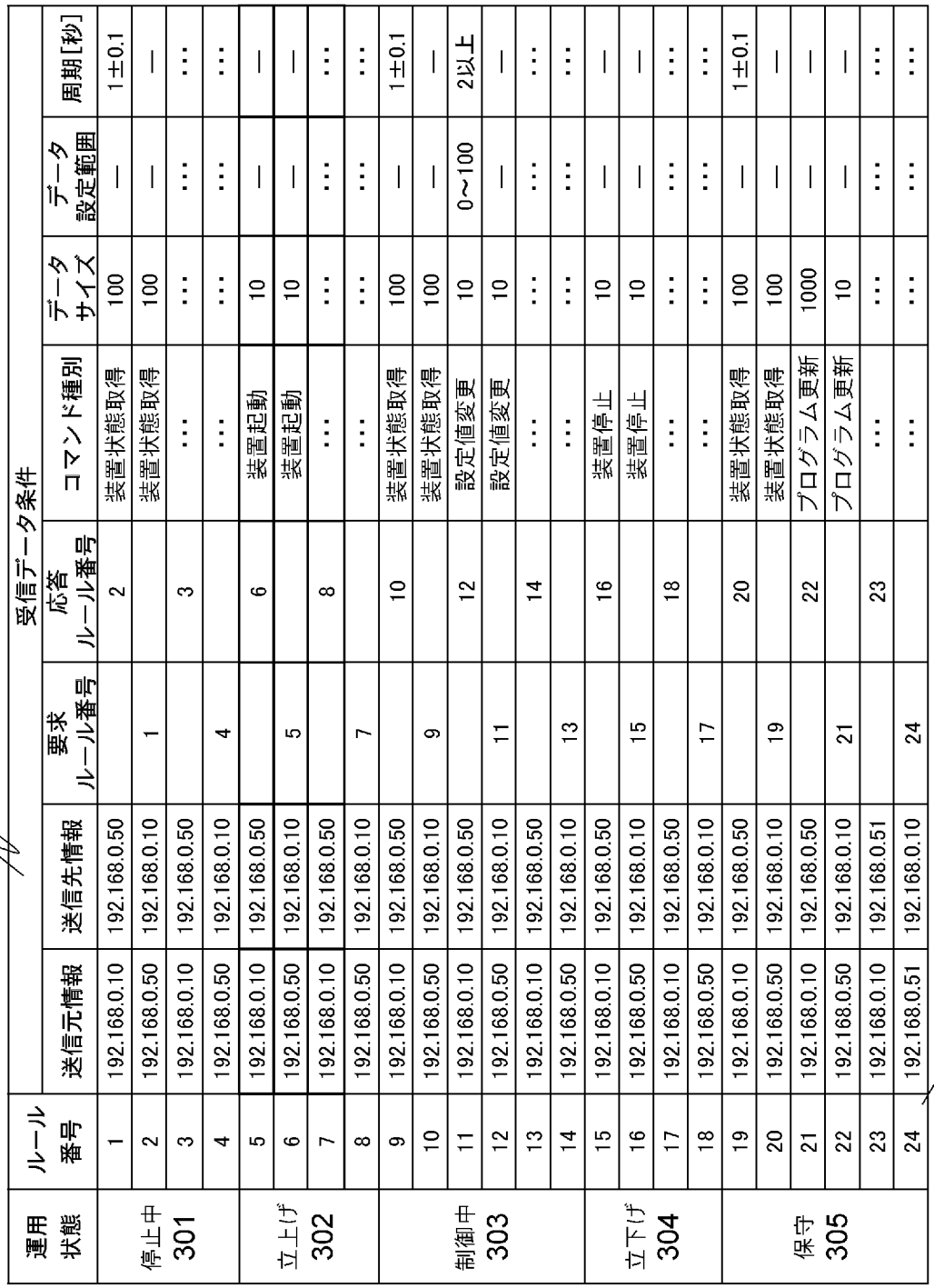
[図2]


500
300
コントローラ
310
アプリケーション
301
通信部
112
111
101a
データ判定装置
124
検知ルール格納部
125
123
通信許可リスト変換部
119a ～119d
109
通信許可リスト格納部
119a ～119d
103
110
警報部
108
タイマー
118
122
107
フラグ管理部
117
116
判定部
113
112
111
400
106
操作部
120
115
状態管理部
121
200
114
状態遷移モデル
105
104
122
102
通信部
監視制御装置

[図3]


