(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
2016 年 7 月 21 日(21.07.2016)

WIPO | PCT

(10) 国際公開番号
WO 2016/114077 A1

(51) 国際特許分類:
*G06F 21/55* (2013.01)

(21) 国際出願番号: PCT/JP2015/085742

(22) 国際出願日: 2015 年 12 月 22 日(22.12.2015)

(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:
PCT/JP2015/051108 2015 年 1 月 16 日(16.01.2015) JP

(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). 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). 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).

(74) 代理人: 溝井 章司, 外(**MIZOI, Shoji** et al.); 〒2470056 神奈川県鎌倉市大船二丁目１７番１０号 ＮＴＡ大船ビル３階 溝井国際特許事務所 Kanagawa (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, 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, KN, KP, KR, 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,

[続葉有]

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

(54) 発明の名称 : データ判定装置、データ判定方法及びプログラム

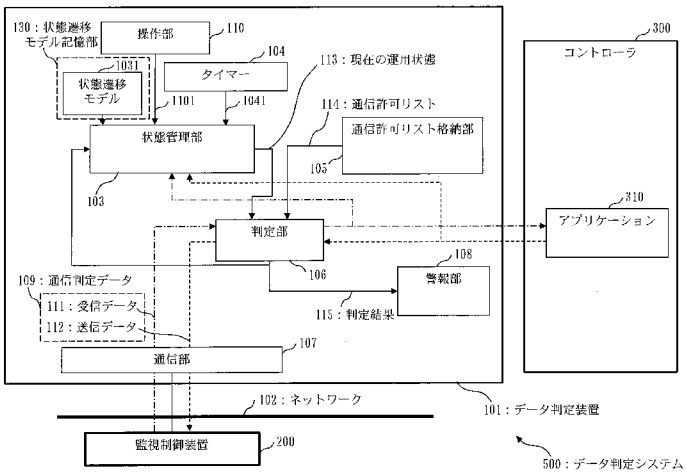



FIG. 1:
101 Data assessment device
102 Network
103 State management unit
104 Timer
105 Communication permission list storage unit
106 Assessment unit
107 Communication unit
108 Alert unit
109 Communication assessment data
110 Console unit
111 Receiving data
112 Transmitting data
113 Current operating state
114 Communication permission list
115 Assessment result
130 State transition model storage unit
200 Monitor control device
300 Controller
310 Application
500 Data assessment system
1031 State transition model

(57) **Abstract**: Provided is a data assessment device, comprising: a state transition model storage unit (130) which stores a state transition model (1031) which represents state transitions; a state management unit (103) which retains operating states of the present device on the basis of the state transition model; a communication permission list storage unit (105) which stores as a communication permission list (114) communication permitted data for which communication is permitted in each operating state; a communication unit (107) which acquires communication data to be assessed (109); and an assessment unit (106) which, using the current operating state (113) and the communication permission list (114), assesses whether the communication data to be assessed (109) is the communication permitted data for which communication is permitted in the current operating state (113).

(57) 要約: 状態遷移を表す状態遷移モデル（１０３１）を記憶する状態遷移モデル記憶部（１３０）と、状態遷移モデルに基づいて自装置の運用状態を保有する状態管理部（１０３）と、各運用状態において通信を許可する通信許可データを通信許可リスト（１１４）として格納する通信許可リスト格納部（１０５）と、通信判定データ（１０９）を取得する通信部（１０７）と、現在の運用状態（１１３）と通信許可リスト（１１４）とを用いて、通信判定データ（１０９）が現在の運用状態（１１３）において通信を許可された通信許可データであるか否かを判定する判定部（１０６）とを備える。

WO 2016/114077 A1

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)）

# 明　細　書

## 発明の名称 ： データ判定装置、データ判定方法及びプログラム

## 技術分野

[0001] 本発明は、データ判定装置、データ判定方法及びプログラムに関する。特に、ネットワークへの攻撃の侵入を検知するデータ判定装置、データ判定方法及び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、システムがネットワークに接続されるケースが増大し、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。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、以下のような方式が取られている。

[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のペアやプロトコル等の許可された通信を定義する。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することによって、未知の攻撃に対しても侵入を検知するホワイトリスト型の対策を取る（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も提案されている（特許文献２参照）。

さらに、通信を許可するアプリケーションを定義することによって、不正なプログラムの実行によるネットワーク侵入を検知する方法も提案されている（特許文献３参照）。

## 先行技術文献

## 特許文献

[0005] 特許文献1：特許第４６８８４２０号公報

特許文献2：特開２００１－０３４５５３号公報

特許文献3：特表２０１３－５３２８６９号公報

## 発明の概要

### 発明が解決しようとする課題

[0006] 近年、産業制御システムをターゲットにＳｔｕｘｎｅｔに代表される高度な攻撃が行われるようになった。Ｓｔｕｘｎｅｔは、通信を許可されたサーバを乗っ取り、正常と定義した通信の中に攻撃通信を紛れ込ませる。このため、攻撃通信は、特許文献１，２のホワイトリスト型対策をすり抜けてしまうという課題がある。

[0007] 特許文献２の技術では、送信元及び送信先の通信状態を監視し、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を判定し、判定結果に従ってアクセス制御を行う。しかし、この場合、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うことで、不正なプログラム書き換え等の攻撃データも通信可能となるという課題がある。

[0008] 特許文献３の技術では、ローカルホストでアプリケーションプログラムと通信を紐づけ、通信が発生した際に、この通信を行うアプリケーションプログラムが通信を許可されたものかどうかを判定して、この通信を遮断する。しかし、この特許文献３の技術では、通信許可されたアプリケーションプログラムに内在する脆弱性を突かれた場合、通信を遮断できない。

[0009] 本発明は、通信を許可されたサーバを乗っ取り、正常と定義した通信の中に攻撃通信を紛れ込ませる攻撃に対しても侵入を検知できるデータ判定装置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

[0010] 本発明に係るデータ判定装置は、

複数の運用状態の各運用状態間の状態遷移を表す状態遷移モデルを記憶する状態遷移モデル記憶部と、

前記状態遷移モデルに基づいて、自装置の運用状態を保有する状態管理部と、

前記複数の運用状態の各運用状態において通信を許可する通信許可データを通信許可リストとして格納する通信許可リスト格納部と、

通信データを通信判定データとして取得する通信部と、

前記通信部により取得された通信判定データを取得すると共に前記状態管理部により保有される前記自装置の運用状態を現在の運用状態として取得し、前記現在の運用状態と前記通信許可リストとを用いて、前記通信判定データが前記現在の運用状態において通信を許可された通信許可データであるか否かを判定する判定部とを備える。

## 発明の効果

[0011] 本発明に係るデータ判定装置によれば、状態遷移モデルに含まれる運用状態毎に通信を許可する通信許可データを通信許可リストとして設定し、判定部が、現在の運用状態と通信許可リストとを用いて、通信判定データが現在の運用状態において通信を許可された通信許可データであるか否かを判定するので、通信を許可されたサーバを乗っ取り、正常と定義した通信の中に攻撃通信を紛れ込ませる攻撃に対しても侵入を検知することができる。

## 図面の簡単な説明

[0012] [図1]実施の形態１に係るデータ判定装置のブロック構成図。

[図2]図１のデータ判定装置とは異なる動作を行うデータ判定装置のブロック構成図。

[図3]実施の形態１に係るデータ判定装置の状態遷移モデルの一例を示す図。

[図4]実施の形態１に係る通信許可リストの構成図。

[図5]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図。

[図6]実施の形態１に係るデータ判定装置のデータ判定方法、データ判定処理を示すフロー図。

[図7]実施の形態１に係る判定部による判定処理を示すフロー図。

[図8]実施の形態２に係るデータ判定装置のブロック構成図。

[図9]取得情報履歴から運用状態を決定するための手順を示す図。

[図10]状態遷移モデルより生成された通信許可リストを示す図。

[図11]まとめ後の通信許可リストを示す図。

[図12]実施の形態３に係るデータ判定装置のブロック構成図。

[図13]図１２のデータ判定装置とは異なる動作を行うデータ判定装置のブロック構成図。

[図14]実施の形態４に係るデータ判定装置のブロック構成図。

[図15]図１４のデータ判定装置とは異なる動作を行うデータ判定装置のブロック構成図。

[図16]実施の形態４に係る通信許可リストの構成図。

[図17]実施の形態４に係るデータ判定装置の状態遷移モデルの一例を示す図。

[図18]実施の形態４に係るデータ判定装置のデータ判定方法、データ判定処理を示すフロー図。

[図19]実施の形態４に係る判定部による判定処理を示すフロー図。

## 発明を実施するための形態

[0013] 実施の形態１.

＊＊＊構成の説明＊＊＊

図１を用いて、本実施の形態に係るデータ判定装置１０１のブロック構成について説明する。ここで、図１に示すように、データ判定装置１０１、監視制御装置２００、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。

[0014] データ判定装置１０１は、ネットワーク１０２に接続され、監視制御装置２００とコントローラ３００との間で通信される通信データを仲介すると共に通信データの判定を行う。データ判定装置１０１は、ネットワーク１０２に侵入する攻撃を検知する侵入検知装置、侵入検知システムである。

[0015] コントローラ３００は、例えば産業制御システム等に備えられる。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１１２をデータ判定装置１０１に送信する。また、アプリケーション３１０は、受信データ１１１を監視制御装置２００から受信する。ここで、データ判定装置１０１が通信するとともに判定する受信データ１１１、送信データ１１２を通信判定データ１０９とも呼ぶ。

監視制御装置２００は、例えば産業制御システム等を監視制御するサーバである。

[0016] データ判定装置１０１は、監視制御装置２００からネットワーク１０２を介して受信した受信データ１１１をコントローラ３００に仲介する。また、データ判定装置１０１は、コントローラ３００が送信した送信データ１１２をネットワーク１０２を介して監視制御装置２００に仲介する。

データ判定装置１０１は、受信データ１１１及び送信データ１１２を仲介する過程において、攻撃の侵入を検知するデータ判定処理を行う。

[0017] データ判定装置１０１は、状態管理部１０３、タイマー１０４、通信許可リスト格納部１０５、判定部１０６、通信部１０７、警報部１０８、操作部１１０、状態遷移モデル記憶部１３０を備える。

[0018] 状態遷移モデル記憶部１３０は、複数の運用状態の各運用状態間の状態遷移を表す状態遷移モデル１０３１を記憶する。状態遷移モデル記憶部１３０は、自装置が取得した取得情報１０３３に応じて複数の運用状態の各運用状態間を遷移する状態遷移モデル１０３１を記憶する。自装置とは、データ判定装置１０１自身である。

取得情報１０３３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１０３３には、通信により取得される通信データと自装置に対する操作を受け付けたことを示す操作信号１１０１とタイマー１０４から出力されるタイマー信号１０４１とを含む。

[0019] 状態管理部１０３は、状態遷移モデル１０３１に基づいて、自装置、すなわちデータ判定装置１０１の運用状態を保有する。

通信許可リスト格納部１０５は、複数の運用状態の各運用状態において通信を許可する通信許可データ１１９を通信許可リスト１１４として格納する。

通信部１０７は、通信データを通信判定データ１０９として取得する。

[0020] 判定部１０６は、通信部１０７により取得された通信判定データ１０９を取得すると共に状態管理部１０３により保有される自装置の運用状態１０３

２を現在の運用状態１１３として取得する。判定部１０６は、現在の運用状態１１３と通信許可リスト１１４とを用いて、通信判定データ１０９が現在の運用状態１１３において通信を許可された通信許可データ１１９であるか否かを判定する。

[0021] 通信部１０７は、ネットワーク１０２を介して監視制御装置２００との接続を行う。通信部１０７は、監視制御装置２００からネットワーク１０２を介して受信データ１１１を受信し、受信した受信データ１１１を判定部１０６に出力する。通信部１０７は、入力した送信データ１１２を、ネットワーク１０２を介して監視制御装置２００に送信する。通信部１０７は、ネットワーク入出力部である。

[0022] 状態管理部１０３は、データ判定装置１０１の運用状態を状態遷移モデル１０３１で管理する。状態遷移モデル１０３１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。

操作部１１０は、人間が操作するボタン、タッチパネルなどである。操作部１１０は、自装置に対する操作を受け付けたことを示す操作信号１１０１を出力する。

[0023] タイマー１０４は、自装置の運用状態が継続する時間を計測する。すなわち、タイマー１０４は、通信に時間制約がある場合に、時間制約における時間を計測する。

通信許可リスト格納部１０５は、通信許可リスト１１４を格納する記憶領域である。

[0024] 判定部１０６は、受信データ１１１または送信データ１１２と、状態管理部１０３が出力する現在の運用状態１１３と、通信許可リスト格納部１０５が格納する通信許可リスト１１４とを取得する。判定部１０６は、取得した受信データ１１１または送信データ１１２と現在の運用状態１１３と通信許可リスト１１４とを比較し、受信データ１１１または送信データ１１２が許可されているものか否かを判定し、判定結果１１５を出力する。

判定部１０６は、通信判定データ１０９が通信許可データ１１９でないと

判定した場合、通信を遮断する。つまり、判定部１０６は、判定結果１１５が異常の場合、通信を遮断する。

[0025] 警報部１０８は、判定部１０６により通信判定データ１０９が通信許可データ１１９でないと判定された場合、異常を検知したことを示す警報を出力する。つまり、警報部１０８は、判定結果１１５が異常の場合に警報を発する。警報部１０８が発する警報は、ランプのような視覚によるものでもよいし、ネットワークを経由して別のサーバに発報してもよい。

[0026] 状態管理部１０３は、判定部１０６により通信判定データ１０９が通信許可データ１１９であると判定された場合、状態遷移モデル１０３１に基づいて自装置の運用状態１０３２を遷移させる。

また、状態管理部１０３は、判定部１０６により通信判定データ１０９が通信許可データ１１９でないと判定された場合、自装置の運用状態１０３２を異常状態に遷移させる。

なお、状態管理部１０３は、正常と判定された場合に状態を遷移するのみでもよい。

以上のように、状態管理部１０３は、自装置であるデータ判定装置１０１の現在の運用状態１１３を保有する。

[0027] 図２を用いて、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について説明する。

図１に示すデータ判定装置１０１では、判定部１０６が通信判定データ１０９を判定した後に受信データ１１１あるいは送信データ１１２を通信する構成を示した。しかし、図２に示すデータ判定装置１０１ａのように監視制御装置２００とアプリケーション３１０との通信を判定部１０６がキャプチャする構成でもよい。図２のデータ判定装置１０１ａでは、判定結果１１５が異常の場合、判定部１０６が通信を遮断することができない。しかし、警報部１０８により発せられた警報により、攻撃に対する対処を行うことができる。

[0028] 図３を用いて、本実施の形態に係る状態管理部１０３が管理するデータ判

定装置１０１の状態遷移モデル１０３１の一例について説明する。図３は一例であり、状態遷移モデル１０３１は必ずしも図３の通りでなくてもよい。

図３において、各状態３０１～３０７は、複数の運用状態３００１の例である。また、各状態間は、複数の運用状態の各運用状態間３００２の例である。

図３では、データ判定装置１０１は、電源投入時にＮＷ構築状態３０１に遷移し、ＮＷ構築に必要な通信を行う。データ判定装置１０１において、ＮＷ構築に必要な通信を通信データ１とする。なお、以下の説明においてもネットワーク構築をＮＷ構築と記載する。状態遷移モデル１０３１では、ＮＷ構築が完了し、通信データ２を受信したら運転Ａ状態３０２に移行する。

[0029] 状態遷移モデル１０３１では、通信データの順番に規定がある通信、例えば通信データ４，５，６の順番で受信するという規定がある通信が存在する場合、規定された通信順に従って運転状態をさらに定義する。図３の状態遷移モデル１０３１では、通信データ４を通信すると運転Ｂ状態３０３に遷移し、通信データ５を通信すると運転Ｃ状態３０４に遷移し、通信データ６を通信すると運転Ａ状態３０２に遷移するように定義されている。このように、それぞれの運転状態への遷移条件を通信データ４，５，６に割り当てるようにしてもよい。

[0030] また、運転Ａ状態３０２において、時間制約のある通信データ７が存在する場合、タイマーをオンにし、待ち状態３０５に移行し、タイマーがオフになったら運転Ａ状態３０２に復帰するようにしてもよい。タイマー信号１０４１は、タイマーのオンオフを示す信号である。

さらに、人の操作１により保守状態３０６に移行し、保守に必要な通信、例えば通信データ８，９を行うようにしてもよい。保守が完了し、通信データ１０を受信したら運転Ａ状態３０２に移行する。さらに、通信データによる状態遷移を行う際は、判定部１０６の判定結果が正常であった場合のみ遷移するようにしてもよい。各状態において、判定部１０６の判定結果が異常であったら、異常状態３０７に遷移してもよい。

[0031] 図４を用いて、本実施の形態に係る通信許可リスト１１４の構成について説明する。

図４は、状態管理部１０３の保持するそれぞれの運用状態において許可された通信許可リスト１１４の例である。図４の通信許可リスト１１４は一例であり、必ずしも図４の通りでなくてもよい。

[0032] 図４に示すように、通信許可リスト１１４は、運用状態、通信データ番号、送信元アドレス、コマンド種別、データサイズ上限、データ設定範囲などの項目を有する。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。

[0033] 図４に示すように、ＮＷ構築時は、通信データ１，２のみ許可し、それ以外の通信を許可しない。また、待ち状態ではすべての通信を許可しない。

[0034] 図５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。

[0035] データ判定装置１０１はコンピュータである。

データ判定装置１０１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と接続され、これら他のハードウェアを制御する。

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。

[0036] プロセッサ９０１は、プロセッシングを行うＩＣ（Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）である。

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。

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）である。

メモリ９０３は、例えば、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）である。

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）である。

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）端子である。

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）端子である。

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である。

ディスプレイ９０８は、例えば、ＬＣＤ（Ｌｉｑｕｉｄ　Ｃｒｙｓｔａｌ　Ｄｉｓｐｌａｙ）である。

[0037] 補助記憶装置９０２には、図１に示す状態管理部１０３、判定部１０６、警報部１０８（以下、状態管理部１０３、判定部１０６、警報部１０８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。

このプログラムは、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。

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。

図５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。

また、「部」の処理の結果を示す情報やデータや信号値や変数値が、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。

[0038] 「部」を「サーキットリー」で提供してもよい。

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。

「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（Ａｐｐｌｉｃａｔｉｏｎ　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。

[0039] 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。

[0040] ＊＊＊動作の説明＊＊＊

図６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、データ判定処理Ｓ１００について説明する。

[0041] 上述したように、データ判定装置１０１は、状態遷移モデル１０３１を記憶する状態遷移モデル記憶部１３０と、通信許可データ１１９を通信許可リスト１１４として格納する通信許可リスト格納部１０５とを備える。

[0042] 状態管理処理Ｓ１０１において、状態管理部１０３は、状態遷移モデル１０３１に基づいて、自装置の運用状態１０３２を保有する状態管理処理Ｓ１０１を実行する。状態管理部１０３は、状態遷移モデル１０３１に基づいて自装置の運用状態１０３２を遷移させ、最新の運用状態を自装置の運用状態１０３２として保有する。

