(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110178137 B
(45)授权公告日 2023.03.24

(21)申请号 201780083467.9
(22)申请日 2017.01.20
(65)同一申请的已公布的文献号
申请公布号 CN 110178137 A
(43)申请公布日 2019.08.27
(85)PCT国际申请进入国家阶段日
2019.07.15
(86)PCT国际申请的申请数据
PCT/JP2017/002013 2017.01.20
(87)PCT国际申请的公布数据
WO2018/134981 JA 2018.07.26
(73)专利权人 三菱电机株式会社
地址 日本东京都
(72)发明人 山口晃由 中井纲人 清水孝一
小林信博
(74)专利代理机构 北京三友知识产权代理有限公司 11127
专利代理师 马建军 邓毅
(51)Int.Cl.
G06F 21/55(2006.01)
(56)对比文件
JP 6054010 B2,2016.12.27
审查员 潘秋羽

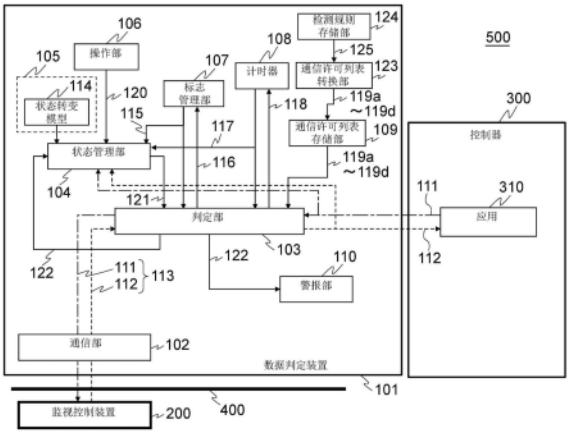
权利要求书3页 说明书16页 附图13页

(54)发明名称

数据判定装置、数据判定方法以及计算机能读取的存储介质

(57)摘要

通信许可列表转换部(123)针对在检测规则中记述有对应关系的请求通信和响应通信分配1个以上的标志,使指定了针对该标志应该设定的值的标志操作的内容与用于判定在该标志中是否设定有该应该设定的值的标志条件相对应地记述在通信许可列表中。判定部(103)在判定为请求通信的通信数据正常之后,在该标志中设置应该设定的值,在判定针对请求通信的响应通信的通信数据是否正常的情况下,判定在该标志中是否设定有应该设定的值,在设定有应该设定的值的情况下,将响应通信的通信数据判定为正常,并重置该标志。



CN 110178137 B

1.一种数据判定装置,该数据判定装置具有:

标志管理部,其存储针对本装置设定的标志的当前值;

状态管理部,其存储在多个运用状态之间转变的本装置的当前的运用状态,并且根据来自外部的输入信号以及所述标志管理部存储的所述标志的当前值中的任意一个以上,按照定义了所述运用状态之间的转变的状态转变模型,使所述本装置的运用状态转变;

通信许可列表转换部,其将检测规则转换成预先按照每个所述运用状态登记被许可通信的通信数据的通信许可列表,该检测规则记述有构成请求通信的通信数据与构成针对所述请求通信的响应通信的通信数据之间的对应关系;以及

判定部,其使用所述状态管理部存储的所述本装置的所述当前的运用状态、所述通信许可列表以及所述标志管理部存储的所述标志的当前值中的任意一个以上,判定被输入到所述本装置的通信数据是否是所述通信许可列表中登记的所述当前的运用状态下的通信数据,由此判定被输入到所述本装置的所述通信数据正常还是异常,

所述通信许可列表转换部在将所述检测规则转换成所述通信许可列表时,针对在所述检测规则中记述有对应关系的所述请求通信和所述响应通信分配标志,使指定了针对该标志的设定值的标志操作的内容与用于判定在所述标志中是否设定有所述设定值的标志条件相对应地记述在所述通信许可列表中,

所述判定部在判定为所述请求通信的通信数据正常之后,按照所述标志操作的内容,对所述标志设置所述设定值,在判定针对所述请求通信的所述响应通信的通信数据是否正常的情况下,根据所述标志条件判定在所述标志中是否设定有所述设定值,在设定有所述设定值的情况下,将所述响应通信的通信数据判定为正常,并重置所述标志。

2.根据权利要求1所述的数据判定装置,其中,

所述数据判定装置具有警报部,在所述判定部判定为所述请求通信的通信数据或者所述响应通信的通信数据异常的情况下,该警报部发出警报。

3.根据权利要求1所述的数据判定装置,其中,

所述数据判定装置具有计时器,该计时器计测所述本装置的所述当前的运用状态持续的持续时间,

所述状态管理部根据来自外部的输入信号、所述计时器的计时器当前值以及所述标志管理部存储的所述标志的当前值中的任意一个以上,按照所述状态转变模型,使所述本装置的运用状态转变,