114
状態遷移モデル
301
停止中
電源投入
304
立下げ
305
保守
306
立上げ
307
試運転
308
立下げ
302
立上げ
303
制御中
立下げ
保守開始
保守完了
立上げ開始
立下げ完了
立上げ開始
立上げ完了
立下げ開始
立下げ完了
立下げ開始
立上げ完了

[図4]



運用状態	ルール番号	受信データ条件							
		送信元情報	送信先情報	要求ルール番号	応答ルール番号	コマンド種別	データサイズ	データ設定範囲	周期[秒]
停止中 301	1	192.168.0.10	192.168.0.50		2	装置状態取得	100	—	1±0.1
	2	192.168.0.50	192.168.0.10	1		装置状態取得	100	—	—
	3	192.168.0.10	192.168.0.50		3	…	…	…	…
	4	192.168.0.50	192.168.0.10	4		…	…	…	…
立上げ 302	5	192.168.0.10	192.168.0.50		6	装置起動	10	—	—
	6	192.168.0.50	192.168.0.10	5		装置起動	10	—	—
	7	192.168.0.10	192.168.0.50		8	…	…	…	…
	8	192.168.0.50	192.168.0.10	7		…	…	…	…
制御中 303	9	192.168.0.10	192.168.0.50		10	装置状態取得	100	—	1±0.1
	10	192.168.0.50	192.168.0.10	9		装置状態取得	100	—	—
	11	192.168.0.10	192.168.0.50		12	設定値変更	10	0～100	2以上
	12	192.168.0.50	192.168.0.10	11		設定値変更	10	—	—
	13	192.168.0.10	192.168.0.50		14	…	…	…	…
	14	192.168.0.50	192.168.0.10	13		…	…	…	…
立下げ 304	15	192.168.0.10	192.168.0.50		16	装置停止	10	—	—
	16	192.168.0.50	192.168.0.10	15		装置停止	10	—	—
	17	192.168.0.10	192.168.0.50		18	…	…	…	…
	18	192.168.0.50	192.168.0.10	17		…	…	…	…
保守 305	19	192.168.0.10	192.168.0.50		20	装置状態取得	100	—	1±0.1
	20	192.168.0.50	192.168.0.10	19		装置状態取得	100	—	—
	21	192.168.0.10	192.168.0.50		22	プログラム更新	1000	—	—
	22	192.168.0.50	192.168.0.10	21		プログラム更新	10	—	—
	23	192.168.0.10	192.168.0.51		23	…	…	…	…
	24	192.168.0.51	192.168.0.10	24		…	…	…	…

[図5]

119a

141

ルール番号	送信元情報	送信先情報	コマンド種別	データサイズ	データ設定範囲	タイマ条件	フラグ条件	アクション番号
1	192.168.0.10	192.168.0.50	装置状態取得	100	—	T1 > 0.9 T1 < 1.1	—	1
2	192.168.0.50	192.168.0.10	装置状態取得	100	—	—	F1==1	2
3	192.168.0.10	192.168.0.50	…	…	…	…	—	3
4	192.168.0.50	192.168.0.10	…	…	…	…	F2==1	4
5	192.168.0.10	192.168.0.50	装置起動	10	—	—	—	5
6	192.168.0.50	192.168.0.10	装置起動	10	—	—	F3==1	6
7	192.168.0.10	192.168.0.50	…	…	…	…	—	7
8	192.168.0.50	192.168.0.10	…	…	…	…	F4==1	8
9	192.168.0.10	192.168.0.50	装置状態取得	100	—	T2 > 0.9 T2 < 1.1	—	9
10	192.168.0.50	192.168.0.10	装置状態取得	100	—	—	F5==1	10
11	192.168.0.10	192.168.0.50	設定値変更	10	0~100	T3 >2	—	11
12	192.168.0.50	192.168.0.10	設定値変更	10	—	—	F6==1	12
13	192.168.0.10	192.168.0.50	…	…	…	…	—	13
14	192.168.0.50	192.168.0.10	…	…	…	…	F7==1	14
15	192.168.0.10	192.168.0.50	装置停止	10	—	—	—	15
16	192.168.0.50	192.168.0.10	装置停止	10	—	—	F8==1	16
17	192.168.0.10	192.168.0.50	…	…	…	…	—	17
18	192.168.0.50	192.168.0.10	…	…	…	…	F9==1	18
19	192.168.0.10	192.168.0.50	装置状態取得	100	—	T4 > 0.9 T4 < 1.1	—	19
20	192.168.0.50	192.168.0.10	装置状態取得	100	—	—	F10==1	20
21	192.168.0.10	192.168.0.50	プログラム更新	1000	—	—	—	21
22	192.168.0.50	192.168.0.10	プログラム更新	10	—	—	F11==1	22
23	192.168.0.10	192.168.0.51	…	…	…	…	—	23
24	192.168.0.51	192.168.0.10	…	…	…	…	F12==1	24