[0043] 通信処理Ｓ１１０において、通信部１０７は、通信データを通信判定データ１０９として取得する通信処理Ｓ１１０を実行する。通信部１０７は、受信データ１１１あるいは送信データ１１２を、判定の対象である通信判定データ１０９として取得する。

[0044] 判定処理Ｓ１２０において、判定部１０６は、通信処理Ｓ１１０により取得された通信判定データ１０９を取得すると共に状態管理処理Ｓ１０１により保有される自装置の運用状態１０３２を現在の運用状態１１３として取得する。判定部１０６は、現在の運用状態１１３と通信許可リスト１１４とを用いて、通信判定データ１０９が現在の運用状態１１３において通信を許可された通信許可データ１１９であるか否かを判定する。判定部１０６は、判定結果１１５を出力する。

Ｓ１３０において、判定結果１１５が正常、すなわち通信判定データ１０９が通信許可データ１１９である場合、正常処理Ｓ１４０に進む。

Ｓ１３０において、判定結果１１５が異常、すなわち通信判定データ１０９が通信許可データ１１９でない場合、異常処理Ｓ１５０に進む。

[0045] 正常処理Ｓ１４０において、状態管理部１０３は、取得した通信判定データ１０９と状態遷移モデル１０３１とに基づいて、自装置の運用状態１０３

２を遷移させる。

異常処理Ｓ１５０において、状態管理部１０３は、自装置の運用状態１０３２を異常状態に遷移させる。また、警報部１０８は、警報を通知する。

[0046] 次に、図７を用いて、判定部１０６による判定処理Ｓ１２０について説明する。

Ｓ１２１において、判定部１０６は、通信判定データ１０９を取得し、取得した通信判定データ１０９を解析する。判定部１０６は、受信データ１１１あるいは送信データ１１２を通信判定データ１０９として取得する。判定部１０６は、通信判定データ１０９の中身を解析し、判定に必要な要素を抽出する。抽出される要素は、通信許可リスト１１４に記載されている項目であり、通信データ番号、送信元アドレス、送信先アドレス、コマンド種別、応答種別等である。

[0047] Ｓ１２２において、判定部１０６は、状態管理部１０３から現在の運用状態１１３を取得する。また、判定部１０６は、通信許可リスト格納部１０５から通信許可リスト１１４を取得する。

[0048] Ｓ１２３において、判定部１０６は、現在の運用状態１１３と通信許可リスト１１４とに基づいて、通信判定データ１０９が現在の運用状態１１３において許可されている通信データ、すなわち通信許可データ１１９であるか否かを判定する。

通信判定データ１０９が通信許可データ１１９であればＳ１２４に進む。

通信判定データ１０９が通信許可データ１１９でない、すなわち通信判定データ１０９が許可されていない通信であれば、Ｓ１２５に進む。

[0049] Ｓ１２４において、判定部１０６は、正常の判定結果１１５を出力する。

Ｓ１２５において、判定部１０６は、異常の判定結果１１５を出力し、通信判定データ１０９の通信を遮断する。あるいは、判定部１０６は、異常の判定結果１１５を出力するだけで、通信判定データ１０９の通信を遮断しなくてもよい。

[0050] 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、デ

ータ判定処理Ｓ１００についての説明を終わる。

[0051] 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）通信データと外部操作とタイマーのいずれか１つ以上の要素によって遷移する状態遷移モデルに従い、運用状態を管理する状態管理部。

（Ｂ）運用状態ごとに許可する通信データを定めた通信許可リストを格納する通信許可リスト格納部。

（Ｃ）状態管理部が出力する現在の運用状態と通信許可リスト格納部が格納している通信許可リストとを用いて、データ判定装置に入力された通信データが正常か否かを判定する判定部。

（Ｄ）判定部が出力する判定結果をもとに警報を発する警報部。

また、状態管理部は、判定部が出力する判定結果によって遷移する状態遷移モデルに従い、運用状態を管理する。判定部は、異常と判断した通信データを遮断する。

[0052] ＊＊＊本実施の形態の効果の説明＊＊＊

比較のために先に述べたＳｔｕｘｎｅｔのような攻撃では、乗っ取られたサーバがコントローラに対しプログラム書き換えを行っている。プログラム書き換え自体は正常通信であり、乗っ取られたサーバも正常と定義されたサーバであるため、ホワイトリスト型対策ではＳｔｕｘｎｅｔのような攻撃を防ぐことができない。

一方、本実施の形態に係るデータ判定装置では、通信データだけでなく人の操作やタイマーによる運用状態の遷移を行うようにしている。よって、保守状態の時のみプログラム書き換えを受け付けるようにし、保守状態への遷移は人の操作によってのみ行われるように対策をすることで、上記のような攻撃を検知することができる。

また、Ｓｔｕｘｎｅｔによってプログラムを書き換えられたコントローラは、制御対象の周波数コンバータに対し高頻度で周波数を変更するコマンドを送信することで機器の故障を誘発する。本実施の形態に係るデータ判定装

置では、タイマーによってそのような高頻度の周波数変更コマンドを検出する対策をとることができる。

なお、上記対策は一例であり、例えば保守状態への移行を、乗っ取りの危険のないことが保障されている専用の装置からの通信データによって行ってもよい。

[0053] また、本実施の形態に係るデータ判定装置によれば、正しい通信順からの逸脱も検知することができる。

[0054] 実施の形態２．

本実施の形態では、主に、実施の形態１と異なる点について説明する。

実施の形態１で説明した構成と同様の構成については同一の符号を付し、その説明を省略する場合がある。

[0055] 上述した実施の形態１では、状態遷移モデル１０３１と通信許可リスト１１４とをあらかじめ設計者が設定する必要があった。しかし、本実施の形態では、状態遷移モデル１０３１と通信許可リスト１１４とを取得情報履歴１５１から生成する方式について説明する。本実施の形態では取得情報履歴１５１に攻撃データが含まれていないことを仮定する。

[0056] ＊＊＊構成の説明＊＊＊

図８を用いて、本実施の形態に係るデータ判定装置１０１ｂのブロック構成について説明する。

図８に示すように、本実施の形態に係るデータ判定装置１０１ｂは、実施の形態１の構成に加え、履歴記憶部１５３、リスト生成部１５２を備える。

[0057] 履歴記憶部１５３は、取得情報の履歴を取得情報履歴１５１として記憶する。取得情報履歴１５１は、データ判定装置１０１ｂが取得した取得情報を蓄積したファイルであり、データ判定装置１０１ｂの記憶領域に記憶される。取得情報履歴１５１は、データ判定装置１０１ｂが取得した取得情報の履歴であり、通信履歴を含むものである。

[0058] リスト生成部１５２は、取得情報履歴１５１に基づいて、状態遷移モデル１０３１と通信許可リスト１１４とを生成する。

なお、状態遷移モデル１０３１と通信許可リスト１１４との生成は人的作業により行ってもよく、人的作業により行う場合にはリスト生成部１５２は無くてもよい。

[0059] ＊＊＊動作の説明＊＊＊

図９は、取得情報履歴１５１からデータ判定装置１０１ｂの運用状態を決定し、状態遷移モデル１０３１を生成するための手順を示す図である。ここでは、リスト生成部１５２が自動的にリスト生成処理を実行するものとして説明する。

図９では、「Ａ電源投入」から「Ｔ通信データ５」までが取得情報履歴１５１により得られたものとする。

[0060] 図９を用いて、リスト生成部１５２による状態遷移モデル生成処理の概要について説明する。

リスト生成部１５２は、取得情報履歴１５１に含まれる連続する通信データ間の経過時間が第１時間以上であれば待ち状態を設定する。

次に、リスト生成部１５２は、通信データ以外の取得情報を取得した時点を第１変化点７０１とし、第１変化点７０１の前後を第１運用状態とする。

次に、リスト生成部１５２は、各第１運用状態において運用状態が遷移すると判定された遷移通信データ７０３を取得した時点を第２変化点７０２として、第２変化点７０２の前後を第２運用状態として状態遷移モデルを生成する。ここで、リスト生成部１５２は、クラスタリング手法を用いて遷移通信データ７０３を抽出する。

[0061] 図１０，１１を用いて、リスト生成部１５２によるリスト生成処理の概要について説明する。

リスト生成部１５２は、状態遷移モデルに含まれる各運用状態において通信された通信データを通信許可データとして通信許可リストに設定する。リスト生成部１５２は、通信許可データに包含関係が成り立つ運用状態同士を１つにまとめる。

[0062] 図９～１１を用いて、リスト生成部１５２による状態遷移モデル生成処理

、リスト生成処理の詳細について説明する。

Ｓ６０１において、リスト生成部１５２は、通信データ間の経過時間が一定以上であれば、「待ち」状態を定義する。待ち状態への遷移の際はタイマーをオンにし、タイマーオフで次の運用状態に遷移するものと定義する。

次に、Ｓ６０２において、リスト生成部１５２は、通信データ以外の入力が発生したら状態の第１変化点７０１とし、第１変化点７０１の間を新たな第１運用状態とする。図９に示すように、「Ａ電源投入」から「Ｉ通信データ５：タイマーオン」までを「状態１」と定義し、同様に、「状態２」、「状態３」を定義する。

[0063] 最後に、Ｓ６０３において、リスト生成部１５２は、Ｓ６０２で定めた第１変化点７０１間の通信データを時系列でクラスタリングし、クラスタの間を新たな第２運用状態とする。クラスタリングにはウォード法やＫ平均法、機械学習などを使用してもよい。通信データによる状態変化が仕様から明らかな場合は、仕様に基づいて第２変化点を定めてもよい。同様に通信データに順序が規定されている場合は、各々の通信データを第２変化点と定めてもよい。

図９に示すように、Ｓ６０３では、第２運用状態として「状態１－１」、「状態１－２」、「状態３－１」、「状態３－２」が定義される。

[0064] 図１０は状態遷移モデルより生成された通信許可リストであり、図１１はまとめ後の通信許可リストである。

図１０及び図１１を用いて、図９で説明した方法により生成された状態遷移モデルから通信許可リストを生成する方法について述べる。

まず、図１０に示すように、リスト生成部１５２は、先に生成した状態遷移モデルの各状態において、許可された通信データを抽出し、通信許可リストの表にする。このとき、遷移条件と遷移先の状態も表にまとめる。

次に、図１１に示すように、リスト生成部１５２は、図１０の通信許可リストにおいて許可された通信データに包含関係が成り立つ状態をまとめる。このとき、遷移先に規定されている状態もまとめる。例えば、図１１に示す

ように、状態１－２と状態２と状態３－２は包含関係が成り立つため、これらをまとめて状態１－２とし、対応する遷移先もまとめる。

[0065] 上述に記載の手法またはその他の手法によって、データ判定装置の外部で生成した状態遷移モデルや通信許可リストをデータ判定装置にインストールする際は、電子署名を加えてインポートし、データ判定装置で署名を検証するようにしてもよい。このような処理により、状態遷移モデルや通信許可リストの改ざんを検知することができる。電子署名としては例えばＲＳＡ署名やＥＣＤＳＡ署名を用いてもよい。

[0066] 以上のように、本実施の形態に係るデータ判定装置１０１ｂは、取得情報履歴から状態遷移モデルと通信許可リストとを生成するリスト生成部を有する。

[0067] また、リスト生成部は、状態遷移モデルと通信許可リストとの生成に以下の処理を用いる。

（１）通信データ間の経過時間が一定以上であれば待ち状態とし、待ち状態に遷移する際にタイマーをオンにし、タイマーオフにより次の状態に遷移させる処理。

（２）通信データ以外の入力が発生したらところを運用状態の変化点とし、変化点の前後を新たな運用状態とする処理。

（３）（２）で定めた運用状態において特定の通信データを変化点として、その前後を新たな運用状態とする処理。

（４）前記各運用状態において、運用状態内で通信されたデータを許可された通信データとしてリストにする処理。

（５）（３）において、前記特定の通信データを求める際に、所定のクラスタリング手法を用いる処理。

（６）前記許可された通信データに包含関係が成り立つ運用状態を１つにまとめる処理。

[0068] また、本実施の形態は、外部で生成した状態遷移モデルと通信許可リストとをデータ判定装置１０１ｂにインストールする際に、状態遷移モデルと通

信許可リストとに付与されている署名を検証して改ざんを検知する処理を有する。

[0069] ＊＊＊本実施の形態の効果の説明＊＊＊

本実施の形態に係るデータ判定装置１０１ｂによれば、実施の形態１の効果に加え、取得情報履歴から状態遷移モデルと通信許可リストとを自動生成できる。よって、設計者の負担を削減することができる。

[0070] 実施の形態３．

本実施の形態では、主に、実施の形態１，２と異なる点について説明する。

実施の形態１，２で説明した構成と同様の構成については同一の符号を付し、その説明を省略する場合がある。

[0071] 実施の形態１，２では、データ判定装置１０１はネットワーク１０２とコントローラ３００との間に接続するものであった。しかし、本実施の形態では、サーバとコントローラとの間に設置可能なデータ判定装置１０１ｃの構成について説明する。

[0072] ＊＊＊構成の説明＊＊＊

図１２を用いて、本実施の形態に係るデータ判定装置１０１ｃのブロック構成について説明する。

データ判定装置１０１ｃは、サーバである監視制御装置２００とはネットワーク１０２を介して接続され、コントローラ３００とはネットワーク１０２ａを介して接続される。データ判定装置１０１ｃは、ネットワーク１０２、ネットワーク１０２ａの各々に対応し、通信部１０７、通信部１０７ａを有する。

図１３を用いて、図１２のデータ判定装置１０１ｃとは異なる動作を行うデータ判定装置１０１ｄのブロック構成について説明する。図１３に示すようにデータ判定装置１０１ｄは、監視制御装置２００とコントローラ３００との通信を判定部１０６がキャプチャする構成でもよい。図１３に示すデータ判定装置１０１ｄでは、１つのネットワーク１０２に監視制御装置２００

とコントローラ３００とが接続されている。

[0073] ＊＊＊動作の説明＊＊＊

データ判定装置１０１ｃは、実施の形態１，２で説明したものと同様に、監視制御装置２００からコントローラ３００への通信およびコントローラ３００から監視制御装置２００への通信を判定する。データ判定装置１０１ｃの判定動作は実施の形態１と同じである。

また、データ判定装置１０１ｄの動作については実施の形態１のデータ判定装置１０１ａと同様である。ただし、通信許可リストの項目について、送信元アドレスやコマンド種別、データサイズ上限やデータ設定範囲などの他に送信先アドレスも規定するようにしてもよい。

[0074] ＊＊＊本実施の形態の効果の説明＊＊＊

実施の形態１，２では、データ判定装置１０１を各コントローラ３００に設置するため、コントローラ３００が増えるとコストが増大する。本実施の形態では、ネットワークに１つ設置すればよいためコストを削減することができる。

[0075] 上記の実施の形態では、状態管理部、判定部、警報部がそれぞれ独立した機能ブロックとしてデータ判定装置を構成している。しかし、データ判定装置は上記のような構成でなくてもよく、データ判定装置の構成は任意である。状態管理部、判定部、警報部をひとつの機能ブロックで実現してもよい。また、状態管理部、判定部を１つの機能ブロックで実現してもよいし、判定部、警報部を１つの機能ブロックで実現してもよい。

[0076] また、データ判定装置は、１つの装置でなく、複数の装置から構成されたデータ判定システムでもよい。データ判定装置の機能ブロックは、実施の形態に記載した機能を実現することができれば、任意であり、これらの機能ブロックを、他のどのような組み合わせでデータ判定装置を構成しても構わない。

[0077] また、実施の形態１～３について説明したが、これらの３つの実施の形態のうち、複数を組み合わせて実施しても構わない。あるいは、これらの３つ

の実施の形態のうち、１つの実施の形態を部分的に実施しても構わない。あるいは、これらの３つの実施の形態のうち、複数を部分的に組み合わせて実施しても構わない。その他、これらの３つの実施の形態を、全体としてあるいは部分的に、どのように組み合わせて実施しても構わない。

なお、上記の実施の形態は、本質的に好ましい例示であって、本発明、その適用物や用途の範囲を制限することを意図するものではなく、必要に応じて種々の変更が可能である。

[0078] 実施の形態４．

本実施の形態では、主に、実施の形態１と異なる点について説明する。

本実施の形態に係るデータ判定装置１０１ｅの基本的な動作は実施の形態１で説明したデータ判定装置１０１と同様であるが、通信許可リスト１１４ｅの構成、状態遷移モデル１０３１ｅの構成及び判定処理Ｓ１２０ｅの動作に実施の形態１と異なる点がある。

本実施の形態では、実施の形態１と同様の構成には同一の符号を付し、その説明を省略する場合がある。

[0079] ＊＊＊構成の説明＊＊＊

図１４を用いて、本実施の形態に係るデータ判定装置１０１ｅのブロック構成について説明する。図１４は、実施の形態１で説明した図１に相当する。

本実施の形態に係るデータ判定装置１０１ｅは、実施の形態１で説明したデータ判定装置１０１の構成に加え、フラグ管理部１７７を備える。また、実施の形態１で説明したタイマー１０４、状態管理部１０３、判定部１０６は、実施の形態１と異なる点を有するため、本実施の形態ではタイマー１０４ｅ、状態管理部１０３ｅ、判定部１０６ｅとする。

したがって、本実施の形態に係るデータ判定装置１０１ｅでは、実施の形態１で説明した「部」の機能にフラグ管理部１７７、タイマー１０４ｅ、状態管理部１０３ｅ、判定部１０６ｅの機能が加わる。

[0080] フラグ管理部１７７は、フラグを管理する。フラグ管理部１７７は、フラ

グの現在の値であるフラグ値１５を状態管理部１０３ｅと判定部１０６ｅとに入力する。また、判定部１０６ｅからフラグ設定値１６が入力される。

タイマー１０４ｅは、時間を計測する。タイマー１０４ｅは、具体的には、設定された値を一定周期、具体的には１ｍｓで減算し、値が０になった場合に減算を終了する。また、タイマー１０４ｅは、現在の値であるタイマー値１７を状態管理部１０３ｅと判定部１０６ｅとに入力する。また、判定部１０６ｅからタイマー設定値１８が入力される。本実施の形態では、タイマー１０４ｅは時間を計測する計時部１４４の一例である。なお、実施の形態１で説明したタイマー信号１０４１については記載を省略する。

[0081] 状態遷移モデル記憶部１３０には、実施の形態１で説明した状態遷移モデル１０３１とは異なる構成の状態遷移モデル１０３１ｅが格納される。

[0082] また、通信許可リスト格納部１０５には、実施の形態１で説明した通信許可リスト１１４とは異なる構成の通信許可リスト１１４ｅが格納される。通信許可リスト１１４ｅには、図１６に示すように、複数の運用状態の各運用状態において通信を許可する通信許可データ１１９ｅと、通信許可データ１１９ｅの通信が許可される許可条件１９２と、通信許可データの通信が許可された場合の許可処理１９３とを含む通信許可ルール１４が格納される。