所述判定部使用所述状态管理部存储的所述本装置的所述当前的运用状态、所述通信许可列表、来自所述计时器的所述计时器当前值以及所述标志管理部存储的所述标志的当前值中的任意一个以上,判定被输入到所述本装置的通信数据是否是所述通信许可列表中登记的所述当前的运用状态下的通信数据。

4.根据权利要求2所述的数据判定装置,其中,

所述数据判定装置具有计时器,该计时器计测所述本装置的所述当前的运用状态持续的持续时间,

所述状态管理部根据来自外部的输入信号、所述计时器的计时器当前值以及所述标志管理部存储的所述标志的当前值中的任意一个以上,按照所述状态转变模型,使所述本装置的运用状态转变,

所述判定部使用所述状态管理部存储的所述本装置的所述当前的运用状态、所述通信许可列表、来自所述计时器的所述计时器当前值以及所述标志管理部存储的所述标志的当前值中的任意一个以上，判定被输入到所述本装置的通信数据是否是所述通信许可列表中登记的所述当前的运用状态下的通信数据。

5.根据权利要求1～4中的任意一项所述的数据判定装置，其中，

所述通信许可列表转换部按照运用状态、发送方、发送目的地的优先顺序或者运用状态、发送目的地、发送方的优先顺序对所述通信许可列表的所述通信数据进行排序，将所述排序后的顺位作为索引赋予给各所述通信数据，并且，

所述通信许可列表转换部根据所述运用状态、所述发送方的信息以及所述发送目的地的信息，生成表示索引开头编号和检索个数的列表，所述索引开头编号表示指定所述排序后的所述通信许可列表的应该参照的检索范围的开头指针，

所述判定部从所述状态管理部取得所述本装置的所述当前的运用状态，并且从作为判定对象的所述通信数据取得发送方的信息和发送目的地的信息，根据所述当前的运用状态、所述发送方的信息以及所述发送目的地的信息，从所述列表提取所述索引开头编号和所述检索个数，根据所述索引开头编号和所述检索个数确定所述排序后的所述通信许可列表中应该参照的检索范围，对所述通信许可列表的符合所述检索范围的所述通信数据与作为所述判定对象的所述通信数据进行比较，由此判定作为所述判定对象的所述通信数据正常还是异常。

6.根据权利要求1～4中的任意一项所述的数据判定装置，其中，

所述状态转变模型还定义所述运用状态根据所述判定部输出的判定结果而转变。

7.根据权利要求5所述的数据判定装置，其中，

所述状态转变模型还定义所述运用状态根据所述判定部输出的判定结果而转变。

8.根据权利要求1～4中的任意一项所述的数据判定装置，其中，

所述判定部在判定为所述通信数据异常的情况下将所述通信数据的通信切断。

9.根据权利要求5所述的数据判定装置，其中，

所述判定部在判定为所述通信数据异常的情况下将所述通信数据的通信切断。

10.根据权利要求6所述的数据判定装置，其中，

所述判定部在判定为所述通信数据异常的情况下将所述通信数据的通信切断。

11.根据权利要求7所述的数据判定装置，其中，

所述判定部在判定为所述通信数据异常的情况下将所述通信数据的通信切断。

12.一种数据判定方法，该数据判定方法具有如下步骤：

标志管理步骤，存储针对本装置设定的标志的当前值；

状态管理步骤，根据来自外部的输入信号以及在所述标志管理步骤中存储的所述标志的当前值中的任意一个以上，按照定义了所述本装置的多个运用状态之间的转变的状态转变模型，使所述本装置的运用状态转变，存储所述本装置的当前的运用状态；

通信许可列表转换步骤，将检测规则转换成预先按照每个所述运用状态登记被许可通信的通信数据的通信许可列表，该检测规则记述有构成请求通信的通信数据与构成针对所述请求通信的响应通信的通信数据之间的对应关系；以及

判定步骤，使用在所述状态管理步骤中存储的所述本装置的所述当前的运用状态、所

述通信许可列表以及在所述标志管理步骤中存储的所述标志的当前值中的任意一个以上，判定被输入到所述本装置的通信数据是否是所述通信许可列表中登记的所述当前的运用状态下的通信数据，由此判定被输入到所述本装置的所述通信数据正常还是异常，