[図6]

119b

運用状態	ルール数	インデックス ルール番号					
停止中301	4	0	1	2	3		
		1	3	2	4		
立上げ302	4	0	1	2	3		
		5	7	6	8		
制御中303	6	0	1	2	3	4	5
		9	11	13	10	12	14
立下げ304	4	0	1	2	3		
		15	17	16	18		
保守305	6	0	1	2	3	4	5
		19	21	23	20	22	24

[図7]

119c

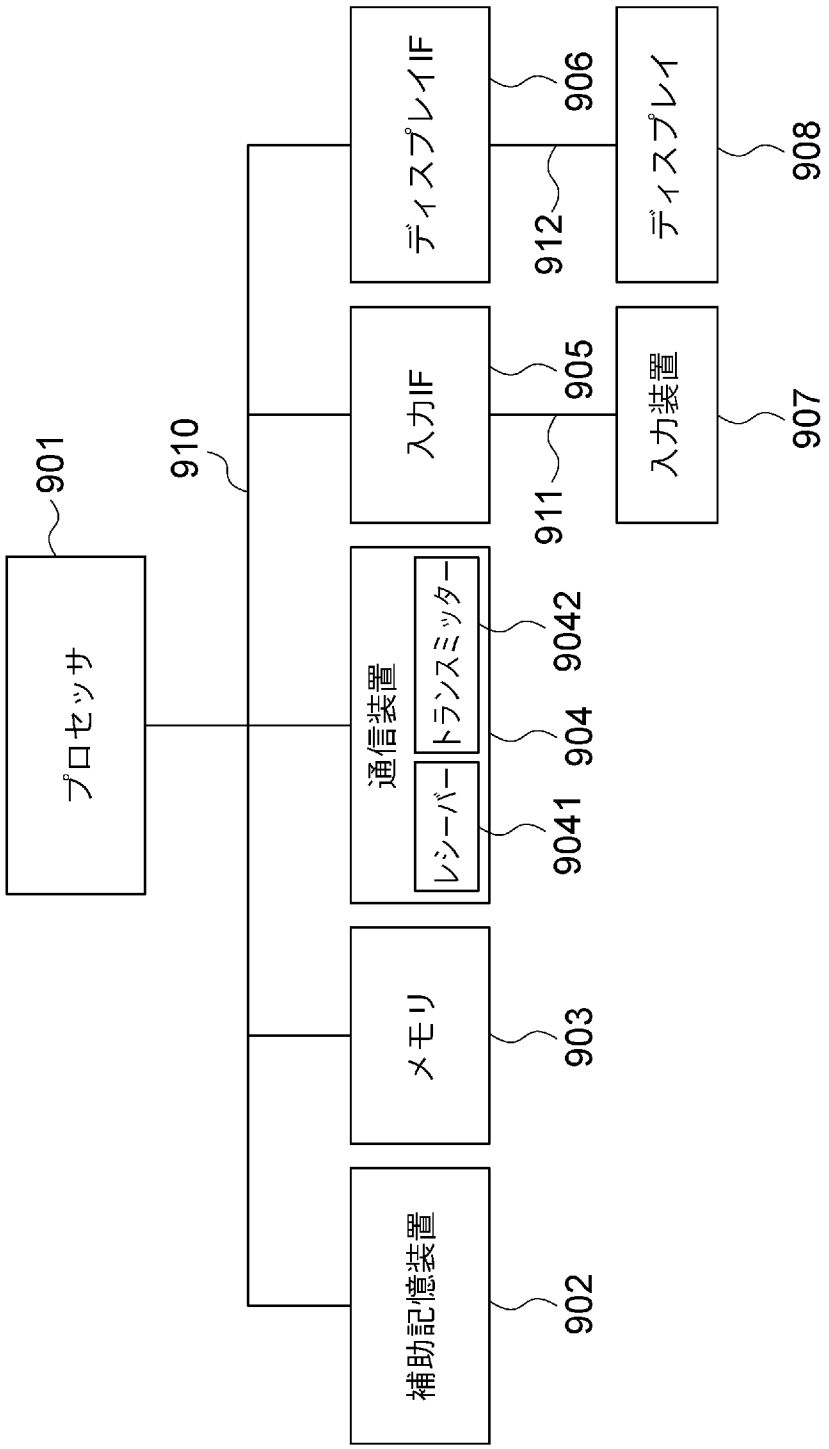
アクション番号	タイマ操作	フラグ操作
1	T1=0	F1=1
2		F1=0
3		F2=1
4		F2=0
5		F3=1
6		F3=0
7		F4=1
8		F4=0
9	T2=0	F5=1
10		F5=0
11	T3=0	F6=1
12		F6=0
13		F7=1
14		F7=0
15		F8=1
16		F8=0
17		F9=1
18		F9=0
19	T4=0	F10=1
20		F10=0
21		F11=1
22		F11=0
23		F12=1
24		F12=0