[0083] 判定部１０６ｅは、実施の形態１で説明したように、受信データ１１１を通信部１０７から、送信データ１１２をアプリケーション３１０から取得すると共に、状態管理部１０３ｅにより保有される自装置の運用状態を、現在の運用状態１１３として取得する。また、判定部１０６ｅは、タイマー１０４ｅからタイマー値１７を、フラグ管理部１７７からフラグ値１５を取得する。判定部１０６ｅは、現在の運用状態１１３、タイマー値１７、フラグ値１５、通信許可リスト１１４ｅを用いて、通信判定データ１０９が現在の運用状態１１３において通信を許可された通信許可ルール１４に該当するか否かを判定する。

[0084] 判定部１０６ｅについてさらに説明する。

判定部１０６ｅは、受信データ１１１または送信データ１１２と、状態管

理部１０３ｅが出力する現在の運用状態１１３と、通信許可リスト格納部１０５が格納する通信許可リスト１１４ｅと、フラグ管理部１７７か管理するフラグ値１５と、タイマー１０４ｅが管理するタイマー値１７とを取得する。判定部１０６ｅは、取得した受信データ１１１または送信データ１１２と、現在の運用状態１１３と、通信許可リスト１１４ｅとフラグ値１５と、タイマー値１７とを比較し、受信データ１１１または送信データ１１２が許可されているものか否かを判定し、判定結果１１５を出力する。

[0085] 判定部１０６ｅは、通信判定データ１０９が通信許可リスト１１４ｅに含まれる通信許可ルール１４に該当すると判定した場合、通信を許可し、該当した通信許可ルール１４に記載されたアクション、すなわち許可処理１９３を実行する。具体的には、フラグ管理部１７７に対して通信許可ルール１４に記載されたフラグ許可値をフラグ設定値１６として設定したり、タイマー１０４ｅに対して通信許可ルール１４に記載されたタイマー許可値をタイマー設定値１８として設定したりする。

判定部１０６ｅは、通信判定データ１０９が通信許可ルール１４に該当しないと判定した場合、通信を遮断する。つまり、判定部１０６ｅは、判定結果１１５が異常の場合、通信を遮断する。

[0086] 警報部１０８は、判定部１０６ｅにより通信判定データ１０９が通信許可ルール１４に該当しないと判定された場合、異常を検知したことを示す警報を出力する。つまり、警報部１０８は、実施の形態１と同様に、判定結果１１５が異常の場合に警報を発する。

[0087] 状態管理部１０３ｅは、判定部１０６ｅにより通信判定データ１０９が通信許可ルール１４に該当すると判定された場合、状態遷移モデル１０３１ｅ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１０３ｅは、判定部１０６ｅにより通信判定データ１０９が通信許可ルール１４に該当しないと判定された場合、自装置の運用状態を異常状態に遷移させる。

なお、状態管理部１０３ｅは、実施の形態１と同様に、正常と判定された

場合に状態を遷移するのみでもよい。

以上のように、状態管理部１０３ｅは、自装置であるデータ判定装置１０１ｅの現在の運用状態１１３を保有する。

[0088] 図１５を用いて、図１４のデータ判定装置１０１ｅとは異なる動作を行うデータ判定装置１０１ｅａのブロック構成について説明する。図１５は、実施の形態１で説明した図２に相当する。

実施の形態１で説明した図２と同様に、図１５に示すデータ判定装置１０１ｅａのように監視制御装置２００とアプリケーション３１０との通信を判定部１０６ｅがキャプチャする構成でもよい。図１５のデータ判定装置１０１ｅａでは、判定結果１１５が異常の場合、判定部１０６ｅが通信を遮断することができない。しかし、警報部１０８により発せられた警報により、攻撃に対する対処を行うことができる。

[0089] 図１６を用いて、本実施の形態に係る通信許可リスト１１４ｅの構成について説明する。

図１６は、状態管理部１０３ｅの保持するそれぞれの運用状態において許可された通信許可リスト１１４ｅの例である。図１６の通信許可リスト１１４ｅは一例であり、必ずしも図１６の通りでなくてもよい。

[0090] 図１６に示すように、通信許可リスト１１４ｅは、運用状態、ルール番号、受信データ条件、アクションといった項目を有する。受信データ条件は、通信許可データ１１９ｅと許可条件１９２とを有する。

通信許可データ１１９ｅには、実施の形態１と同様に、送信元アドレス、コマンド種別、データサイズ上限、データ設定範囲といった情報が設定される。

許可条件１９２は、通信許可データ１１９ｅの通信を許可する計時部１４４の値の範囲であるタイマー許可値１９２１と、通信許可データ１１９ｅの通信を許可するフラグの値であるフラグ許可値１９２２とを有する。

また、アクションは、通信許可データ１１９ｅの通信が許可された場合の許可処理１９３である。アクションは、通信許可データ１１９ｅの通信が許

可された場合に計時部１４４に設定するタイマー設定値１８と、通信許可データ１１９ｅの通信が許可された場合にフラグに設定するフラグ設定値１６とを有する。

なお、これらの項目は任意であり、通信を許可する通信データを特定することができる項目であれば、上記以外の項目でも構わない。

[0091] 図１６では、具体的には、運用状態がＮＷ構築の場合、ルール１，２のみ許可し、それ以外のルールを許可しないことを意味する。また、運用状態が運転Ａの場合、ルール３ａ，３ｂ，３ｃ，７，４のみ許可し、それ以外のルールを許可しないことを意味する。また、また、運用状態が異常の場合はすべての通信を許可しないことを意味している。

また、通信許可ルール１４とは、運用状態における通信の許否が設定された通信許可リスト１１４ｅの各行のことである。図１６では、通信許可ルール１４としてルール１からルール１０までが設定されている。運用状態が異常の場合はすべての通信を許可しないことを意味している。

[0092] 図１７を用いて、本実施の形態に係るデータ判定装置１０１ｅの状態遷移モデル１０３１ｅの一例について説明する。図１７は一例であり、状態遷移モデル１０３１ｅは必ずしも図１７の通りでなくてもよい。

図１７において、実施の形態１と同様に、各状態３０１から３０６は、複数の運用状態の例である。また、各状態間は、複数の運用状態の各運用状態間の例である。

図１７では、データ判定装置１０１ｅは、電源投入時にＮＷ構築状態３０１に遷移し、ＮＷ構築に必要な通信を行う。データ判定装置１０１ｅにおいて、ＮＷ構築に必要な通信に適用されるルールをルール１とする。なお、以下の説明においてもネットワーク構築をＮＷ構築と記載する。状態遷移モデル１０３１ｅでは、ＮＷ構築が完了し、ルール２が適用されたら運転Ａ状態３０２に移行する。

[0093] 状態遷移モデル１０３１ｅは、通信データの順番が規定された通信が存在する場合、規定された通信の順番に従って運転状態をさらに定義する。規定

された通信の具体例としては、「パラメータファイル送信」、「パラメータファイル設定」、「ベリファイ」の順番で受信すると規定された通信がある。状態遷移モデル１０３１ｅでは、運転Ａ状態３０２で「パラメータファイル送信」を判定するルール４が適用されると運転Ｂ状態３０３に遷移し、ルール５が適用されると運転Ｃ状態３０４に遷移し、ルール６が適用されると運転Ａ状態３０２に遷移するように定義されている。このように、それぞれの運転状態への遷移条件をルール４，５，６に割り当てるようにしてもよい。

[0094] 以下において、タイマー値１７をＴ１とし、フラグ値１５をＦ１として説明する。

運転Ａ状態３０２において、コマンド受信後に一定時間を空ける必要のある通信が存在する場合がある。具体的には図１６におけるルール７の「運転データ設定」である。ルール７では、許可条件１９２のようにＴ１がタイマー許可値１９２１に設定された０であること、すなわちＴ１＝０を条件に「運転データ設定」を受け入れ、許可処理１９３のようにＴ１に所定の値を設定する。具体的には、１ｍｓごとに減算するタイマーで１００ｍｓの間隔をあける場合は、Ｔ１にタイマー設定値１８である１００を設定する。すなわち、Ｔ１＝１００とする。

[0095] また、運転Ａ状態３０２において、ｂ秒間隔（誤差±ｄ秒）でコマンドを受信する必要がある通信、具体的には図１６におけるルール３ａ，３ｂの「状態データ取得」である。ルール３ａ，３ｂでは、Ｔ１及びＦ１の各々が許可条件１９２に設定されている許可値に合致した場合に通信を許可し、Ｔ１及びＦ１の各々に許可処理１９３に設定されている設定値を設定する。また、状態データ取得を終了する際は、ルール３ｃのように状態データ取得終了コマンドを発行し、この状態データ取得終了コマンドを受信した際に、Ｔ１及びＦ１をクリアする。すなわち、Ｔ１及びＦ１の各々に許可処理１９３に設定されている設定値である０を設定する。さらに、図１７に示すように、運転Ａ状態３０２において、Ｆ１が１でかつＴ１が０になった場合に異常状

態３０６に遷移してもよい。

[0096] また、運転Ａ状態３０２において、人の操作１により保守状態３０５に移行し、保守に必要な通信、具体的にはプログラム更新やベリファイを行うようにしてもよい。保守状態３０５において、保守が完了し、ルール１０が適用されたら運転Ａ状態３０２に移行する。さらに、通信データによる状態遷移を行う際は、判定部１０６ｅの判定結果が正常であった場合のみ遷移するようにしてもよい。各状態において、判定部１０６ｅの判定結果が異常であったら、異常状態３０６に遷移してもよい。

[0097] ＊＊＊動作の説明＊＊＊

図１８を用いて、本実施の形態に係るデータ判定装置１０１ｅのデータ判定方法、データ判定処理Ｓ１００ｅについて説明する。データ判定処理Ｓ１００ｅにおいて、実施の形態１のデータ判定処理Ｓ１００と異なる点は判定処理Ｓ１２０ｅである。判定処理Ｓ１２０ｅ以外の処理は実施の形態１と同様であるため、簡潔に説明する。

[0098] 上述したように、データ判定装置１０１ｅは、状態遷移モデル１０３１ｅを記憶する状態遷移モデル記憶部１３０と、通信許可ルール１４を通信許可リスト１１４ｅとして格納する通信許可リスト格納部１０５とを備える。

[0099] 状態管理処理Ｓ１０１において、状態管理部１０３ｅは、状態遷移モデル１０３１ｅ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。状態管理部１０３ｅは、状態遷移モデル１０３１ｅに基づい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。

[0100] 通信処理Ｓ１１０は、実施の形態１で説明したものと同様である。

[0101] 判定処理Ｓ１２０ｅにおいて、判定部１０６ｅは、通信処理Ｓ１１０により取得された通信判定データ１０９を取得すると共に状態管理処理Ｓ１０１により保有される自装置の運用状態を現在の運用状態１１３として取得する。また、判定部１０６ｅは、タイマー１０４ｅよりタイマー値１７を、フラグ管理部１７７よりフラグ値１５を取得する。判定部１０６ｅは、現在の運用状態１１３、タイマー値１７、フラグ値１５、通信許可リスト１１４ｅを

用いて、通信判定データ１０９が現在の運用状態１１３において通信許可ルール１４に該当するか否かを判定する。

具体的には、判定部１０６ｅは、タイマー値１７がタイマー許可値１９２１の範囲内であるか否かの判定結果を用いて、通信判定データ１０９が通信許可ルール１４に該当するか否かを判定する。また、判定部１０６ｅは、タイマー値１７がタイマー許可値１９２１の範囲内であるか否か、フラグ値１５がフラグ許可値１９２２であるか否かの判定結果を用いて、通信判定データ１０９が通信許可ルール１４に該当するか否かを判定してもよい。すなわち、図１６に示すように、判定部１０６ｅは、通信判定データ１０９が通信許可データ１１９ｅであると判定した場合、許可条件１９２を満たしているか否かの判定結果に基づいて、通信判定データ１０９が通信許可ルール１４に該当するか否かを示す判定結果１１５を出力する。

[0102] Ｓ１３０において、判定結果１１５が正常、すなわち通信判定データ１０９が通信許可ルール１４に該当する場合、正常処理Ｓ１４０に進む。

Ｓ１３０において、判定結果１１５が異常、すなわち通信判定データ１０９が通信許可ルール１４に該当しない場合、異常処理Ｓ１５０に進む。

[0103] 正常処理Ｓ１４０において、状態管理部１０３ｅは、取得した通信判定データ１０９と状態遷移モデル１０３１ｅとに基づいて、自装置の運用状態を遷移させる。

異常処理Ｓ１５０において、状態管理部１０３ｅは、自装置の運用状態を異常状態に遷移させる。

[0104] 次に、図１９を用いて、判定部１０６ｅによる判定処理Ｓ１２０ｅについて説明する。判定処理Ｓ１２０ｅにおいて、実施の形態１の判定処理Ｓ１２０と異なる点はＳ１２３ｅ，Ｓ１２４ｅである。Ｓ１２３ｅ，Ｓ１２４ｅ以外の処理は実施の形態１と同様であるため、簡潔に説明する。

[0105] Ｓ１２１において、判定部１０６ｅは、受信データ１１１あるいは送信データ１１２を通信判定データ１０９として取得する。判定部１０６ｅは、通信判定データ１０９の中身を解析し、判定に必要な要素を抽出する。抽出さ

れる要素は、通信許可リスト１１４ｅに記載されている項目であり、送信元アドレス、コマンド種別といった情報である。

[0106] Ｓ１２２において、判定部１０６ｅは、状態管理部１０３ｅから現在の運用状態１１３を取得する。また、判定部１０６ｅは、通信許可リスト格納部１０５から通信許可リスト１１４ｅを取得する。

[0107] Ｓ１２３ｅにおいて、判定部１０６ｅは、現在の運用状態１１３と通信許可リスト１１４ｅとに基づいて、通信判定データ１０９が現在の運用状態１１３において許可されている通信データ、すなわち通信許可ルール１４に該当するか否かを判定する。

通信判定データ１０９が通信許可ルール１４に該当すると判定されると、Ｓ１２４ｅに進む。

通信判定データ１０９がいずれの通信許可ルール１４にも該当しないと判定されると、Ｓ１２５に進む。

Ｓ１２５において、判定部１０６ｅは、異常の判定結果１１５を出力し、通信判定データ１０９の通信を遮断する。あるいは、判定部１０６ｅは、異常の判定結果１１５を出力するだけで、通信判定データ１０９の通信を遮断しなくてもよい。この処理は実施の形態１で説明したものと同様である。

[0108] Ｓ１２４ｅにおいて、判定部１０６ｅは、通信を許可すると共に、通信判定データ１０９が該当した通信許可ルール１４に対応するアクションがあれば、そのアクションを実行する。すなわち、判定部１０６ｅは、正常の判定結果１１５を出力し、通信を許可すると共に、通信判定データ１０９が該当した通信許可ルール１４に対応するアクションがあれば、そのアクションを実行する。具体的には、判定部１０６ｅは、フラグ管理部１７７にフラグ設定値１６をセットしたり、タイマー１０４ｅにタイマー設定値１８をセットしたりする。

[0109] 以下に、判定処理Ｓ１２０ｅについて具体例を用いて説明する。

データ判定装置１０１ｅが、ルール４，５，６に該当する通信判定データ１０９を受信した場合について説明する。

データ判定装置１０１ｅが、運転Ａ状態３０２において通信判定データ１０９を受信し、通信判定データ１０９の送信元アドレスとコマンド種別とデータサイズとから通信判定データ１０９がルール４の「パラメータファイル送信」であると判定したとする。データ判定装置１０１ｅは、通信を許可すると共に、運転状態を運転Ｂ状態３０３に遷移する。

データ判定装置１０１ｅが、運転Ｂ状態３０３において通信判定データ１０９を受信し、通信判定データ１０９の送信元アドレスとコマンド種別とデータサイズとから通信判定データ１０９がルール５の「パラメータファイル設定」であると判定したとする。データ判定装置１０１ｅは、通信を許可すると共に、運転状態を運転Ｃ状態３０４に遷移する。

データ判定装置１０１ｅが、運転Ｃ状態３０４において通信判定データ１０９を受信し、通信判定データ１０９の送信元アドレスとコマンド種別とデータサイズとから通信判定データ１０９がルール６の「ベリファイ」であると判定したとする。データ判定装置１０１ｅは、通信を許可すると共に、運転状態を運転Ａ状態３０２に遷移する。

[0110] 次に、データ判定装置１０１ｅが、ルール７に該当する通信判定データ１０９を受信した場合について説明する。

データ判定装置１０１ｅが、運転Ａ状態３０２において通信判定データ１０９を受信し、通信判定データ１０９の送信元アドレスとコマンド種別とデータサイズとデータ設定範囲とタイマー値１７とフラグ値１５とから、通信判定データ１０９がルール７の「運転データ設定」であると判定したとする。データ判定装置１０１ｅは、通信を許可すると共に、タイマー設定値を１００ｍｓとする。

このように判定処理Ｓ１２０ｅを行うことにより、コマンド受信後に一定時間を空ける必要のある通信についても正常かどうかの判定をすることができる。

[0111] 次に、データ判定装置１０１ｅが、ルール３ａ，３ｂ，３ｃに該当する通信判定データ１０９を受信した場合について説明する。ルール３ａ，３ｂ，

３ｃは、運転Ａ状態３０２において、約ｂ秒間隔でコマンドを受信する必要がある通信である。この通信では、ｂ秒に±ｄ秒の誤差を許容するものとする。

データ判定装置１０１ｅが、運転Ａ状態３０２において通信判定データ１０９を受信し、通信判定データ１０９の送信元アドレスとコマンド種別とデータサイズと、タイマー値１７及びフラグ値１５とから通信判定データ１０９がルール３ａの「状態データ取得」であると判定したとする。データ判定装置１０１ｅは、通信を許可すると共に、タイマー１０４ｅの値であるＴ１にｂ＋ｄを設定し、フラグの値であるＦ１を１とする。

データ判定装置１０１ｅが、運転Ａ状態３０２において通信判定データ１０９を受信し、通信判定データ１０９の送信元アドレスとコマンド種別とデータサイズと、タイマー値１７及びフラグ値１５とから通信判定データ１０９がルール３ｂの「状態データ取得」であると判定したとする。データ判定装置１０１ｅは、通信を許可すると共に、Ｔ１にｂ＋Ｔ１を設定する。

データ判定装置１０１ｅが、運転Ａ状態３０２において通信判定データ１０９を受信し、通信判定データ１０９の送信元アドレスとコマンド種別とデータサイズと、タイマー値１７及びフラグ値１５とから通信判定データ１０９がルール３ｃの「状態データ取得終了」であると判定したとする。データ判定装置１０１ｅは、通信を許可すると共に、Ｔ１とＦ１とを０に初期化する。

このように判定処理Ｓ１２０ｅを行うことにより、一定間隔でコマンドを受信する必要がある通信についても正常かどうかの判定をすることができる。

[0112] 次に、データ判定装置１０１ｅが、人の操作により保守状態に移行し、ルール８，９，１０に該当する通信判定データ１０９を受信した場合について説明する。ルール８，９，１０は、保守状態３０５において、保守に必要な通信である。

データ判定装置１０１ｅが、保守状態３０５において通信判定データ１０

９を受信し、通信判定データ１０９の送信元アドレスとコマンド種別とデータサイズとから通信判定データ１０９がルール８の「プログラム更新」であると判定したとする。データ判定装置１０１ｅは、通信を許可する。