在所述通信许可列表转换步骤中，当将所述检测规则转换成所述通信许可列表时，针对在所述检测规则中记述有对应关系的所述请求通信和所述响应通信分配标志，使指定了针对该标志的设定值的标志操作的内容与用于判定在所述标志中是否设定有所述设定值的标志条件相对应地记述在所述通信许可列表中，

在所述判定步骤中，在判定为所述请求通信的通信数据正常之后，按照所述标志操作的内容，对所述标志设置所述设定值，在判定针对所述请求通信的所述响应通信的通信数据是否正常的情况下，根据所述标志条件判定在所述标志中是否设定有所述设定值，在设定有所述设定值的情况下，将所述响应通信的通信数据判定为正常，并重置所述标志。

13.一种存储有数据判定程序的计算机能读取的存储介质，该数据判定程序为了进行数据判定，使计算机作为如下部件发挥作用：

标志管理部，其存储针对本装置设定的标志的当前值；

状态管理部，其存储在多个运用状态之间转变的本装置的当前的运用状态，并且根据来自外部的输入信号以及所述标志管理部存储的所述标志的当前值中的任意一个以上，按照定义了所述运用状态之间的转变的状态转变模型，使所述本装置的运用状态转变；

通信许可列表转换部，其将检测规则转换成预先按照每个所述运用状态登记被许可通信的通信数据的通信许可列表，该检测规则记述有构成请求通信的通信数据与构成针对所述请求通信的响应通信的通信数据之间的对应关系；以及

判定部，其使用所述状态管理部存储的所述本装置的所述当前的运用状态、所述通信许可列表以及所述标志管理部存储的所述标志的当前值中的任意一个以上，判定被输入到所述本装置的通信数据是否是所述通信许可列表中登记的所述当前的运用状态下的通信数据，由此判定被输入到所述本装置的所述通信数据正常还是异常，

所述通信许可列表转换部在将所述检测规则转换成所述通信许可列表时，针对在所述检测规则中记述有对应关系的所述请求通信和所述响应通信分配标志，使指定了针对该标志的设定值的标志操作的内容与用于判定在所述标志中是否设定有所述设定值的标志条件相对应地记述在所述通信许可列表中，

所述判定部在判定为所述请求通信的通信数据正常之后，按照所述标志操作的内容，对所述标志设置所述设定值，在判定针对所述请求通信的所述响应通信的通信数据是否正常的情况下，根据所述标志条件判定在所述标志中是否设定有所述设定值，在设定有所述设定值的情况下，将所述响应通信的通信数据判定为正常，并重置所述标志。

数据判定装置、数据判定方法以及计算机能读取的存储介质

技术领域

[0001] 本发明涉及数据判定装置、数据判定方法以及计算机能读取的存储介质，尤其涉及用于检测对网络的非法侵入的数据判定装置、数据判定方法以及计算机能读取的存储介质。

背景技术

[0002] 近年来，在工业控制系统中，该系统与网络连接的情况不断增加。因此，系统成为网络攻击目标的情况不断增加。因此，在工业控制系统中，为了检测由网络攻击引起的对网络的侵入，使用以下的侵入检测系统。

[0003] 在以往的侵入检测系统中，利用工业控制系统的网络通信是固定的这一点，通过设定发送目的地地址与发送方地址的对并且设定协议，定义被许可的通信。并且，侵入检测系统采取的是通过将被许可的通信以外的通信判定为异常，针对未知的攻击也检测其侵入的白名单型的对策(例如参照专利文献1、2)。

[0004] 另外，提出了如下方式：定义许可的通信序列，在各个通信序列中对未连接、通信中、异常处理等的通信状态进行管理(例如，参照专利文献2)。

[0005] 并且，提出了如下方法：用状态机记述通信的事务，能够将通信的顺序作为白名单进行记述(例如，参照非专利文献1)。

[0006] 另外，随着检测规则的增加，如何使检索高速化成为课题。提出了在进行分组数据的匹配的DPI(Deep Packet Inspection:深度分组检测)中使用Bloom Filter的方法(例如，参照非专利文献2)以及使用多核处理器的方法(例如，参照非专利文献3、4)。

[0007] 现有技术文献

[0008] 专利文献

[0009] 专利文献1:日本特许第4688420号公报

[0010] 专利文献2:日本特开2001-034553号公报

[0011] 非专利文献

[0012] 非专利文献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.

[0013] 非专利文献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.

[0014] 非专利文献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.

[0015] 非专利文献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.