[図8]

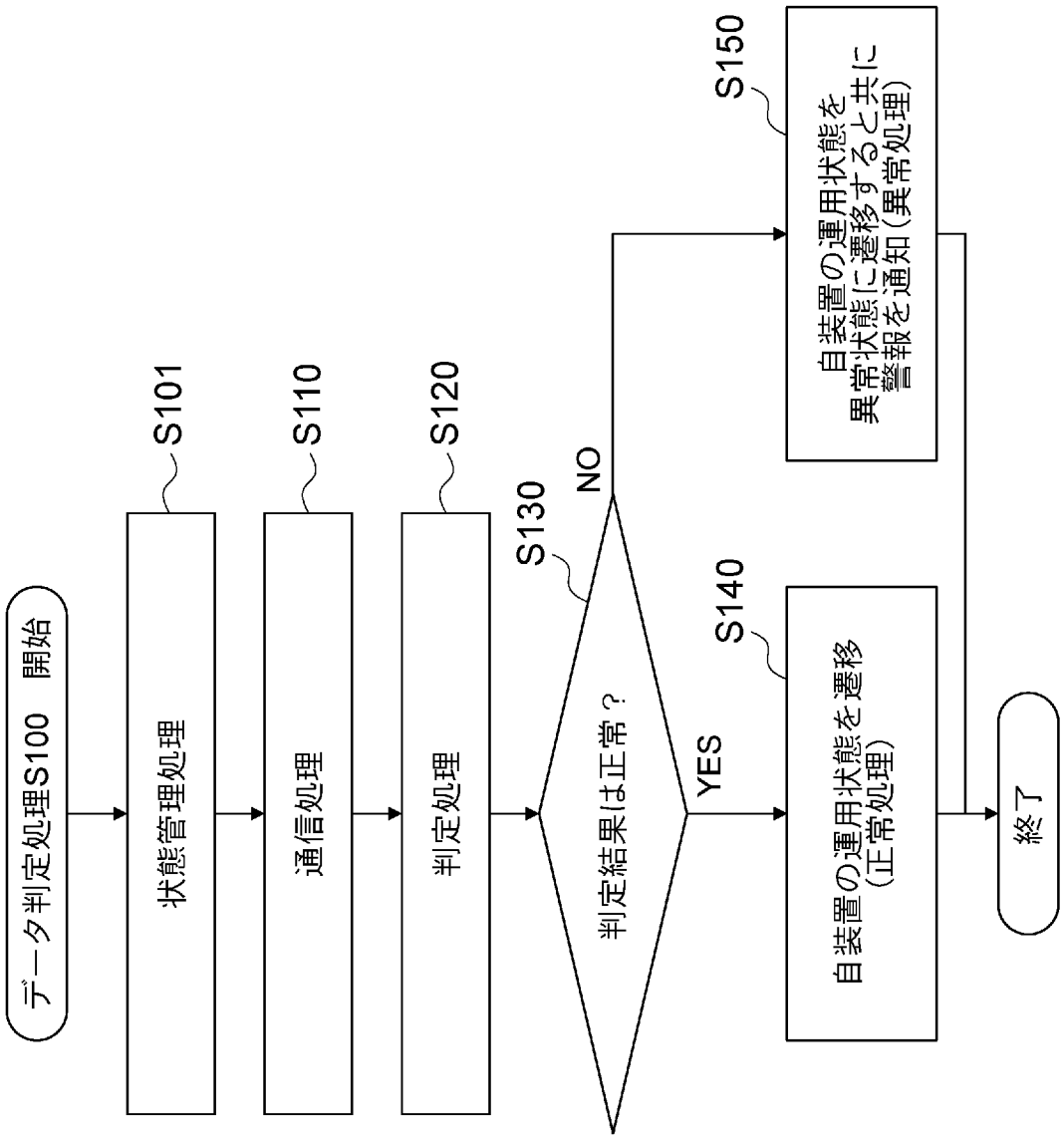
119d

運用状態	送信元	送信先	インデックス先頭番号	検索個数
停止中301	192.168.0.10	192.168.0.50	0	2
	192.168.0.50	192.168.0.10	2	2
立上げ302	192.168.0.10	192.168.0.50	0	2
	192.168.0.50	192.168.0.10	2	2
制御中303	192.168.0.10	192.168.0.50	0	3