データ判定装置１０１ｅが、保守状態３０５において通信判定データ１０９を受信し、通信判定データ１０９の送信元アドレスとコマンド種別とデータサイズとから通信判定データ１０９がルール９の「ベリファイ」であると判定したとする。データ判定装置１０１ｅは、通信を許可する。

データ判定装置１０１ｅが、保守状態３０５において通信判定データ１０９を受信し、通信判定データ１０９の送信元アドレスとコマンド種別とデータサイズとから通信判定データ１０９がルール９の「保守完了」であると判定したとする。データ判定装置１０１ｅは、通信を許可すると共に、運転状態を運転Ａ状態３０２に遷移する。

[0113] 以上で、本実施の形態に係るデータ判定装置１０１ｅのデータ判定方法、データ判定処理Ｓ１００ｅについての説明を終わる。

[0114] 以上のように、本実施の形態に係るデータ判定装置は、以下の構成を有する。

（Ａ）通信データと外部操作とタイマーとの少なくともいずれか１つの要素によって遷移する状態遷移モデルに従い、運用状態を管理する状態管理部。

（Ｂ）運用状態ごとに許可する通信データを定めた通信許可リストを格納する通信許可リスト格納部。

（Ｃ）状態管理部が出力する現在の運用状態と通信許可リスト格納部が格納している通信許可リストとタイマーの値とフラグの値とを用いて、データ判定装置に入力された通信データが正常か否かを判定する判定部。

（Ｄ）判定部が出力する判定結果をもとに警報を発する警報部。

また、状態管理部は、判定部が出力する判定結果によって遷移する状態遷移モデルに従い、運用状態を管理する。判定部は、異常と判断した通信データを遮断する。さらに判定部は、正常と判断した際に通信許可ルールに記載されたアクションを実行する。すなわち、判定部は、正常と判断した際に、

タイマーおよびフラグの少なくともいずれかを所定の値に設定する。

[0115] ＊＊＊本実施の形態の効果の説明＊＊＊

比較のために先に述べたＳｔｕｘｎｅｔのような攻撃では、乗っ取られたサーバがコントローラに対しプログラム書き換えを行っている。プログラム書き換え自体は正常通信であり、乗っ取られたサーバも正常と定義されたサーバであるため、ホワイトリスト型対策では防ぐことができない。

一方、本実施の形態に係るデータ判定装置では、通信データだけでなく人の操作やタイマーによる運用状態の遷移をも定義している。よって、保守状態の時のみプログラム書き換えを受け付けるようにし、保守状態への遷移は人の操作によってのみ行われるように対策をすることで、上記のような攻撃を検知することができる。

また、Ｓｔｕｘｎｅｔによってプログラムを書き換えられたコントローラは、制御対象の周波数コンバータに対し高頻度で周波数を変更するコマンドを送信することで機器の故障を誘発する。本実施の形態に係るデータ判定装置では、タイマーによってそのような高頻度の周波数変更コマンドを検知することができる。

[0116] また、本実施の形態に係るデータ判定装置によれば、正しい通信順からの逸脱を検知することができる。

[0117] 本実施の形態に係るデータ判定装置によれば、受信間隔が一定か否かを検知できるので、断線や攻撃による監視制御装置の停止といった事象も検知できる。その際、複数の通信の受信間隔を管理する場合においても、状態遷移図の記述を単純化でき、検知に係るリソースを抑えることができる。受信間隔の制御を状態遷移だけで行おうとすると、対象となる通信数ｎに対しての状態数$n^2$を管理しなければならない。しかし、本実施の形態に係るデータ判定装置によれば、１つの状態で管理できる。

[0118] さらに、本実施の形態に係るデータ判定装置によれば、攻撃を受けた監視制御装置が、本来発行しないはずのコマンド発行や、運用上、データ取得を行わない監視制御装置からのデータ取得も検知できる。

[0119] なお、実施の形態１～３に加えて、実施の形態４について説明したが、これらの４つの実施の形態のうち、複数を組み合わせて実施しても構わない。あるいは、これらの４つの実施の形態のうち、１つの実施の形態を部分的に実施しても構わない。あるいは、これらの４つの実施の形態のうち、複数を部分的に組み合わせて実施しても構わない。その他、これらの４つの実施の形態を、全体としてあるいは部分的に、どのように組み合わせて実施しても構わない。

なお、上記の実施の形態は、本質的に好ましい例示であって、本発明、その適用物や用途の範囲を制限することを意図するものではなく、必要に応じて種々の変更が可能である。

## 符号の説明

[0120] １０１，１０１ａ，１０１ｂ，１０１ｃ，１０１ｄ，１０１ｅ，１０１ｅａ データ判定装置、１０２，１０２ａ ネットワーク、１０３，１０３ｅ 状態管理部、１０４，１０４ｅ タイマー、１０５ 通信許可リスト格納部、１０６，１０６ｅ 判定部、１０７，１０７ａ 通信部、１０８ 警報部、１０９ 通信判定データ、１１０ 操作部、１１１ 受信データ、１１２ 送信データ、１１３ 現在の運用状態、１１４，１１４ｅ 通信許可リスト、１１５ 判定結果、１１９，１１９ｅ 通信許可データ、１３０ 状態遷移モデル記憶部、１５１ 取得情報履歴、１５２ リスト生成部、１５３ 履歴記憶部、２００ 監視制御装置、３００ コントローラ、３０１，３０２，３０３，３０４，３０５，３０６，３０７ 状態、３１０ アプリケーション、５００ データ判定システム、７０１ 第１変化点、７０２ 第２変化点、７０３ 遷移通信データ、９０１ プロセッサ、９０２ 補助記憶装置、９０３ メモリ、９０４ 通信装置、９０５ 入力インタフェース、９０６ ディスプレイインタフェース、９０７ 入力装置、９０８ ディスプレイ、９１０ 信号線、９１１，９１２ ケーブル、９０４１ レシーバー、９０４２ トランスミッター、１０３１，１０３１ｅ 状態遷移モデル、１０３２ 自装置の運用状態、１０３３ 取得情報、１０４１ タイ

マー信号、１１０１　操作信号、３００１　複数の運用状態、３００２　複数の運用状態の各運用状態間、Ｓ１０１　状態管理処理、Ｓ１００，Ｓ１００ｅ　データ判定処理、Ｓ１１０　通信処理、Ｓ１２０，Ｓ１２０ｅ　判定処理、Ｓ１４０　正常処理、Ｓ１５０　異常処理、１４４　計時部、１４　通信許可ルール、１５　フラグ値、１６　フラグ設定値、１７　タイマー値、１８　タイマー設定値、１７７　フラグ管理部、１９２　許可条件、１９３　許可処理、１９２１　タイマー許可値、１９２２　フラグ許可値。

# 請求の範囲

[請求項1] 複数の運用状態の各運用状態間の状態遷移を表す状態遷移モデルを記憶する状態遷移モデル記憶部と、

前記状態遷移モデルに基づいて、自装置の運用状態を保有する状態管理部と、

前記複数の運用状態の各運用状態において通信を許可する通信許可データを通信許可リストとして格納する通信許可リスト格納部と、

通信データを通信判定データとして取得する通信部と、

前記通信部により取得された通信判定データを取得すると共に前記状態管理部により保有される前記自装置の運用状態を現在の運用状態として取得し、前記現在の運用状態と前記通信許可リストとを用いて、前記通信判定データが前記現在の運用状態において通信を許可された通信許可データであるか否かを判定する判定部と

を備えるデータ判定装置。

[請求項2] 前記データ判定装置は、

前記判定部により前記通信判定データが前記通信許可データでないと判定された場合、異常を検知したことを示す警報を出力する警報部を備える請求項１に記載のデータ判定装置。

[請求項3] 前記判定部は、

前記通信判定データが前記通信許可データでないと判定した場合、通信を遮断する請求項１または２に記載のデータ判定装置。

[請求項4] 前記状態管理部は、

前記判定部により前記通信判定データが前記通信許可データであると判定された場合、前記状態遷移モデルに基づいて前記自装置の運用状態を遷移させる請求項１から３のいずれか１項に記載のデータ判定装置。

[請求項5] 前記状態管理部は、

前記判定部により前記通信判定データが前記通信許可データでない

と判定された場合、前記自装置の運用状態を異常状態に遷移させる請求項１から４のいずれか１項に記載のデータ判定装置。

[請求項6] 前記データ判定装置は、

前記自装置の運用状態が継続する時間を計測するタイマーを備え、

前記状態遷移モデル記憶部は、

自装置が取得した取得情報に応じて前記複数の運用状態の各運用状態間を遷移する前記状態遷移モデルを記憶し、

前記取得情報は、通信により取得される通信データと自装置に対する操作を受け付けたことを示す操作信号と前記タイマーから出力されるタイマー信号とを含む請求項１から５のいずれか１項に記載のデータ判定装置。

[請求項7] 前記データ判定装置は、

前記取得情報の履歴を取得情報履歴として記憶する履歴記憶部と、

前記取得情報履歴に基づいて、前記状態遷移モデルと前記通信許可リストとを生成するリスト生成部とを備える請求項６に記載のデータ判定装置。

[請求項8] 前記リスト生成部は、

前記取得情報履歴に含まれる連続する通信データ間の経過時間が第１時間以上であれば待ち状態を設定し、通信データ以外の取得情報を取得した時点を第１変化点とし、前記第１変化点の前後を第１運用状態とし、各第１運用状態において運用状態が遷移すると判定された遷移通信データを取得した時点を第２変化点として、前記第２変化点の前後を第２運用状態として前記状態遷移モデルを生成する請求項７に記載のデータ判定装置。

[請求項9] 前記リスト生成部は、

前記状態遷移モデルに含まれる各運用状態において通信された通信データを前記通信許可データとして前記通信許可リストに設定する請求項８に記載のデータ判定装置。

[請求項10] 前記リスト生成部は、

クラスタリング手法を用いて前記遷移通信データを抽出する請求項８または９に記載のデータ判定装置。

[請求項11] 複数の運用状態の各運用状態間の状態遷移を表す状態遷移モデルを記憶する状態遷移モデル記憶部と、前記複数の運用状態の各運用状態において通信を許可する通信許可データを通信許可リストとして格納する通信許可リスト格納部とを備えるデータ判定装置のデータ判定方法において、

状態管理部が、前記状態遷移モデルに基づいて、自装置の運用状態を保有し、

通信部が、通信データを通信判定データとして取得し、

判定部が、前記通信部により取得された通信判定データを取得すると共に前記状態管理部により保有される前記自装置の運用状態を現在の運用状態として取得し、前記現在の運用状態と前記通信許可リストとを用いて、前記通信判定データが前記現在の運用状態において通信を許可された通信許可データであるか否かを判定するデータ判定方法。

[請求項12] 複数の運用状態の各運用状態間の状態遷移を表す状態遷移モデルを記憶する状態遷移モデル記憶部と、前記複数の運用状態の各運用状態において通信を許可する通信許可データを通信許可リストとして格納する通信許可リスト格納部とを備えるデータ判定装置のプログラムにおいて、

前記状態遷移モデルに基づいて、自装置の運用状態を保有する状態管理処理と、

通信データを通信判定データとして取得する通信処理と、

前記通信処理により取得された通信判定データを取得すると共に前記状態管理処理により保有される前記自装置の運用状態を現在の運用状態として取得し、前記現在の運用状態と前記通信許可リストとを用

いて、前記通信判定データが前記現在の運用状態において通信を許可された通信許可データであるか否かを判定する判定処理と
をコンピュータに実行させるプログラム。

[請求項13] 複数の運用状態の各運用状態間の状態遷移を表す状態遷移モデルを記憶する状態遷移モデル記憶部と、

前記状態遷移モデルに基づいて、自装置の運用状態を保有する状態管理部と、

前記複数の運用状態の各運用状態において通信を許可する通信許可データと、前記通信許可データの通信が許可される許可条件と、前記通信許可データの通信が許可された場合の許可処理とを含む通信許可ルールを通信許可リストとして格納する通信許可リスト格納部と、

時間を計測する計時部と、

通信データを通信判定データとして取得する通信部と、

前記通信部により取得された通信判定データと、前記状態管理部により保有される前記自装置の運用状態である現在の運用状態と、前記計時部の現在の値であるタイマー値とを取得し、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値とを用いて、前記通信判定データが前記現在の運用状態において通信を許可された通信許可ルールに該当するか否かを判定する判定部と
を備えるデータ判定装置。

[請求項14] 前記通信許可リスト格納部は、

前記許可条件として、前記通信許可データの通信を許可する前記計時部の値の範囲であるタイマー許可値を格納し、前記許可処理として、前記通信許可データの通信が許可された場合に前記計時部に設定するタイマー設定値を格納し、

前記判定部は、

前記タイマー値が前記タイマー許可値の範囲内であるか否かの判定結果を用いて、前記通信判定データが前記通信許可ルールに該当する

か否かを判定する請求項１３に記載のデータ判定装置。

[請求項15] 前記データ判定装置は、さらに、

フラグを管理するフラグ管理部を備え、

前記判定部は、

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値と前記フラグの現在の値であるフラグ値とを取得し、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値と前記フラグ値とを用いて、前記通信判定データが前記現在の運用状態において通信を許可された通信許可ルールに該当するか否かを判定する請求項１３または１４に記載のデータ判定装置。

[請求項16] 前記通信許可リスト格納部は、

前記許可条件として、さらに、前記通信許可データの通信を許可する前記フラグの値であるフラグ許可値を格納し、前記許可処理として、さらに、前記通信許可データの通信が許可された場合に前記フラグに設定するフラグ設定値を格納し、

前記判定部は、

前記フラグ値が前記フラグ許可値であるか否かの判定結果を用いて、前記通信判定データが前記通信許可ルールに該当するか否かを判定する請求項１５に記載のデータ判定装置。

[請求項17] 前記データ判定装置は、

前記判定部により前記通信判定データが前記通信許可ルールに該当しないと判定された場合、異常を検知したことを示す警報を出力する警報部を備える請求項１３から１６のいずれか１項に記載のデータ判定装置。

[請求項18] 前記判定部は、

前記通信判定データが前記通信許可ルールに該当しないと判定した場合、通信を遮断する請求項１３から１７のいずれか１項に記載のデータ判定装置。

[請求項19] 前記状態管理部は、

前記判定部により前記通信判定データが前記通信許可ルールに該当すると判定された場合、前記状態遷移モデルに基づいて前記自装置の運用状態を遷移させる請求項１３から１８のいずれか１項に記載のデータ判定装置。

[請求項20] 複数の運用状態の各運用状態間の状態遷移を表す状態遷移モデルを記憶する状態遷移モデル記憶部と、前記複数の運用状態の各運用状態において通信を許可する通信許可データと、前記通信許可データの通信が許可される許可条件と、前記通信許可データの通信が許可された場合の許可処理とを含む通信許可ルールを通信許可リストとして格納する通信許可リスト格納部とを備えるデータ判定装置のデータ判定方法において、

状態管理部が、前記状態遷移モデルに基づいて、自装置の運用状態を保有し、

通信部が、通信データを通信判定データとして取得し、

判定部が、前記通信部により取得された通信判定データと、前記状態管理部により保有される前記自装置の運用状態である現在の運用状態と、時間を計測する計時部の現在の値であるタイマー値とを取得し、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値とを用いて、前記通信判定データが前記現在の運用状態において通信を許可された通信許可ルールに該当するか否かを判定するデータ判定方法。

[請求項21] 複数の運用状態の各運用状態間の状態遷移を表す状態遷移モデルを記憶する状態遷移モデル記憶部と、前記複数の運用状態の各運用状態において通信を許可する通信許可データと、前記通信許可データの通信が許可される許可条件と、前記通信許可データの通信が許可された場合の許可処理とを含む通信許可ルールを通信許可リストとして格納する通信許可リスト格納部とを備えるデータ判定装置のプログラムにおいて、