发明内容

[0016] 发明要解决的课题

[0017] 专利文献1、2等记载的以往的白名单大多是判定分组单体是否与规则匹配。然而，近年来，还存在以工业控制系统为目标的、例如像Stuxnet那样通过单一分组的判定无法检测到的攻击。为了检测这些攻击，需要在检测对象中包含进行通信时的系统或装置的状态以及请求与响应之间的对应关系等。但是，在专利文献1中没有采取这样的对策。

[0018] 在专利文献2记载的现有技术中，对发送方和发送目的地的通信状态进行监视，判定这些通信状态是否是依照预先规定的通信序列的通信状态，根据判定结果进行访问控制。但是，在这种情况下，在第三者从侵占的服务器进行了依照通信顺序的通信的情况下，无法检测出该通信是网络攻击，因此，其结果是，存在非法改写程序的攻击数据等也能够通信这样的课题。

[0019] 另一方面，在非专利文献1等记载的现有技术中，请求与响应之间的对应关系也包含在检测对象中，因此能够更高度地检测网络攻击。但是，在非专利文献1中，在用一台检测装置检测多台设备的通信的情况下，必须用状态机记述全部装置之间的通信的组合，引发组合爆炸。

[0020] 另外，在检索的高速化方面，在非专利文献2记载的现有技术中，存在False Positive(假定位)的可能性，因此，当以白名单型使用时，有可能错过攻击。

[0021] 另外，非专利文献3记载的现有技术的目的在于通过判定处理的并行化而实现高速化，无法削减判定对象本身。另外，存在只在能够执行并行编程的处理器上进行动作这样的课题。

[0022] 本发明正是为了解决上述课题而完成的，其目的在于提供一种数据判定装置、数据判定方法以及计算机能读取的存储介质，能够抑制组合爆炸，即使在由第三者侵占服务器而被该服务器进行了网络攻击的情况下，也能够高速且高精度地检测出通信数据是非法的。

[0023] 用于解决课题的手段

[0024] 本发明是一种数据判定装置，该数据判定装置具有：标志管理部，其存储针对本装置设定的标志的当前值；状态管理部，其存储在多个运用状态之间转变的本装置的当前的运用状态，并且根据来自外部的输入信号以及所述标志管理部存储的所述标志的当前值中的任意一个以上，按照定义了所述运用状态之间的转变的状态转变模型，使所述本装置的运用状态转变；通信许可列表转换部，其将检测规则转换成预先按照每个所述运用状态登记被许可通信的通信数据的通信许可列表，该检测规则记述有构成请求通信的通信数据与构成针对所述请求通信的响应通信的通信数据之间的对应关系；以及判定部，其使用所述状态管理部存储的所述本装置的所述当前的运用状态、所述通信许可列表以及所述标志管理部存储的所述标志的当前值中的任意一个以上，判定被输入到所述本装置的通信数据是否是所述通信许可列表中登记的所述当前的运用状态下的通信数据，由此判定被输入到所

述本装置的所述通信数据正常还是异常，所述通信许可列表转换部在将所述检测规则转换成所述通信许可列表时，针对在所述检测规则中记述有对应关系的所述请求通信和所述响应通信分配标志，使指定了针对该标志的设定值的标志操作的内容与用于判定在所述标志中是否设定有所述设定值的标志条件相对应地记述在所述通信许可列表中，所述判定部在判定为所述请求通信的通信数据正常之后，按照所述标志操作的内容，对所述标志设置所述设定值，在判定针对所述请求通信的所述响应通信的通信数据是否正常的情况下，根据所述标志条件判定在所述标志中是否设定有所述设定值，在设定有所述设定值的情况下，将所述响应通信的通信数据判定为正常，并重置所述标志。

[0025] 发明效果

[0026] 在本发明的数据判定装置中，由于在通信许可列表中定义正常的通信时，记述请求通信与响应通信之间的对应关系，因此能够在不引起组合爆炸的情况下记述全部通信数据。另外，由于使其能够通过标志的设置/重置来判定请求通信与响应通信之间的对应关系，并且使其还考虑请求通信与响应通信之间的对应关系来判定通信数据正常还是异常，因此，即使在由第三者侵占服务器而被该服务器进行了网络攻击的情况下，也能够检测出通信数据是非法的。另外，通过对请求通信与响应通信之间的对应关系进行定义，能够高速地进行增大的检测规则的检索。