	192.168.0.50	192.168.0.10	3	3
立下げ304	192.168.0.10	192.168.0.50	0	2
	192.168.0.50	192.168.0.10	2	2
保守305	192.168.0.10	192.168.0.50	0	2
	192.168.0.10	192.168.0.51	2	1
	192.168.0.50	192.168.0.10	3	2
	192.168.0.51	192.168.0.10	5	1

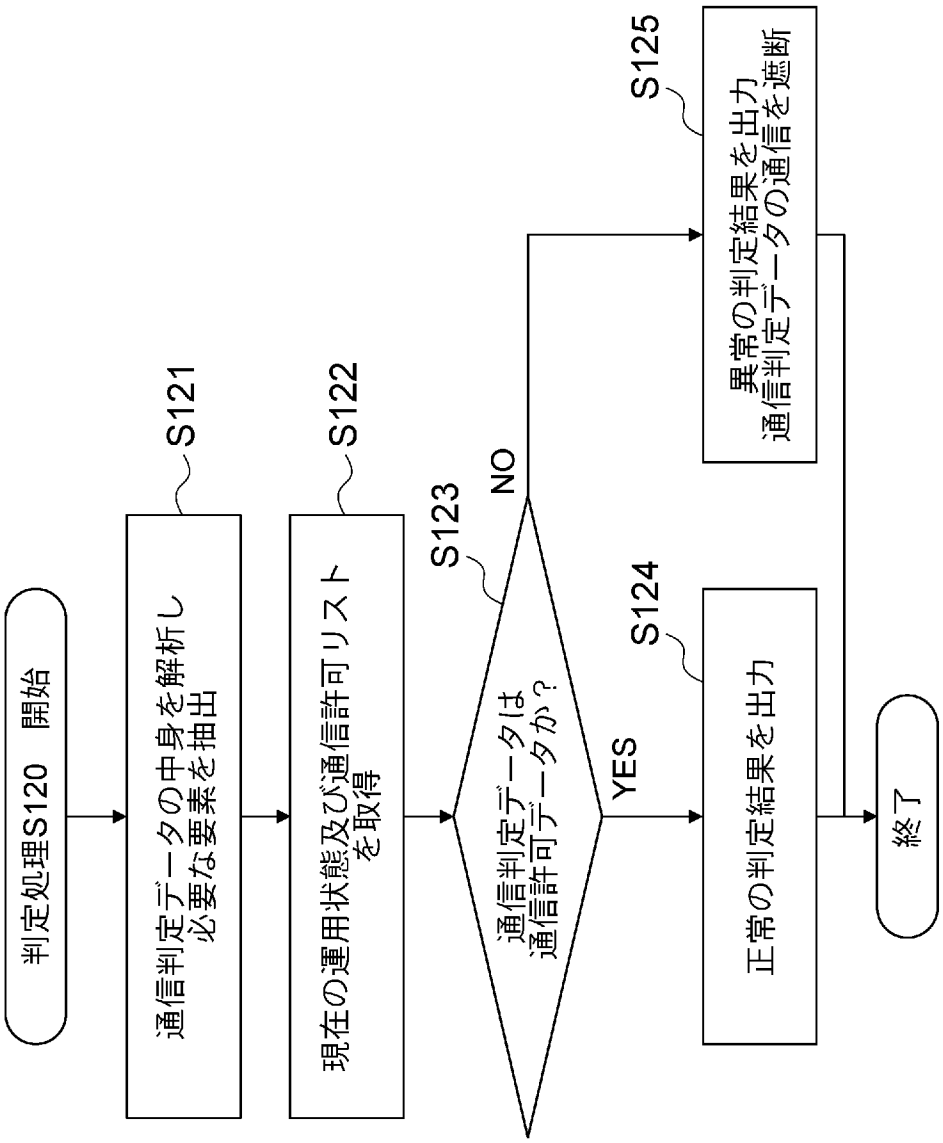
[図9]