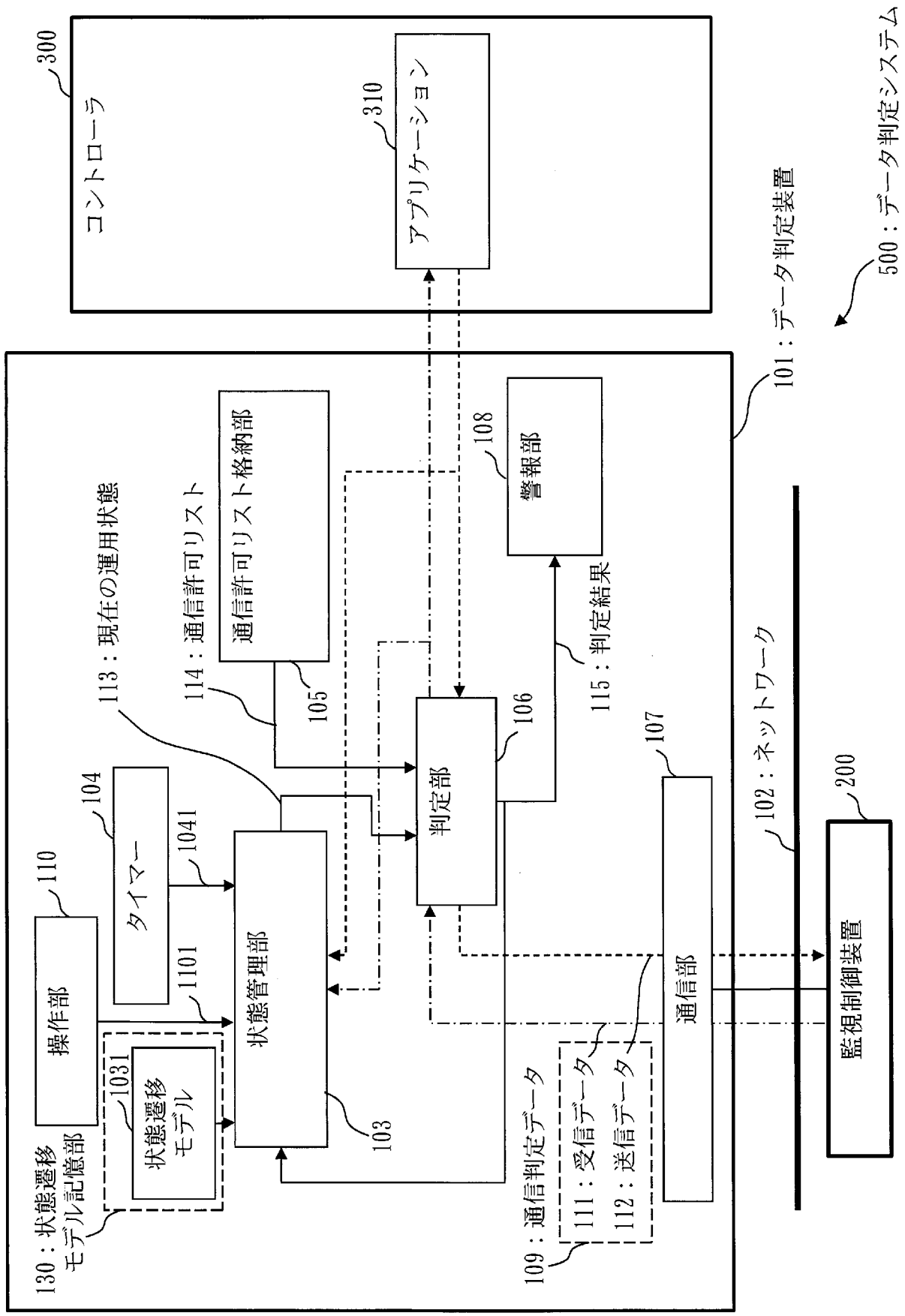
前記状態遷移モデルに基づいて、自装置の運用状態を保有する状態管理処理と、

通信データを通信判定データとして取得する通信処理と、

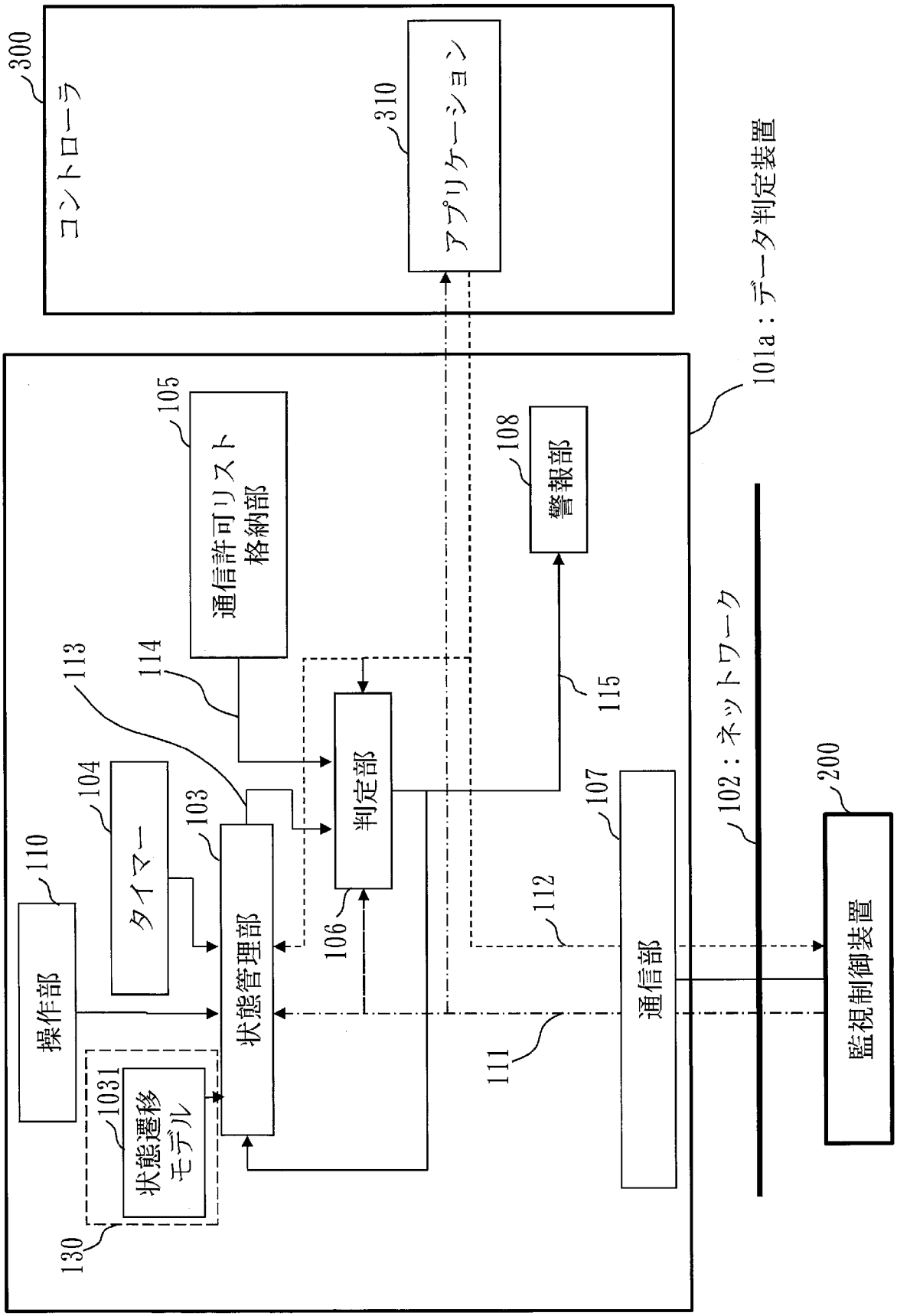
前記通信処理により取得された通信判定データと、前記状態管理処理により保有される前記自装置の運用状態である現在の運用状態と、時間を計測する計時部の現在の値であるタイマー値とを取得し、前記現在の運用状態と前記通信許可リストと前記タイマー値とを用いて、前記通信判定データが前記現在の運用状態において通信を許可された通信許可ルールに該当するか否かを判定する判定処理と

をコンピュータに実行させるプログラム。

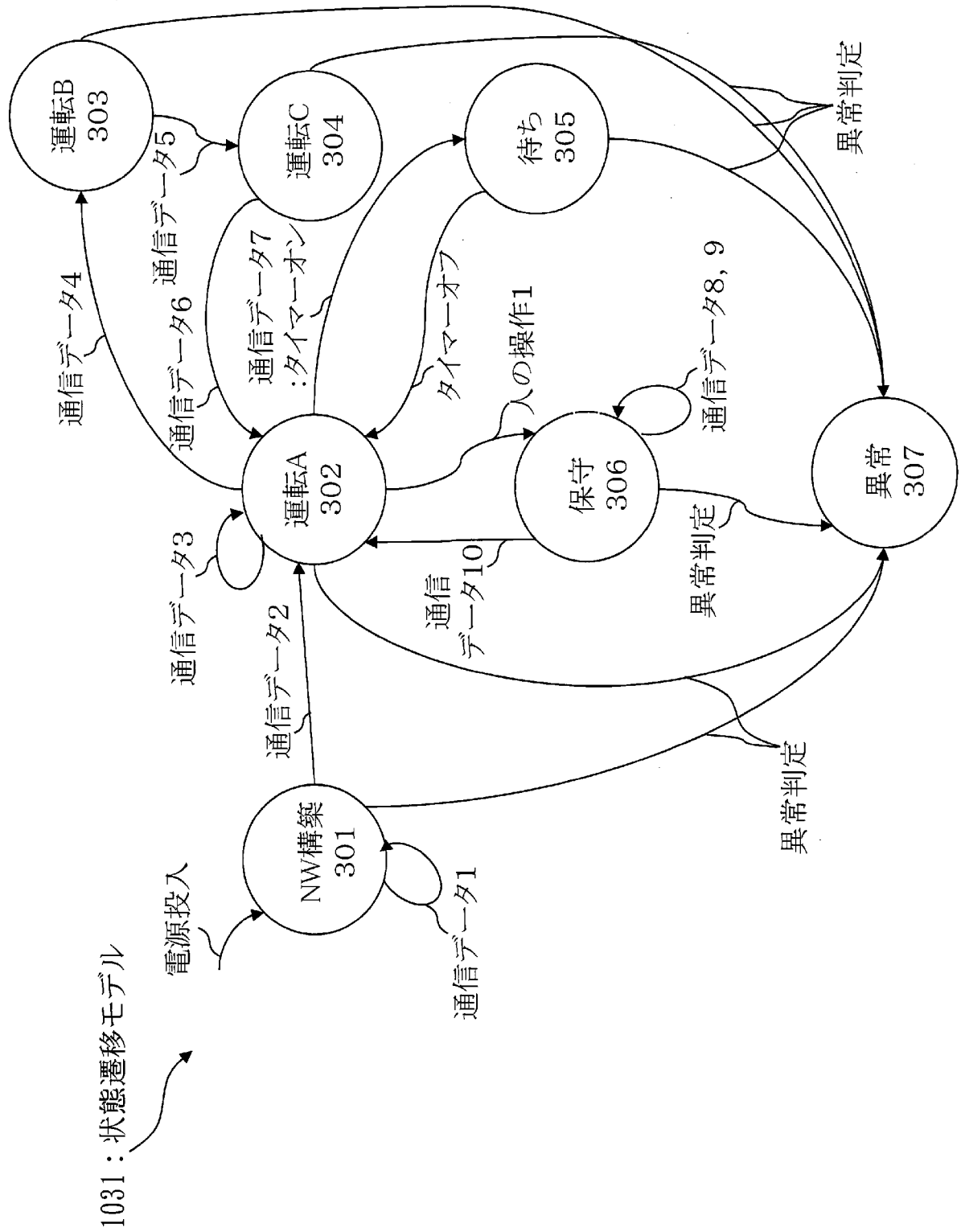
[図1]


500：データ判定システム
101：データ判定装置
300
コントローラ
310
アプリケーション
102：ネットワーク
200
監視制御装置
107
通信部
109：通信判定データ
111：受信データ
112：送信データ
106
判定部
115：判定結果
108
警報部
105
通信許可リスト格納部
114：通信許可リスト
113：現在の運用状態
103
状態管理部
1041
1101
104
タイマー
110
操作部
1031
状態遷移
モデル
130：状態遷移
モデル記憶部

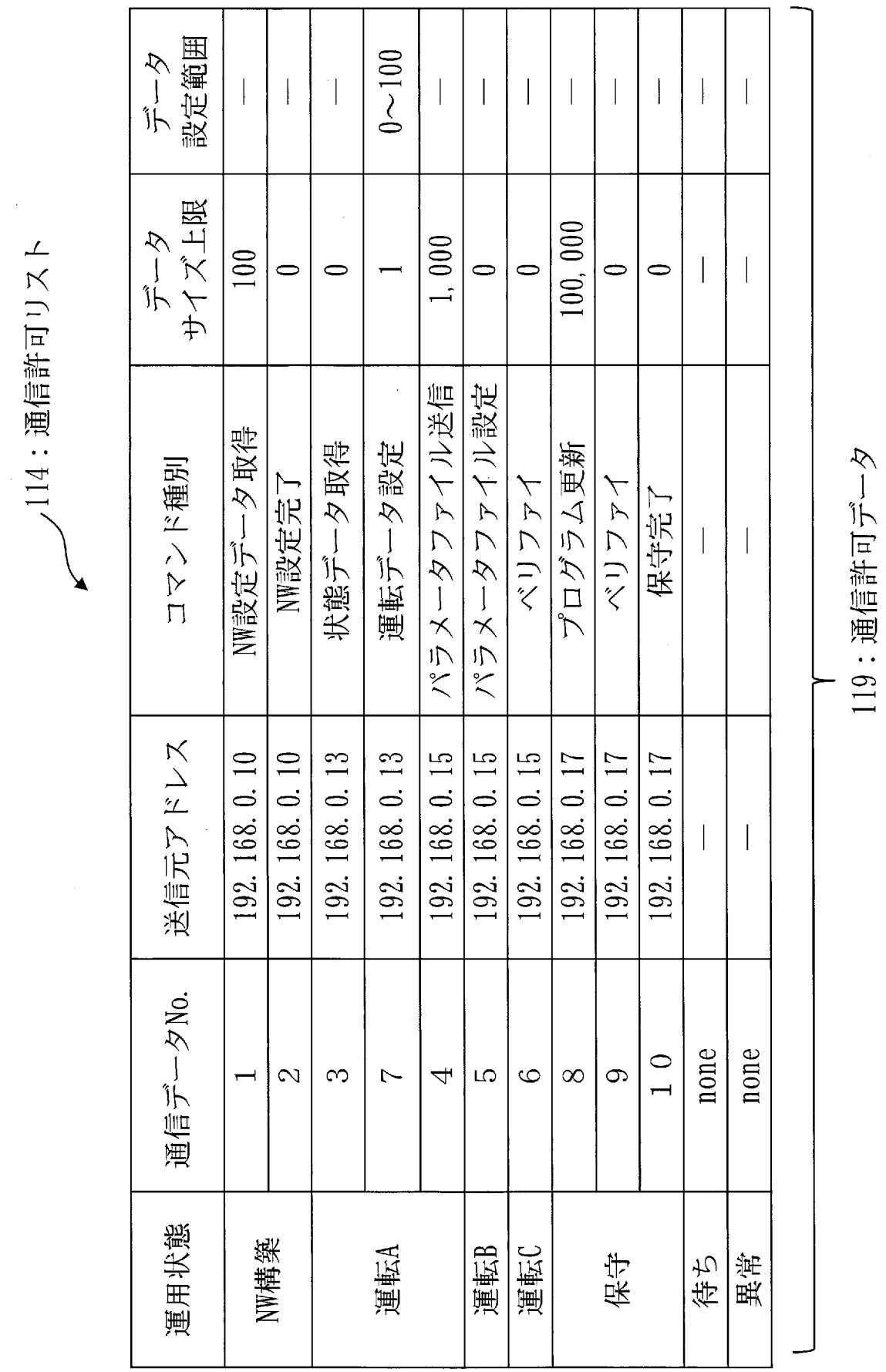
[図2]


300
コントローラ
310
アプリケーション
101a：データ判定装置
105
通信許可リスト格納部
108
警報部
113
114
115
104
タイマー
103
判定部
110
操作部
106
状態管理部
112
107
通信部
102：ネットワーク
200
監視制御装置
1031
状態遷移モデル
130
111

[図3]

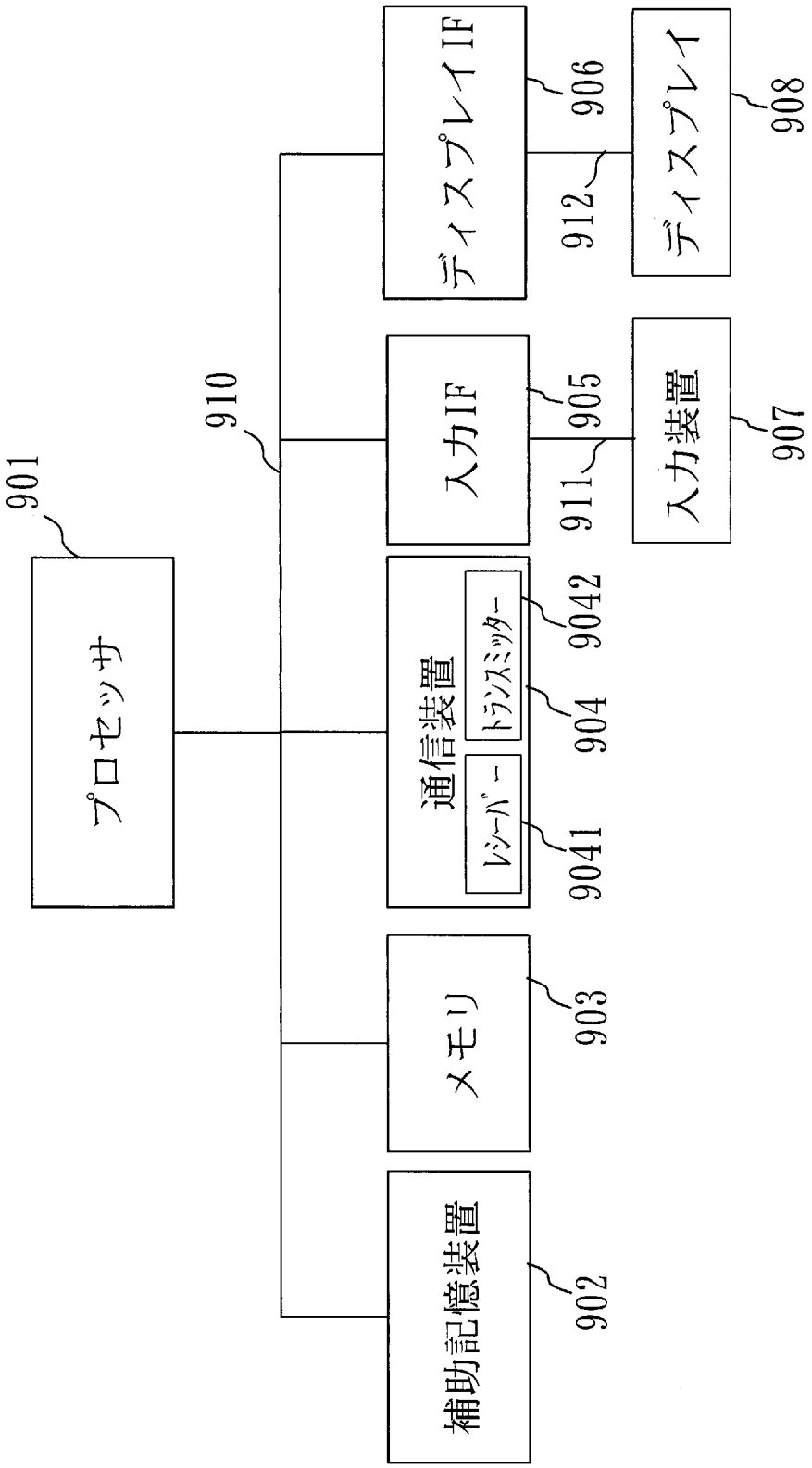

1031：状態遷移モデル
電源投入
NW構築
301
通信データ1
通信データ2
運転A
302
通信データ3
運転B
303
通信データ4
運転C
304
通信データ5
通信データ6
通信データ7
:タイマーオン
待ち
305
タイマーオフ
人の操作1
保守
306
通信データ8，9
通信
データ10
異常
307
異常判定
異常判定
異常判定

[図4]