附图说明

[0027] 图1是示出本发明的实施方式1的数据判定装置的结构的框图。

[0028] 图2是示出本发明的实施方式1的数据判定装置的变形例的结构的框图。

[0029] 图3是示出本发明的实施方式1的数据判定装置中的状态转变模型存储部中存储的状态转变模型的一例的图。

[0030] 图4是示出本发明的实施方式1的数据判定装置中的检测规则存储部中存储的检测规则列表的一例的图。

[0031] 图5是示出本发明的实施方式1的数据判定装置中的通信许可列表存储部中存储的通信许可列表的一例的图。

[0032] 图6是示出本发明的实施方式1的数据判定装置中的通信许可列表存储部中存储的通信许可列表的一例的图。

[0033] 图7是示出本发明的实施方式1的数据判定装置中的通信许可列表存储部中存储的通信许可列表的一例的图。

[0034] 图8是示出本发明的实施方式1的数据判定装置中的通信许可列表存储部中存储的通信许可列表的一例的图。

[0035] 图9是示出本发明的实施方式1的数据判定装置的硬件结构的框图。

[0036] 图10是示出本发明的实施方式1的数据判定装置中的数据判定处理的流程的流程图。

[0037] 图11是示出本发明的实施方式1的数据判定装置中的判定部的处理流程的流程图。

[0038] 图12是示出本发明的实施方式1的数据判定装置中的通信许可列表变换部的处理流程的流程图。

[0039] 图13是说明从本发明的实施方式1的数据判定装置得到的效果的图。

具体实施方式

[0040] 实施方式1

[0041] 使用图1和图3～图8，对本发明的实施方式1的数据判定装置101的结构进行说明。这里，如图1所示，对本实施方式1的数据判定装置101与监视控制装置200和控制器300连接，将在监视控制装置200与控制器300之间进行双向通信的通信数据作为判定对象的情况进行说明。其中，在下文中，将从控制器300向监视控制装置200发送的数据称作发送数据111，将控制器300从监视控制装置200接收的数据称作接收数据112。另外，将具备数据判定装置101、监视控制装置200以及控制器300的系统称作数据判定系统500。

[0042] 如图1所示，数据判定装置101与网络400连接。数据判定装置101经由网络400而与监视控制装置200连接。另外，数据判定装置101与控制器300连接。数据判定装置101对在监视控制装置200与控制器300之间发送的通信数据进行中继。另外，数据判定装置101还判定该通信数据是否是基于非法访问的通信数据。这样，数据判定装置101构成对侵入网络400的攻击进行检测的侵入检测装置和侵入检测系统。

[0043] 这里，列举工业控制系统具备控制器300的情况。但是，并不限于这种情况，控制器300能够配置在任意的系统中。控制器300具有应用310。应用310将发送数据111经由数据判定装置101发送给监视控制装置200。另外，应用310经由数据判定装置101从监视控制装置200接收接收数据112。由于发送数据111和接收数据112是本实施方式1的数据判定装置的判定对象，因此，在下文中，将接收数据112和发送数据111总称作通信判定数据113。

[0044] 另一方面，监视控制装置200是对具有控制器300的工业控制系统进行监视控制的服务器。

[0045] 数据判定装置101将从监视控制装置200经由网络400接收到的接收数据112发送给控制器300。另外，数据判定装置101将控制器300的应用310发送的发送数据111经由网络400发送给监视控制装置200。数据判定装置101在中继接收数据112和发送数据111的过程中，进行检测对网络400的攻击性侵入的数据判定处理。

[0046] 如图1所示，数据判定装置101具有状态管理部104、计时器108、通信许可列表存储部109、通信许可列表转换部123、检测规则存储部124、判定部103、通信部102、警报部110、操作部106、标志管理部107以及状态转变模型存储部105。但是，也可以不必设置计时器108、通信许可列表存储部109、检测规则存储部124、警报部110以及操作部106。

[0047] 状态转变模型存储部105根据本装置取得的取得信息，存储用于在多个运用状态的各运用状态之间转变的状态转变模型114。本装置是指数据判定装置101本身。另外，取得信息是使数据判定装置101的状态转变的要素。取得信息包含通过通信从外部取得的通信数据、表示已受理针对本装置的输入操作的操作信号120、从计时器108输出的计时器当前值117以及从标志管理部107输出的标志当前值115。

[0048] 图3示出状态转变模型114的一例。图3只是一例，状态转变模型114也可以不必如图3所示。

[0049] 在图3中，标号301～308表示数据判定装置101的多个运用状态的例子。这里，作为运用状态的例子，举出停止中301、启动302、控制中303、关闭304、维护305、启动306、试运行