プロセッサ
901
910
補助記憶装置
902
メモリ
903
通信装置
レシーバー
9041
トランスミッター
9042
904
入力IF
905
911
入力装置
907
ディスプレイIF
906
912
ディスプレイ
908

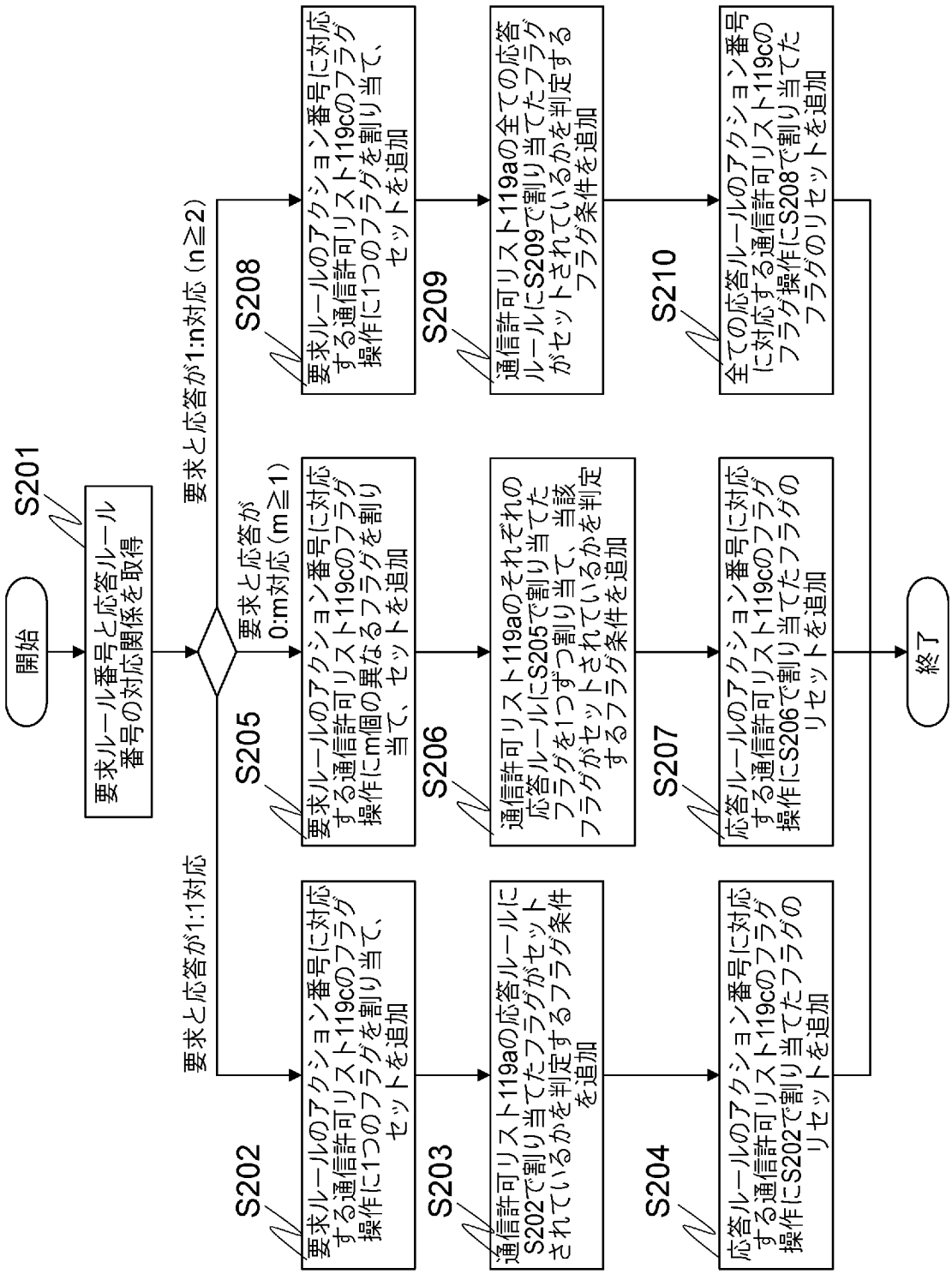
[図10]


データ判定処理S100　開始
S101
状態管理処理
S110
通信処理
S120
判定処理
S130
判定結果は正常？
NO
YES
S140
自装置の運用状態を遷移
(正常処理)
S150
自装置の運用状態を
異常状態に遷移すると共に
警報を通知(異常処理)
終了