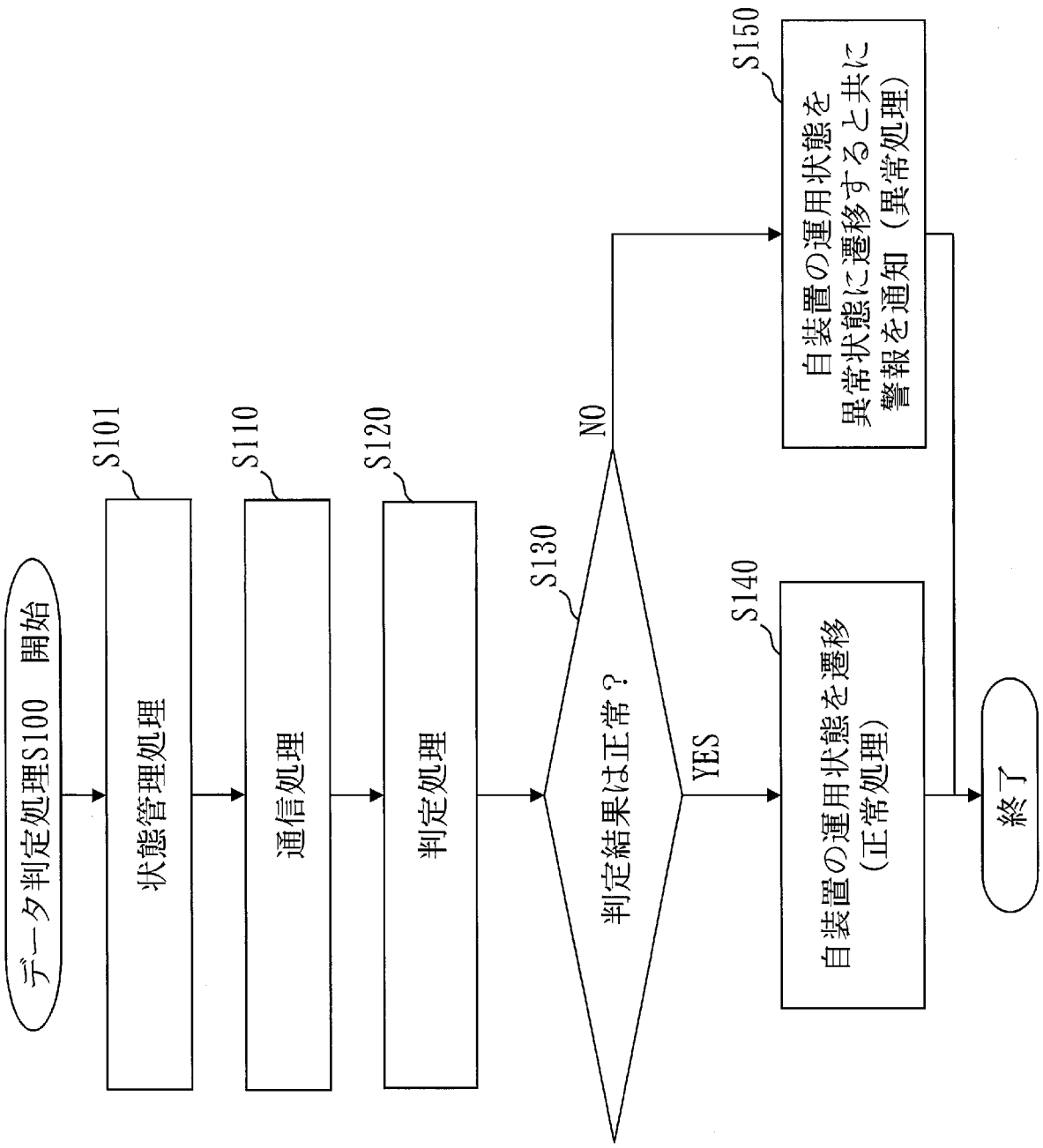



| 運用状態 | 通信データNo. | 送信元アドレス | コマンド種別 | データサイズ上限 | データ設定範囲 |
|---|---|---|---|---|---|
| NW構築 | 1 | 192.168.0.10 | NW設定データ取得 | 100 | — |
| | 2 | 192.168.0.10 | NW設定完了 | 0 | — |
| 運転A | 3 | 192.168.0.13 | 状態データ取得 | 0 | — |
| | 7 | 192.168.0.13 | 運転データ設定 | 1 | 0～100 |
| | 4 | 192.168.0.15 | パラメータファイル送信 | 1,000 | — |
| 運転B | 5 | 192.168.0.15 | パラメータファイル設定 | 0 | — |
| 運転C | 6 | 192.168.0.15 | ベリファイ | 0 | — |
| 保守 | 8 | 192.168.0.17 | プログラム更新 | 100,000 | — |
| | 9 | 192.168.0.17 | ベリファイ | 0 | — |
| | 10 | 192.168.0.17 | 保守完了 | 0 | — |
| 待ち | none | — | — | — | — |
| 異常 | none | — | — | — | — |

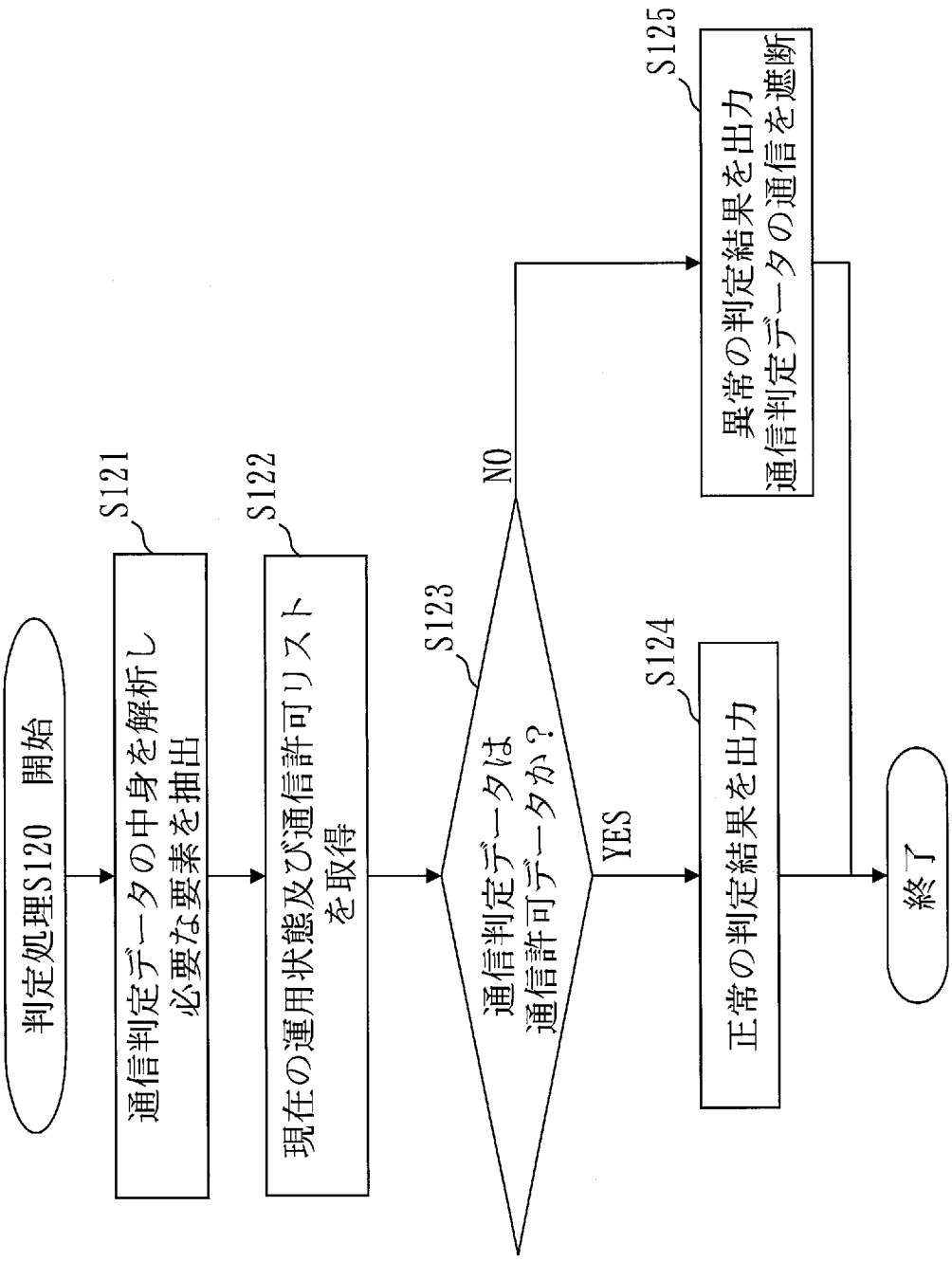
[図5]


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
トランスミッター
9041
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

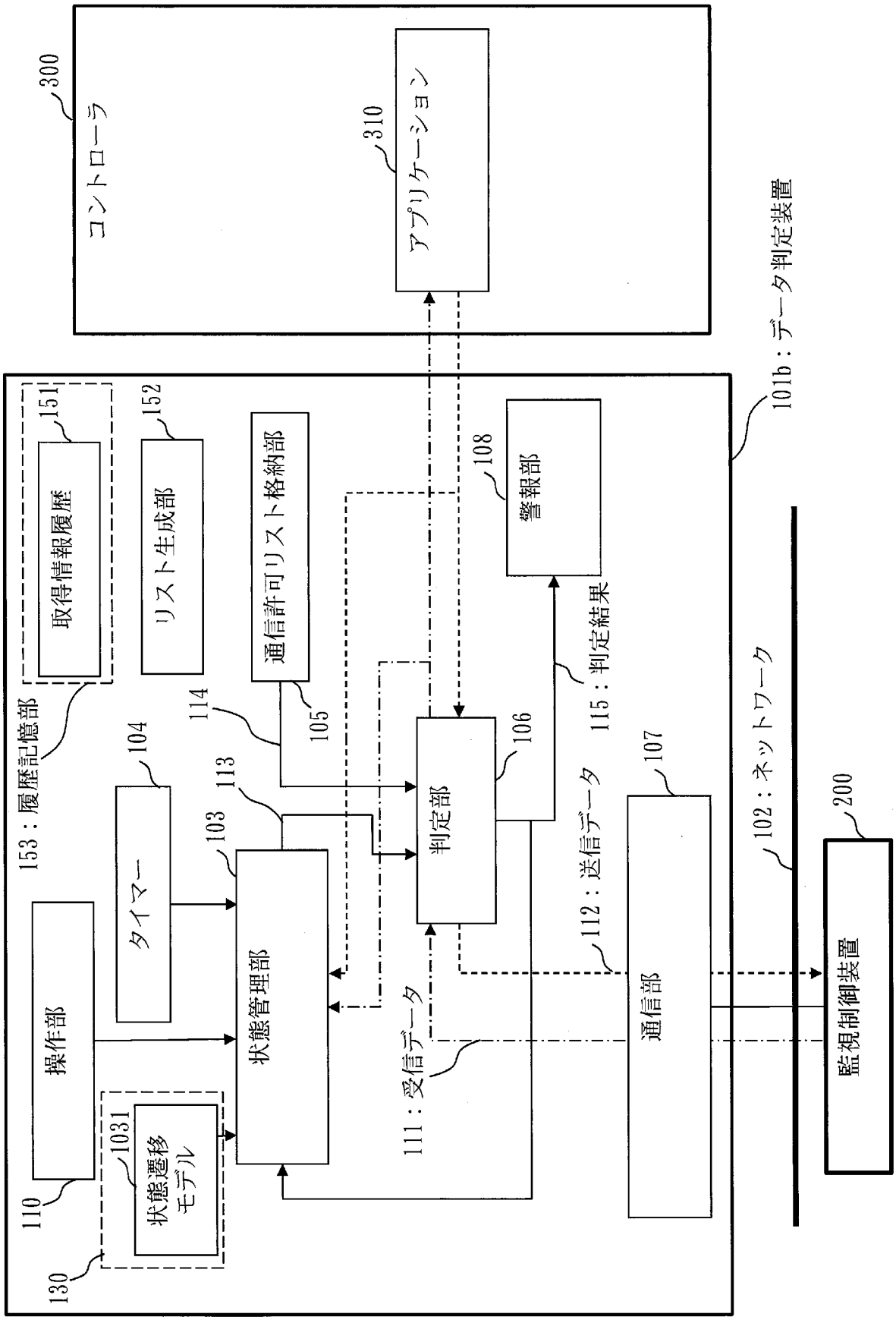
[図6]


データ判定処理S100　開始
S101
状態管理処理処理
S110
通信処理
S120
判定処理
S130
判定結果は正常？
NO
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）
YES
S140
自装置の運用状態を遷移
（正常処理）
終了

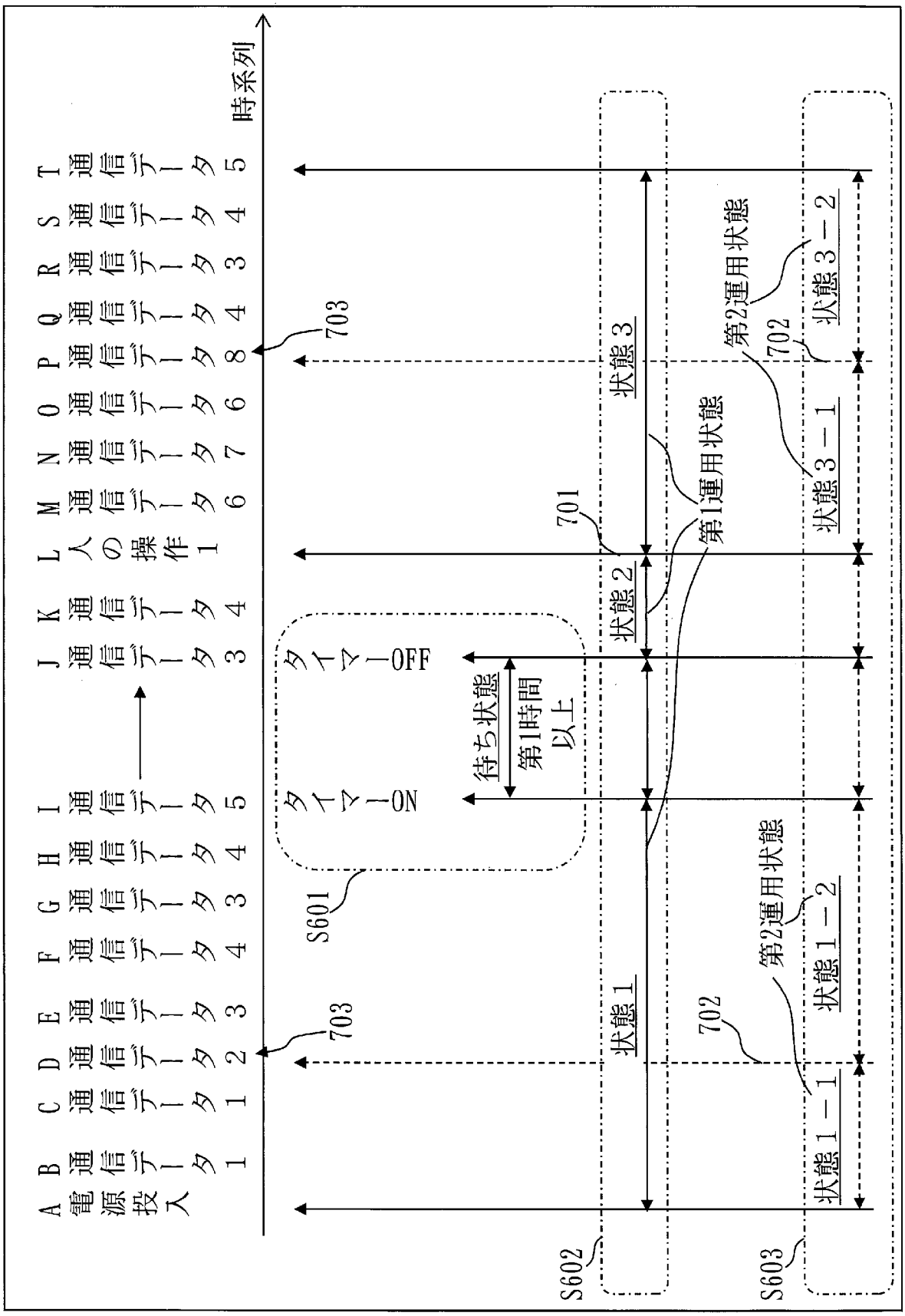
[図7]


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

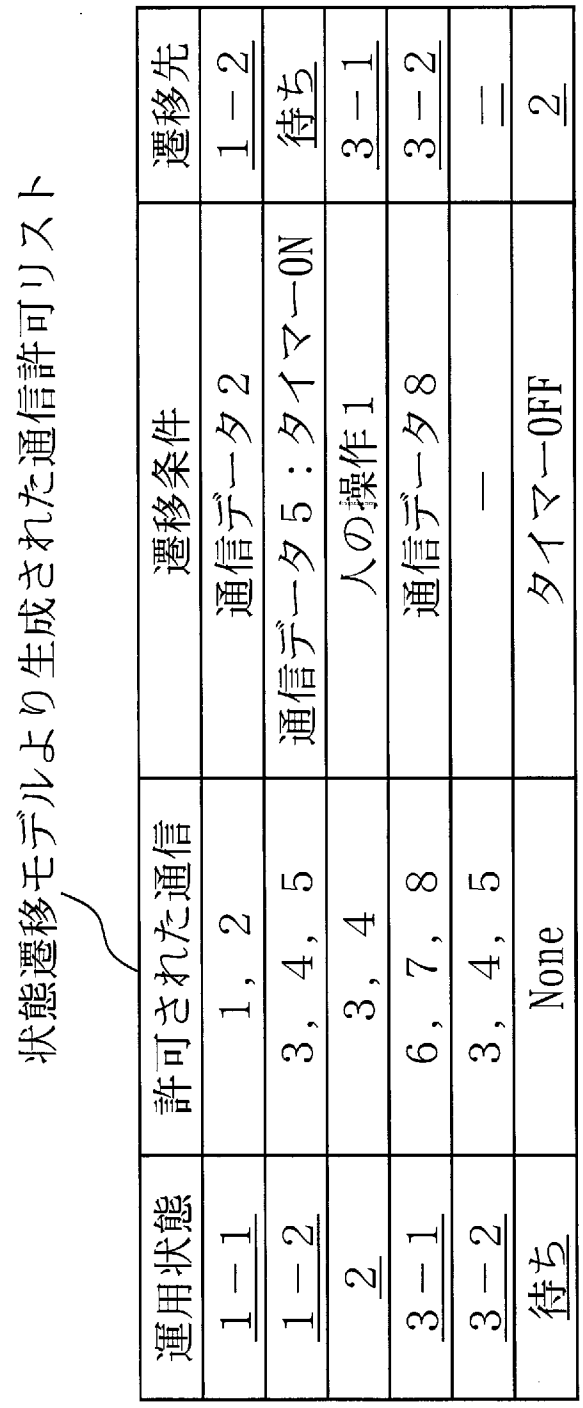
[図8]


300
コントローラ
310
アプリケーション
101b：データ判定装置
151
取得情報履歴
152
リスト生成部
通信許可リスト格納部
108
警報部
153：履歴記憶部
114
105
106
115：判定結果
104
113
103
107
タイマー
判定部
102：ネットワーク
200
操作部
状態管理部
112：送信データ
通信部
監視制御装置
111：受信データ
1031
状態遷移モデル
110
130

[図9]


A 電源投入データ
B 通信データ1
C 通信データ2
D 通信データ3
E 通信データ4
F 通信データ5
G 通信データ6
H 通信データ7
I 通信データ8
J 通信データ1
K 通信データ2
L 人の操作データ
M 通信データ3
N 通信データ4
O 通信データ5
P 通信データ6
Q 通信データ7
R 通信データ8
S 通信データ9
T 通信データ10
時系列
703
703
S601
タイマーON
タイマーOFF
待ち状態
第1時間以上
701
第1運用状態
状態1
状態2
状態3
S602
S603
702
第2運用状態
状態1－1
状態1－2
702
第2運用状態
状態3－1
状態3－2

[図10]