307以及关闭308。

[0050] 另外，在图3中，在1个运用状态与其他运用状态之间，示出运用状态之间的状态转变的例子。例如，在图3的例子中，数据判定装置101在接通电源时转变到停止中301。另外，若从停止中301执行“启动开始”，则转变到启动302。另外，若从启动302进行“启动结束”，则转变到控制中303。这些“启动开始”、“启动结束”等是各运用状态之间的状态转变的信息。在状态转变模型114中，预先定义了从哪个运用状态转变到哪个运用状态。因此，由于定义了从停止中301向启动302转变，因此，不会从停止中301转变到其他的任何运用状态303～307。

[0051] 另外，指示“启动开始”等的状态转变的状态转变指令信号是由用户输入到操作部106的操作信号120、数据判定装置101接收到的接收数据112或者发送数据111、来自标志管理部107的标志当前值115以及来自计时器108的计时器当前值117。

[0052] 这样，状态转变模型114包含各运用状态301～307的信息以及这些运用状态之间的状态转变的信息。

[0053] 当被输入由用户输入到操作部106的操作信号120、数据判定装置101接收到的接收数据112或者发送数据111、来自标志管理部107的标志当前值115以及来自计时器108的计时器当前值117中的至少一个时，状态管理部104根据状态转变模型114，使本装置即数据判定装置101的运用状态转变而保持最新的运用状态。

[0054] 通信许可列表存储部109存储通信许可列表119a～119d作为通信许可规则141。图5～图8分别示出通信许可列表119a～119d的例子。图5～图8只是一例，通信许可列表119a～119d也可以不必如图5～图8所示。

[0055] 图5所示的通信许可列表119a具有规则编号、发送方信息、发送目的地信息、命令种类、数据大小、数据设定范围、计时器条件、标志条件以及动作编号的各项目。

[0056] 图6所示的通信许可列表119b具有运用状态、规则数、索引以及规则编号的各项目。

[0057] 图7所示的通信许可列表119c具有动作编号、计时器操作以及标志操作的各项目。

[0058] 图8所示的通信许可列表119d具有运用状态、发送方信息、发送目的地信息、索引开头编号以及检索个数的各项目。

[0059] 其中，各通信许可列表119a～119d中的项目不限于这些例子，可以任意设定。

[0060] 另外，各通信许可列表119a～119d的详细情况容后再述。

[0061] 检测规则存储部124存储检测规则列表125。检测规则列表125预先登记有请求通信与对其进行响应的响应通信之间的对应关系。为了根据请求通信与响应通信之间的对应关系判定通信数据正常还是异常，检测规则列表125记述有请求通信与响应通信之间的对应关系。图4示出检测规则列表125的例子。图4只是一例，检测规则列表也可以不必如图4所示。

[0062] 在图4的例子中，检测规则列表125包含24个检测规则126。

[0063] 在各检测规则126中附有固有的规则编号。各检测规则126具有运用状态、规则编号、发送方信息、发送目的地信息、请求通信的规则编号(以下作为请求规则编号)、响应通信的规则编号(以下作为响应规则编号)、命令种类、数据大小的上限值、数据设定范围以及命令执行周期的各项目。各检测规则126还可以具有计时器当前值、标志当前值等项目。这

些项目是任意的，只要是能够确定通信数据的项目，也可以是其他项目。

[0064] 如图4所示，在检测规则126中，在运用状态为停止中301的情况下，仅允许规则编号1～4而不允许除此以外的规则。同样，在运用状态为启动302的情况下，只允许规则编号5～8而不允许除此以外的规则。在运用状态为控制中303、关闭304、维护305的情况下也是同样的。这样，在检测规则列表125中，按照每个运用状态，对允许通信的通信数据登记请求通信与响应通信之间的对应关系。

[0065] 另外，在检测规则列表125中，请求通信与响应通信之间的对应关系是通过请求规则编号和响应规则编号的对来表现的。但是，也可以对1个请求规则编号设定多个响应规则编号。另外，也可以相反地对1个响应规则编号设定多个请求规则编号。

[0066] 具体地，对请求通信与响应通信之间的对应关系进行说明，在图4的检测规则列表125中，停止中301的规则编号“1”的检测规则126是从发送方“192.168.0.10”到发送目的地“192.168.0.50”的“装置状态取得”的请求通信。与该请求通信相对的响应规则编号为“2”。即，与该请求通信相对的响应通信是停止中301的规则编号“2”的检测规则126。该响应通信是从发送方“192.168.0.50”向请求“装置状态取得”的发送目的地“192.168.0.10”发送装置状态的信息的响应通信。这里，在规则编号“1”的检测规则126中，作为命令执行周期设定有“1±0.1”。由此可知，在“1±0.1”秒的周期内，“装置状态取得”的请求通信从发送方“192.168.0.10”反复发送到发送目的地“192.168.0.50”。这样，在各检测规则126中，如果本身是请求通信，则登记与该请求通信对应的响应通信的规则编号作为“响应规则编号”，反之，如果本身是响应通信，则登记与该响应通信对应的请求通信的规则编号作为“请求规则编号”。这样，在检测规则列表125中，请求通信与响应通信之间的对应关系是按照每个运用状态全部进行登记的。