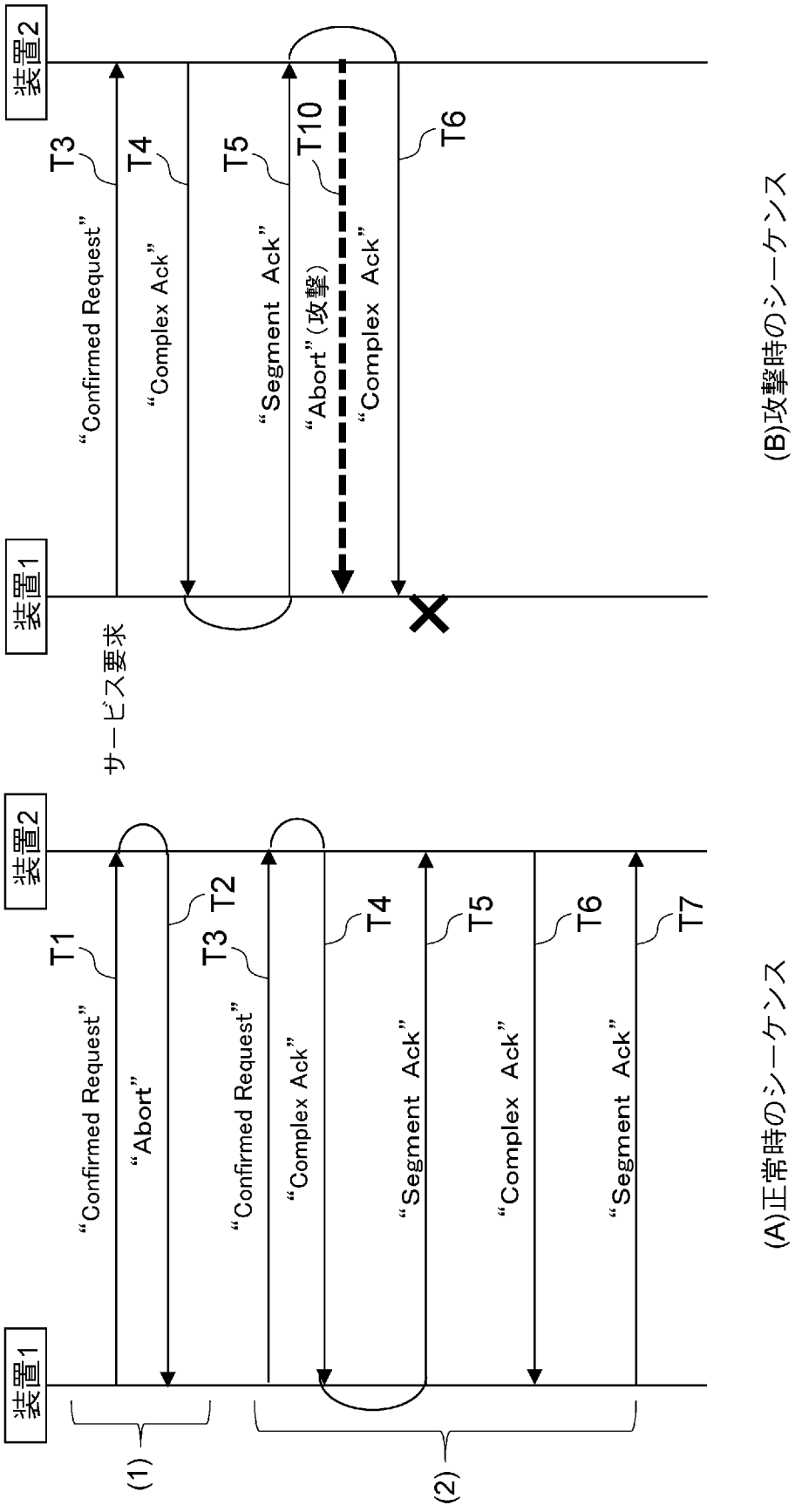
[図11]


判定処理S120　開始
S121
通信判定データの中身を解析し
必要な要素を抽出
S122
現在の運用状態及び通信許可リストを取得
S123
通信判定データは
通信許可データか？
NO
YES
S124
正常の判定結果を出力
S125
異常の判定結果を出力
通信判定データの通信を遮断
終了

[図12]