状態遷移モデルより生成された通信許可リスト

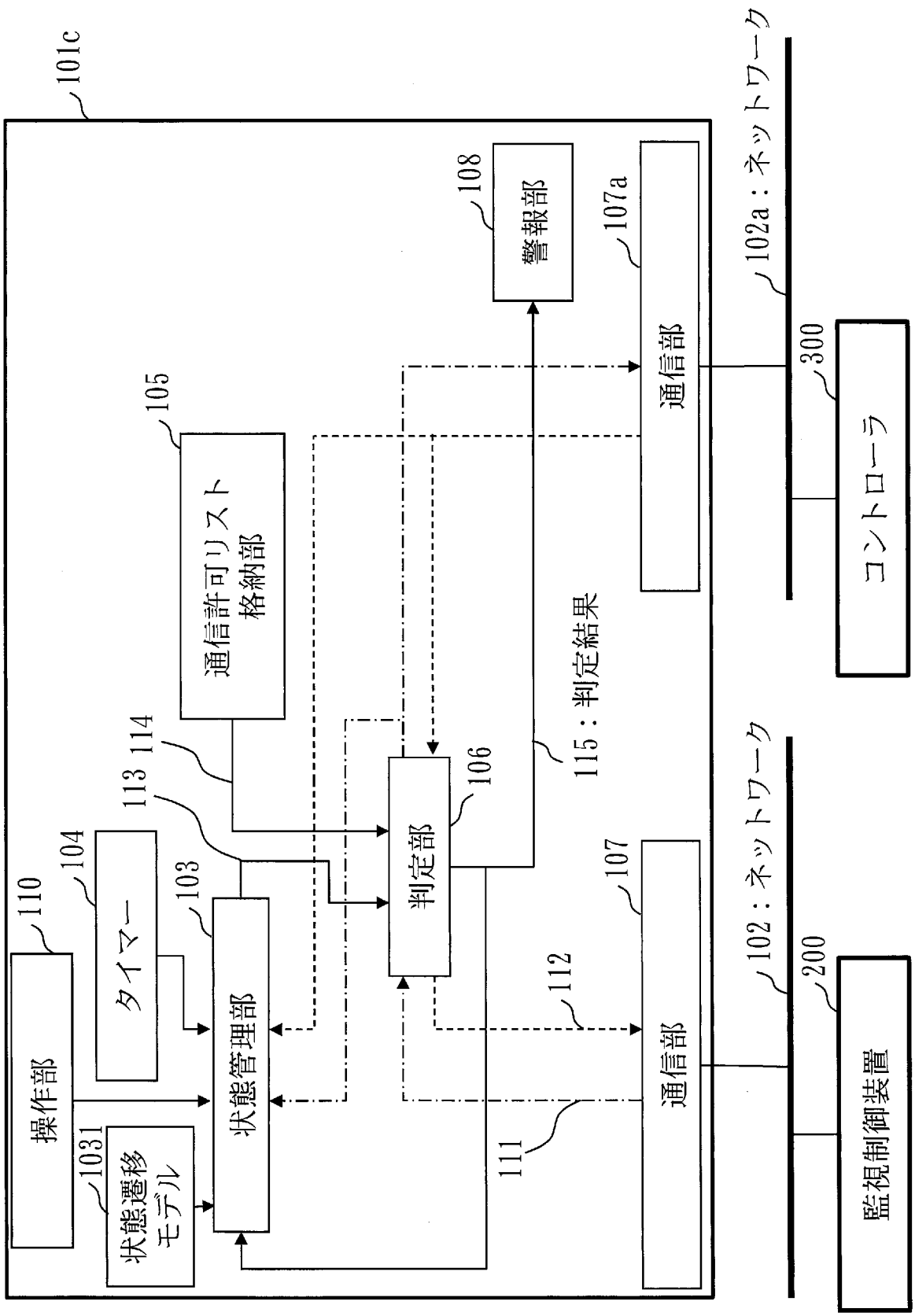
| 運用状態 | 許可された通信 | 遷移条件 | 遷移先 |
|---|---|---|---|
| 1－1 | 1，2 | 通信データ2 | 1－2 |
| 1－2 | 3，4，5 | 通信データ5：タイマーON | 待ち |
| 2 | 3，4 | 人の操作1 | 3－1 |
| 3－1 | 6，7，8 | 通信データ8 | 3－2 |
| 3－2 | 3，4，5 | — | — |
| 待ち | None | タイマーOFF | 2 |

[図11]

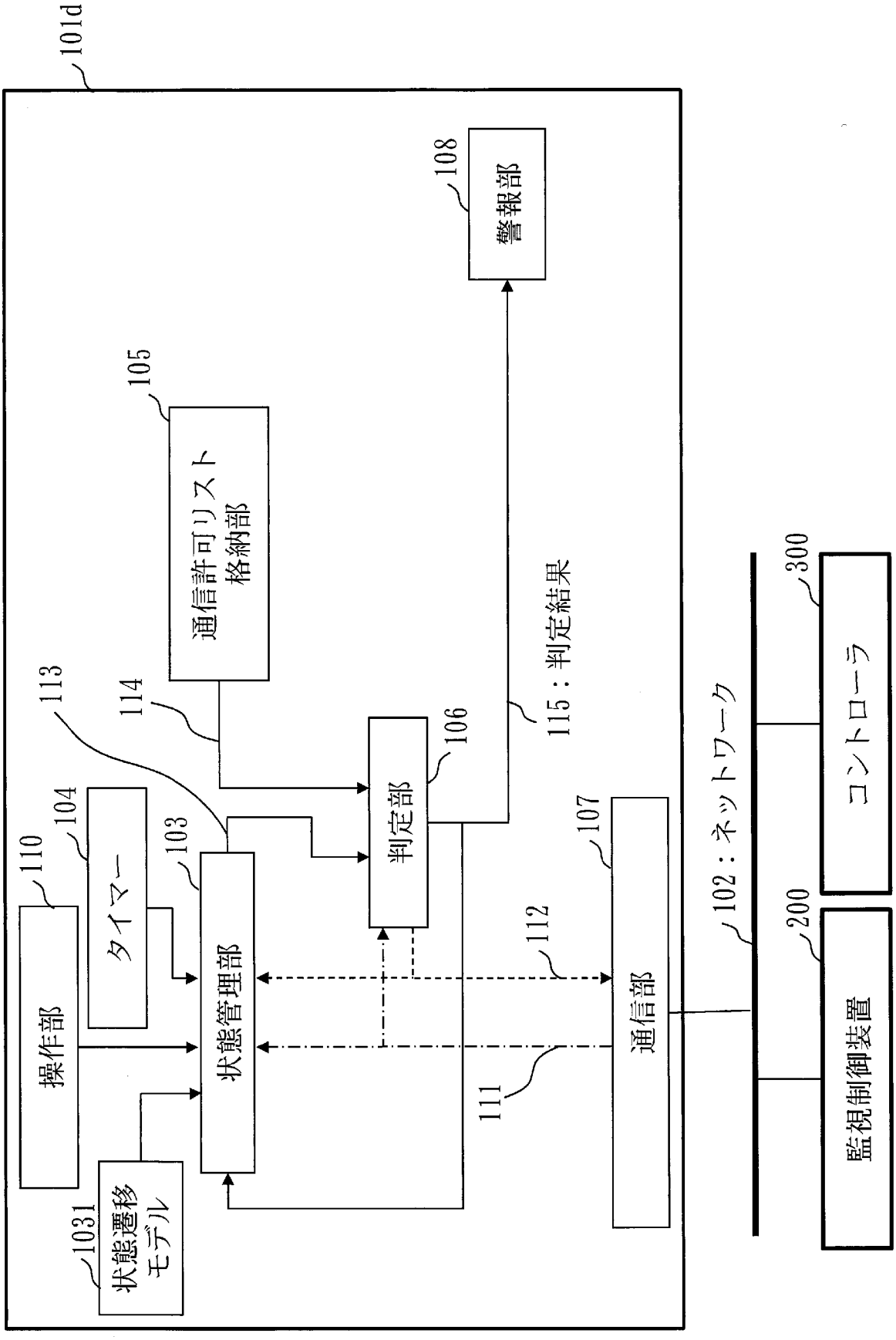
まとめ後の通信許可リスト

| 運用状態 | 許可された通信 | 遷移条件 | 遷移先 |
|---|---|---|---|
| 1－1 | 1，2 | 通信データ2 | 1－2 |
| 1－2 | 3，4，5 | 通信データ5：タイマーON<br>人の操作1 | 待ち<br>3－1 |
| 3－1 | 6，7，8 | 通信データ8 | 1－2 |
| 待ち | None | タイマーOFF | 1－2 |

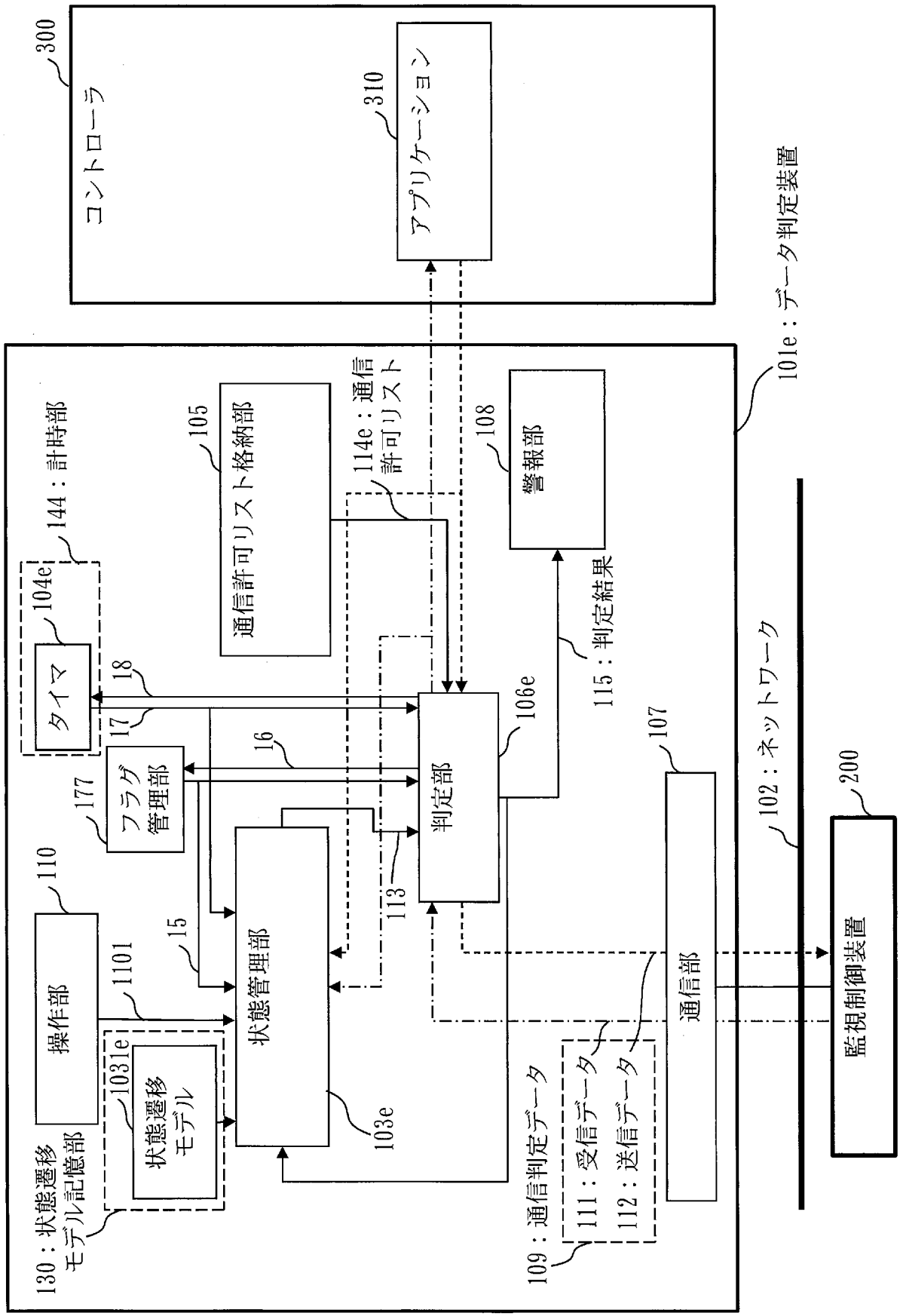
[図12]


101c
操作部
110
状態遷移モデル
1031
タイマー
104
状態管理部
103
113
114
通信許可リスト格納部
105
判定部
106
115：判定結果
112
111
警報部
108
通信部
107a
通信部
107
102a：ネットワーク
102：ネットワーク
300
コントローラ
200
監視制御装置

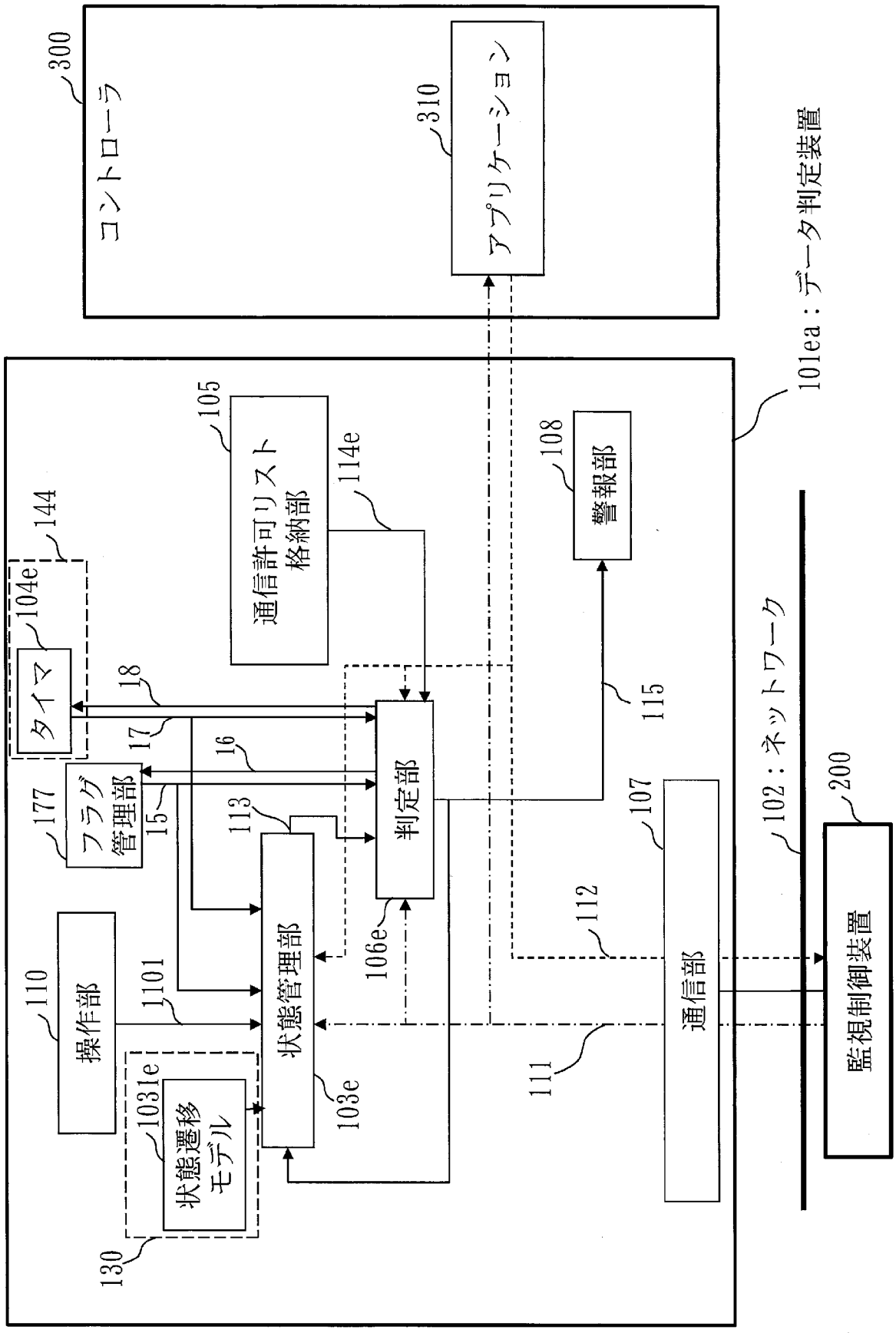
[図13]


101d
108
警報部
105
通信許可リスト格納部
113
114
106
判定部
115：判定結果
104
タイマー
103
110
操作部
状態管理部
107
112
通信部
102：ネットワーク
300
コントローラ
200
監視制御装置
111
1031
状態遷移モデル

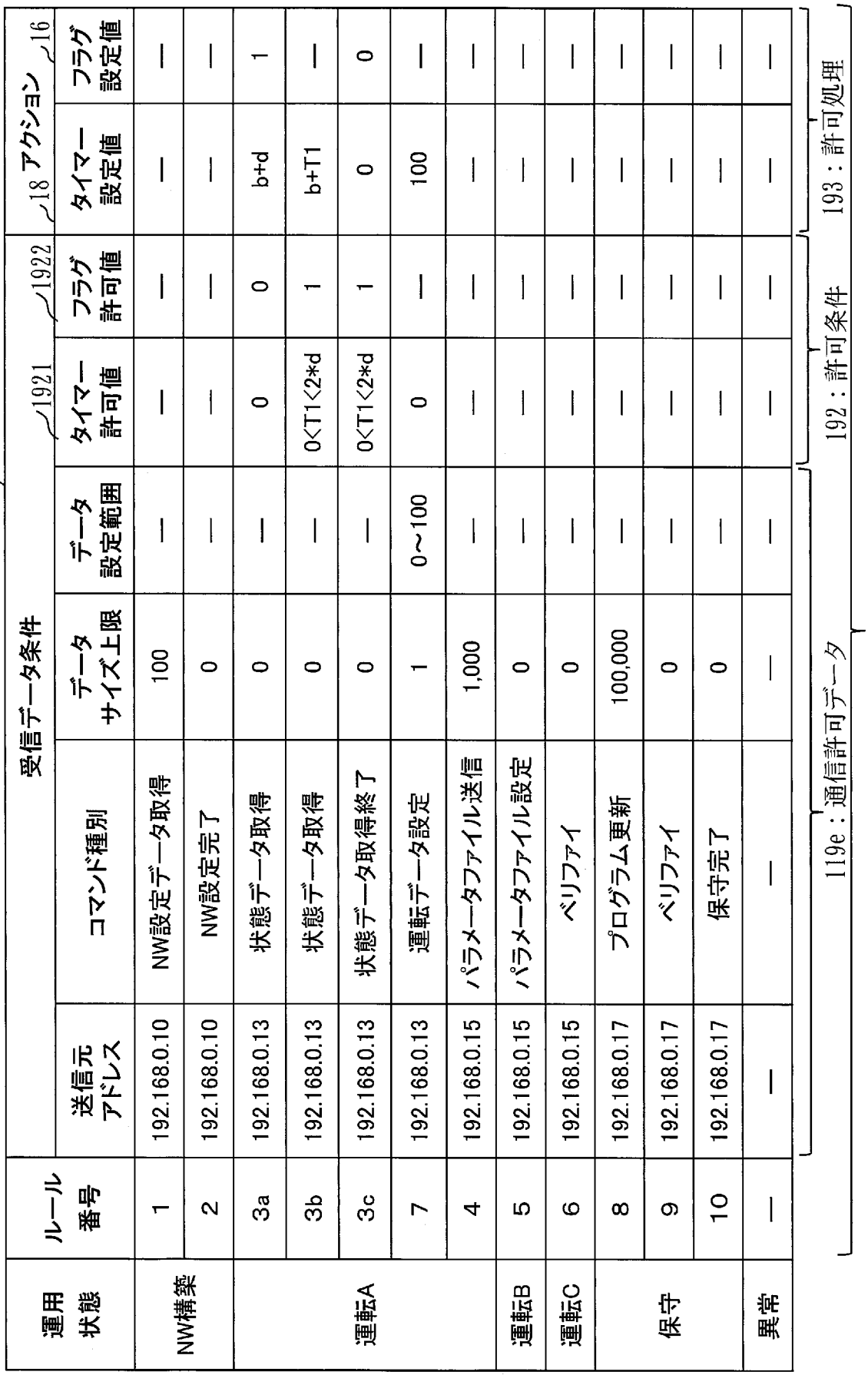
[図14]