[0067] 再列举具体的例子，检测规则列表125的启动302的规则编号“5”的请求通信和规则编号“6”的响应通信成对。这些检测规则的命令是“装置启动”。另外，请求通信与响应通信之间的对应关系被设定成，规则编号“7”的请求通信和规则编号“8”的响应通信成对，规则编号“9”的请求通信和规则编号“10”的响应通信成对，规则编号“11”的请求通信和规则编号“12”的响应通信成对……。

[0068] 这样，在检测规则列表125中，利用规则编号记述有请求通信与响应通信之间的对应关系。即，为了检测作为请求通信的通信数据与作为与之相对的响应通信的通信数据之间的对应关系，检测规则列表125记述有该对应关系。

[0069] 通信许可列表转换部123根据检测规则列表125生成图5～图8所示的通信许可列表119a～119d。

[0070] 通信许可列表转换部123首先对在检测规则中记述有对应关系的请求通信和响应通信分配1个以上的标志。这样，在通信许可列表119a、119c中，按照每个请求通信和每个响应通信使指定应该对该标志设定的值的标志操作的内容与用于判定在该标志中是否设定有该值的标志条件相对应地进行记述。在图5的通信许可列表119a中，按照每个通信数据记述有规则编号、动作编号以及标志条件之间的对应关系。另外，在图7的通信许可列表119c中，记述有动作编号与标志操作之间的对应关系。因此，通过同时参照通信许可列表119a、119c，由于这些动作编号是共同的，因此可知标志操作的内容与标志条件之间的对应关系。在本实施方式中，将通信许可列表119a、119c分开，但也可以将它们汇总作为1个通信许可

列表。

[0071] 并且，通信许可列表转换部123按照运用状态、发送方、发送目的地的优先顺序或者运用状态、发送目的地、发送方的优先顺序对通信许可列表的各通信数据进行排序，将排序后的顺位按照每个运用状态作为索引赋予给各通信数据，从而生成通信许可列表119b。

[0072] 另外，通信许可列表转换部123根据运用状态、发送方信息以及发送目的地信息，生成表示索引开头编号和检索范围内包含的检索个数的通信许可列表119d，该索引开头编号表示指定排序后的通信许可列表的应该参照的检索范围的开头指针。

[0073] 以下，使用图4～图8说明本实施方式的通信许可列表转换部123的动作。

[0074] 当给出图4所示的检测规则列表125时，通信许可列表转换部123用标志的ON/OFF来表现请求规则编号与响应规则编号之间的对应关系。

[0075] 例如，在检测规则列表125中，当规则编号1的请求通信的响应规则编号为“2”时，通信许可列表转换部123识别出规则编号“1”与规则编号“2”对应。因此，针对规则编号“1”和规则编号“2”分配标志F1。通信许可列表转换部123在通信许可列表119a的规则编号“1”的规则成立时，作为请求通信的动作，在图7的通信许可列表119c中，作为动作编号“1”的“标志操作”，记述为“F1＝1”以将标志F1设定为“1”。这就是标志的ON。接着，通信许可列表转换部123在图5的通信许可列表119a中，在规则编号“2”的通信数据中，作为标志条件记述“F1＝＝1”，使得在标志F1被设置为1时该通信的许可有效。由此，当规则编号“2”的通信数据为判定对象时，当运用状态为“停止中301”时，发送方信息为“192.168.0.50”，发送目的地信息为“192.168.0.10”，命令种类为“装置状态取得”，并且在标志管理部107的标志当前值115中，只在标志F1被设定为“1”时，该通信数据的通信许可是有效的。即，在标志F1未被设定为“1”的状态下发送了规则编号“2”的通信数据的情况下，该通信数据是基于非法访问的通信数据，因此，可以判定为应该使通信不允许。

[0076] 另外，通信许可列表转换部123在通信许可列表119a的规则编号“2”的规则成立时，作为响应通信的动作，在图7的通信许可列表119c中，作为动作编号“2”的“标志操作”，记述为“F1＝0”以将标志F1设定为“0”。这就是标志的OFF。