開始
S201
要求ルール番号と応答ルール番号の対応関係を取得
要求と応答が1:1対応
要求と応答が0:m対応（m≧1）
要求と応答が1:n対応（n≧2）
S202
要求ルールのアクション番号に対応する通信許可リスト119cのフラグ操作に1つのフラグを割り当て、セットを追加
S203
通信許可リスト119aの応答ルールにS202で割り当てたフラグがセットされているかを判定するフラグ条件を追加
S204
応答ルールのアクション番号に対応する通信許可リスト119cのフラグ操作にS202で割り当てたフラグのリセットを追加
S205
要求ルールのアクション番号に対応する通信許可リスト119cのフラグ操作にm個の異なるフラグを割り当て、セットを追加
S206
通信許可リスト119aのそれぞれの応答ルールにS205で割り当てたフラグを1つずつ割り当て、当該フラグがセットされているかを判定するフラグ条件を追加
S207
応答ルールのアクション番号に対応する通信許可リスト119cのフラグ操作にS206で割り当てたフラグのリセットを追加
S208
要求ルールのアクション番号に対応する通信許可リスト119cのフラグ操作に1つのフラグを割り当て、セットを追加
S209
通信許可リスト119aの全ての応答ルールにS209で割り当てたフラグがセットされているかを判定するフラグ条件を追加
S210
全ての応答ルールのアクション番号に対応する通信許可リスト119cのフラグ操作にS208で割り当てたフラグのリセットを追加
終了

[図13]


装置1
装置2
T1
T2
T3
T4
T5
T6
T7
"Confirmed Request"
"Abort"
"Confirmed Request"
"Complex Ack"
"Segment Ack"
"Complex Ack"
"Segment Ack"
(1)
(2)
(A)正常時のシーケンス
サービス要求
装置1
装置2
T3
T4
T5
T10
T6
"Confirmed Request"
"Complex Ack"
"Segment Ack"
"Abort"(攻撃)
"Complex Ack"
(B)攻撃時のシーケンス

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2017/002013

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/55(2013.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F21/55

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2017
Kokai Jitsuyo Shinan Koho	1971-2017	Toroku Jitsuyo Shinan Koho	1994-2017

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.
A	WO 2016/114077 A1 (Mitsubishi Electric Corp.), 21 July 2016 (21.07.2016), paragraphs [0078] to [0112]; fig. 14 to 19 & JP 6054010 B2	1-8
A	Tsunato NAKAI, "Plant Seigyo System Muke Whitelist-gata Kogeki Kenchi Kino no Sekkei", SCIS2016 [USB] SCIS2016 2016 Symposium on Cryptography and Information Security, 19 January 2016 (19.01.2016), pages 1 to 8	1-8
A	Koichi SHIMIZU, "Whitelist-gata Kogeki Kenchi ni Okeru Kenchi Rule no Jido Seisei", SCIS2016 [USB] SCIS2016 2016 Symposium on Cryptography and Information Security, 19 January 2016 (19.01.2016), pages 1 to 7	1-8

☒ 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
15 February 2017 (15.02.17)	28 February 2017 (28.02.17)

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2017/002013

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Niv Goldenberg et al., Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems, International Journal of Critical Infrastructure Protection, Volume 6, Issue 2, 2013.06, p.63-75	1-8

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１７／００２０１３

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/55(2013.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/55

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	１９７１－２０１７年
日本国実用新案登録公報	１９９６－２０１７年
日本国登録実用新案公報	１９９４－２０１７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
A	WO 2016/114077 A1 (三菱電機株式会社) 2016.07.21, 段落[0078]-[0112],図 14-19 & JP 6054010 B2	1-8
A	中井　綱人, プラント制御システム向けホワイトリスト型攻撃検知機能の設計, ＳＣＩＳ２０１６［ＵＳＢ］ＳＣＩＳ２０１６　２０１６　Ｓｙｍｐｏｓｉｕｍ　ｏｎ　Ｃｒｙｐｔｏｇｒａｐｈｙ　ａｎｄ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｓｅｃｕｒｉｔｙ, 2016.01.19, p.1-8	1-8

☑　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
１５．０２．２０１７	２８．０２．２０１７

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

特許庁審査官（権限のある職員）　５Ｓ　９０７１
平井　誠
電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	清水　孝一，ホワイトリスト型攻撃検知における検知ルールの自動生成，ＳＣＩＳ２０１６　［ＵＳＢ］　ＳＣＩＳ２０１６　２０１６　Ｓｙｍｐｏｓｉｕｍ　ｏｎ　Ｃｒｙｐｔｏｇｒａｐｈｙ　ａｎｄ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｓｅｃｕｒｉｔｙ，2016.01.19, p.1-7	1-8
A	Niv Goldenberg et al., Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems, International Journal of Critical Infrastructure Protection, Volume 6, Issue 2, 2013.06, p.63-75	1-8