300
コントローラ
310
アプリケーション
101e：データ判定装置
144：計時部
104e
タイマ
18
17
16
105
通信許可リスト格納部
114e：通信許可リスト
108
警報部
115：判定結果
106e
判定部
177
フラグ管理部
107
110
操作部
1101
15
状態管理部
113
1031e
状態遷移モデル
103e
130：状態遷移モデル記憶部
109：通信判定データ
111：受信データ
112：送信データ
通信部
102：ネットワーク
200
監視制御装置

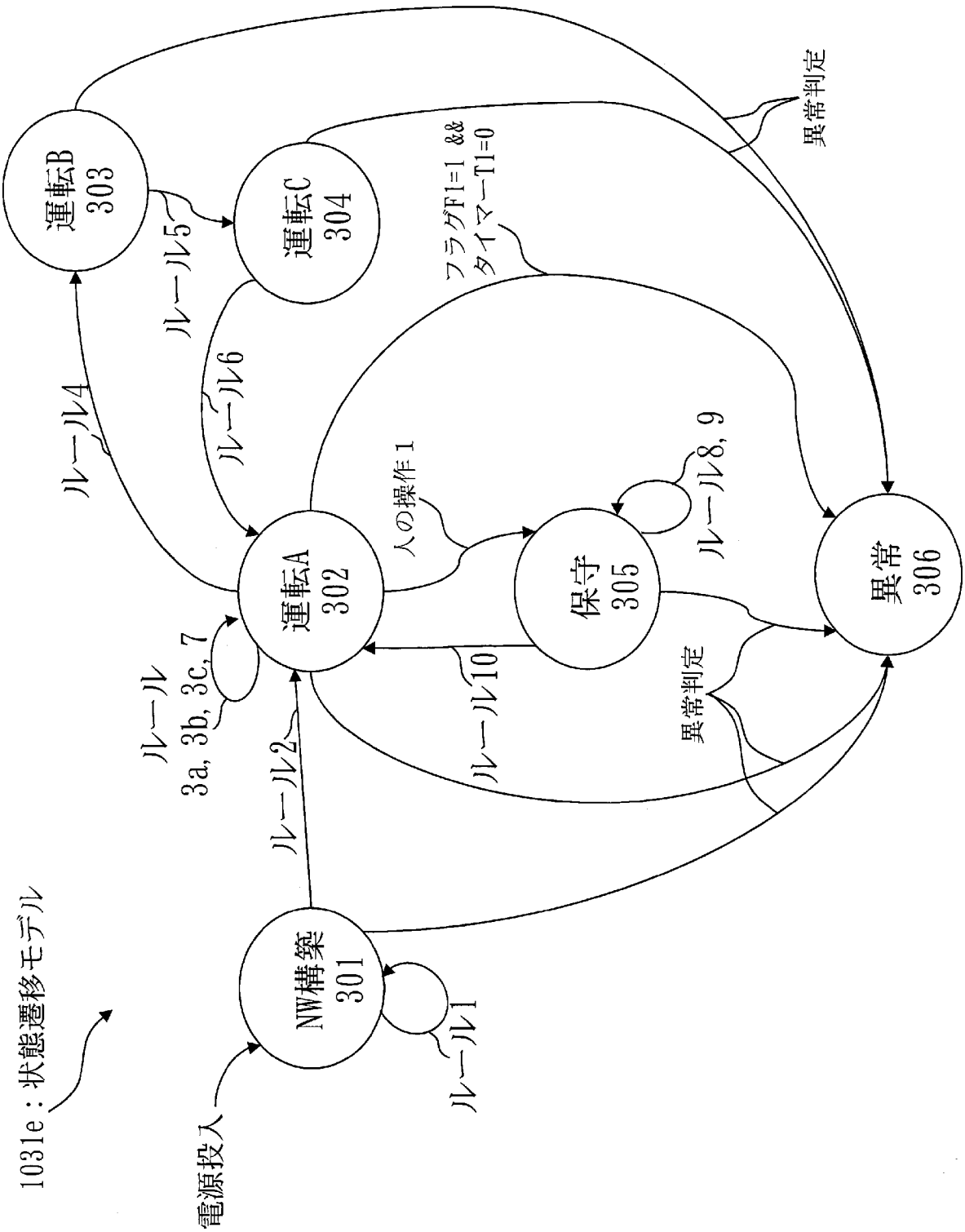
[図15]


300
コントローラ
310
アプリケーション
101ea：データ判定装置
105
通信許可リスト格納部
114e
108
警報部
144
104e
タイマ
18
17
16
177
フラグ管理部
15
113
判定部
115
107
102：ネットワーク
200
112
110
操作部
1101
106e
通信部
監視制御装置
111
1031e
状態遷移モデル
103e
状態管理部
130

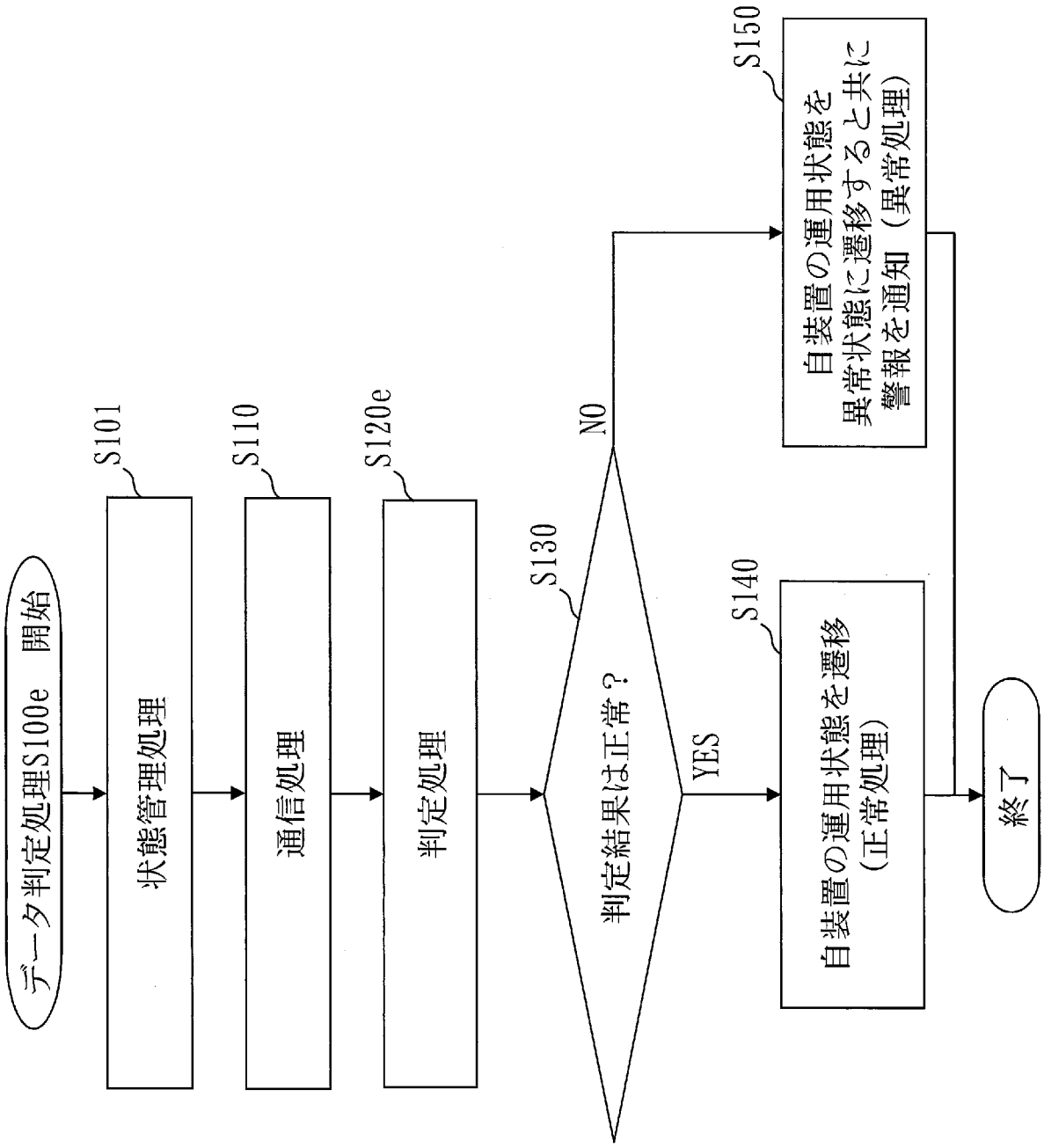
[図16]


114e：通信許可リスト
運用状態
ルール番号
受信データ条件
送信元アドレス
コマンド種別
データサイズ上限
データ設定範囲
1921 タイマー許可値
1922 フラグ許可値
18 アクション
タイマー設定値
16 フラグ設定値
NW構築
1
192.168.0.10
NW設定データ取得
100
—
—
—
—
2
192.168.0.10
NW設定完了
0
—
—
—
—
運転A
3a
192.168.0.13
状態データ取得
0
—
0
0
b+d
1
3b
192.168.0.13
状態データ取得
0
—
0<T1<2*d
1
b+T1
—
3c
192.168.0.13
状態データ取得終了
0
—
0<T1<2*d
1
0
0
7
192.168.0.13
運転データ設定
1
0～100
0
—
100
—
4
192.168.0.15
パラメータファイル送信
1,000
—
—
—
—
—
運転B
5
192.168.0.15
パラメータファイル設定
0
—
—
—
—
—
運転C
6
192.168.0.15
ベリファイ
0
—
—
—
—
—
保守
8
192.168.0.17
プログラム更新
100,000
—
—
—
—
—
9
192.168.0.17
ベリファイ
0
—
—
—
—
—
10
192.168.0.17
保守完了
0
—
—
—
—
—
異常
—
—
—
—
—
—
—
119e：通信許可データ
192：許可条件
193：許可処理
14：通信許可ルール

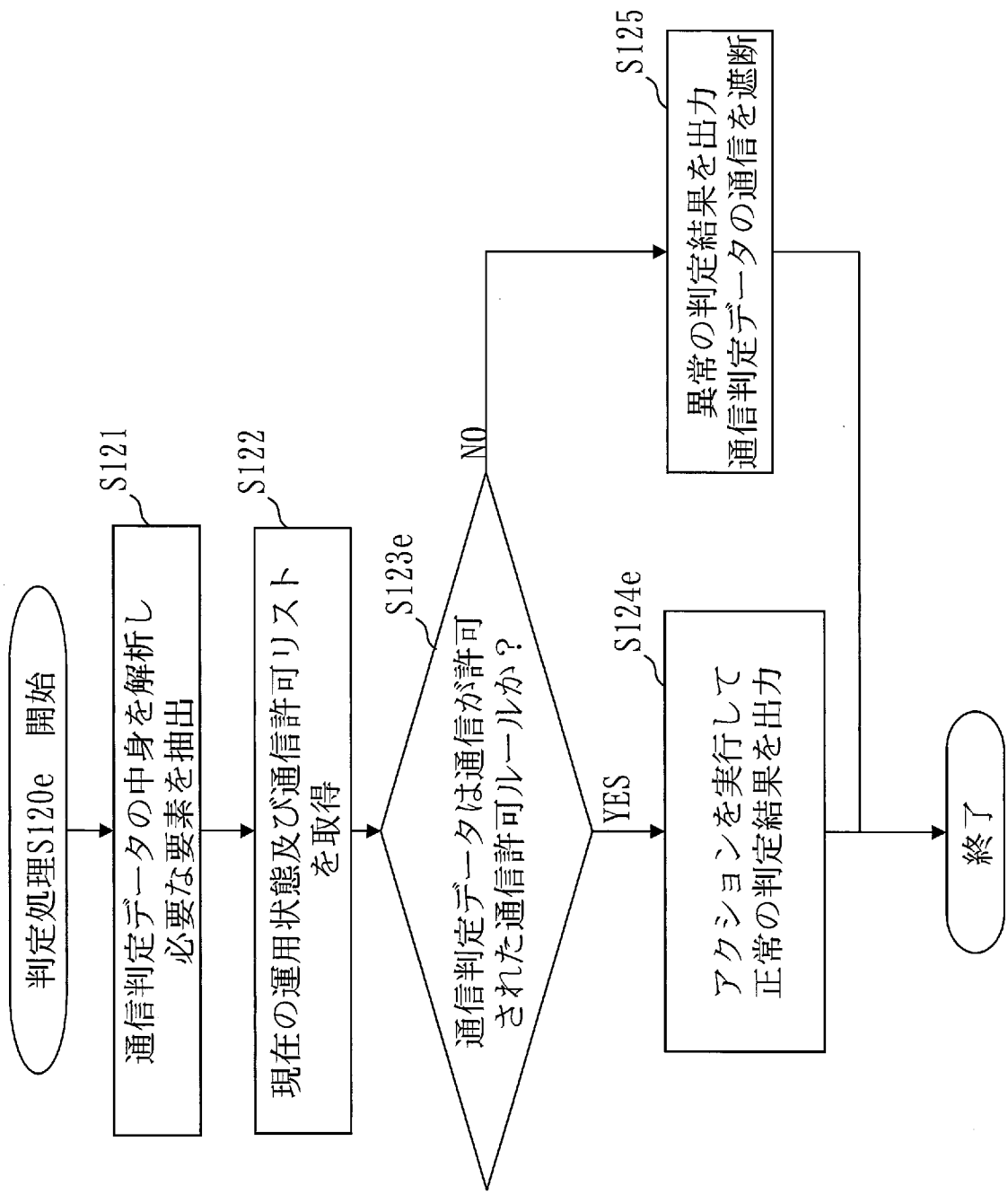
[図17]


1031e：状態遷移モデル
電源投入
NW構築
301
ルール1
ルール2
運転A
302
運転B
303
運転C
304
保守
305
異常
306
ルール3a, 3b, 3c, 7
ルール4
ルール5
ルール6
人の操作1
フラグF1=1 &&
タイマーT1=0
ルール8, 9
ルール10
異常判定
異常判定

[図18]


データ判定処理S100e 開始
S101
状態管理処理
S110
通信処理
S120e
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19]


判定処理S120e 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
S123e
通信判定データは通信が許可された通信許可ルールか？
NO
S125
異常の判定結果を出力
通信判定データの通信を遮断
YES
S124e
アクションを実行して正常の判定結果を出力
終了

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2015/085742

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 1996-2016
Kokai Jitsuyo Shinan Koho 1971-2016 Toroku Jitsuyo Shinan Koho 1994-2016

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus/JMEDPlus/JST7580(JDreamIII), IEEE Xplore,
Intrusion Detection System, state transition, white list

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | JP 2012-34273 A (Yokogawa Electric Corp.), 16 February 2012 (16.02.2012), paragraphs [0001] to [0095] | 1-21 |
| A | JP 2012-168686 A (International Business Machines Corp.), 06 September 2012 (06.09.2012), paragraphs [0001] to [0072] | 1-21 |
| A | Fovino, I.N. et al., Modbus/DNP3 State-Based Intrusion Detection System, 2010 24th IEEE International Conference on Advanced InformationNetworking and Applications, 2010, p.729-736, especially V.LANGUAGES FOR THE RULES | 1-21 |

☒ 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 |
|---|---|
| 01 February 2016 (01.02.16) | 09 February 2016 (09.02.16) |
| Name and mailing address of the ISA/<br>Japan Patent Office<br>3-4-3,Kasumigaseki,Chiyoda-ku,<br>Tokyo 100-8915,Japan | Authorized officer<br><br>Telephone No. |

**INTERNATIONAL SEARCH REPORT**

International application No.
PCT/JP2015/085742

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | Yang, Y. et al., Multiattribute SCADA-Specific Intrusion Detection Systemfor Power Networks, IEEE Transactions on Power Delivery, 2014.06, p.1092-1102, especially IV. PROPOSED MULTIATTRIBUTE IDS FOR SCADA | 1-21 |
| P,X | Teruyoshi YAMAGUCHI, Koichi SHIMIZU, Nobuhiro KOBAYASHI, "Sangyo Seigyo System ni Okeru Shinnyu Kenchi Shuho", 2015 Nen Symposium on Cryptography and Information Security Koen Ronbunshu, 20 January 2015 (20.01.2015), 4 Kodo na Kogeki ni Taio shita Shinnyu Kenchi Hoshiki no Kento (concept) | 1-21 |

**INTERNATIONAL SEARCH REPORT**
Information on patent family members

International application No.
PCT/JP2015/085742

| | | | |
|---|---|---|---|
| JP 2012-34273 A | 2012.02.16 | US 2012/0030761 A1<br>paragraphs [0001] to [0137]<br>CN 102347872 A | 2012.02.02<br><br>2012.02.08 |
| JP 2012-168686 A | 2012.09.06 | US 2012/0210158 A1<br>paragraphs [0001] to [0089] | 2012.08.16<br> |

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１５／０８５７４２

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 | １９７１－２０１６年 |
| 日本国実用新案登録公報 | １９９６－２０１６年 |
| 日本国登録実用新案公報 | １９９４－２０１６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）

JSTPlus/JMEDPlus/JST7580(JDreamⅢ), IEEE Xplore
Intrusion Detection System, state transition, white list

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 | JP 2012-34273 A (横河電機株式会社) 2012.02.16, 段落[0001]-[0095] | 1-21 |
| A | JP 2012-168686 A (インターナショナル・ビジネス・マシーンズ・コーポレーション) 2012.09.06, 段落[0001]-[0072] | 1-21 |
| A | Fovino, I.N. et al., Modbus/DNP3 State-Based Intrusion Detection System, 2010 24th IEEE International Conference on Advanced InformationNetworking and Applications, 2010, p.729-736, especially V.LANGUAGES FOR THE RULES | 1-21 |

☑　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 |
|---|---|
| ０１．０２．２０１６ | ０９．０２．２０１６ |

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　９３６４
中里　裕正
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 | Yang, Y. et al., Multiattribute SCADA-Specific Intrusion Detection Systemfor Power Networks, IEEE Transactions on Power Delivery, 2014.06, p.1092-1102, especially IV. PROPOSED MULTIATTRIBUTE IDS FOR SCADA | 1-21 |
| ＰＸ | 山口晃由，清水孝一，小林信博，産業制御システムにおける侵入検知手法，2015年暗号と情報セキュリティシンポジウム講演論文集，2015.01.20，4 高度な攻撃に対応した侵入検知方式の検討(コンセプト) | 1-21 |

| | | | |
|---|---|---|---|
| JP 2012-34273 A | 2012.02.16 | US 2012/0030761 A1<br>pars.[0001]-[0137] | 2012.02.02 |
| | | CN 102347872 A | 2012.02.08 |
| JP 2012-168686 A | 2012.09.06 | US 2012/0210158 A1<br>pars.[0001]-[0089] | 2012.08.16 |