[0077] 这样，通信许可列表转换部123在通信许可列表119a～119d中，用标志的ON/OFF来表现请求规则编号与响应规则编号之间的对应关系。

[0078] 由此，后述的判定部103在进行作为请求通信的通信数据的判定时，在判定为该通信数据正常的情况下，作为该请求通信的动作，根据通信许可列表中记述的标志操作的内容，设置标志管理部107的标志的当前值。这里，例如将标志F1设定为1，将标志F1设为ON。

[0079] 判定部103在进行与该请求通信对应的响应通信的通信数据的判定时，根据通信许可列表中记述的标志条件，判定标志F1的当前值与作为请求通信的动作而被更新后的标志F1的值即“1”是否一致，由此判定该响应通信是否与之前的请求通信正确地对应，判定该响应通信是否正常。

[0080] 判定部103在判定为响应通信正常的情况下，作为该响应通信的动作，按照通信许可列表中记述的标志操作的内容，重置标志管理部107的标志的当前值。即，这里例如在标志F1中设定0。

[0081] 这样，在本实施方式1中，判定部103能够通过标志的ON/OFF来确认请求通信与响应通信之间的对应关系。

[0082] 另外，通信许可列表转换部123按照每个运用状态，生成表示在各运用状态下应用的规则数和规则编号的图6的通信许可列表119b。通信许可列表转换部123在生成图6的通信许可列表119b时，根据运用状态、发送方信息以及发送目的地信息的优先级，按照运用状态、发送目的地以及发送方的优先顺序，对通信数据进行排序。在图6的通信许可列表119b中，按照运用状态、发送方、发送目的地的优先顺序对图1的通信许可列表119a的各通信数据进行排序，将排序后的顺位按照每个运用状态作为索引被赋予给各通信数据。即，例如在停止中301中，按照规则编号1、3、2、4的顺序对通信数据进行排序，对它们分别赋予索引编号0、1、2、3。

[0083] 另外，通信许可列表转换部123根据发送方信息和发送目的地信息，生成用于计算通信许可列表119b的应该参照的索引开头编号和检索个数的、图8的通信许可列表119d。在图8的通信许可列表119d中，在停止中301中，当发送方信息为“192.168.0.50”且发送目的地信息为“192.168.0.10”时，索引开头编号为“2”，检索个数为“2”。由此可知，当判定部103基于索引开头编号“2”和检索个数“2”，参照图6的通信许可列表119b时，在排序后的通信许可列表中，从“2”开始的索引成为检索范围的开头指针，包含该开头指针的检索个数2个是检索范围。这样，判定部103确定检索范围，对符合该检索范围的通信许可列表的通信数据和作为判定对象的通信数据进行比较，由此判定作为判定对象的通信数据正常还是异常。

[0084] 并且，也可以是，通信许可列表转换部123根据图5的通信许可列表119a中记载的通信许可规则141的参照频率，重新排列图6的通信许可列表119b的规则编号。此时，按照保持发送方信息与发送目的地信息的对应关系的方式实施重新排列。例如，在维护305的规则中，由于规则编号19、21是同一发送方/同一发送目的地的规则，因此可以重新排列，由于规则编号21、23的发送方/发送目的地不同，因此不能重新排序。

[0085] 另外，在本实施方式中，说明了通信许可列表转换部123这样地生成4个通信许可列表119a～119d的情况，但不限于该情况，也可以仅生成其中的通信许可列表119a、119c。但是，在生成了通信许可列表119b、119d的情况下，由于能够缩小检索范围，因此能够缩短判定部103的判定处理的处理时间。

[0086] 返回图1的说明。通信部102经由网络400而与监视控制装置200连接。通信部102从监视控制装置200经由网络400接收接收数据112，将接收到的接收数据112输出给判定部103。另外，通信部102从判定部103接收发送数据111，将接收到的发送数据111经由网络400发送给监视控制装置200。通信部102构成网络输入输出部。

[0087] 状态管理部104根据状态转变模型114管理数据判定装置101的运用状态。状态转变模型114是预先设定的，存储在数据判定装置101的存储区域。存储区域例如由后述的图9的存储器903或辅助存储装置902构成。在被输入到来自操作部106的操作信号120、来自控制器300的发送数据111、来自监视控制装置200的接收数据112以及来自计时器108的计时器当前值中的至少任意一个的情况下，状态管理部104根据状态转变模型114，使本装置的运用状态转变。

[0088] 另外，在由判定部103判定为通信判定数据113符合通信许可规则141的情况下，即，由判定部103判定为通信判定数据113正常的情况下，状态管理部104根据状态转变模型114，使本装置的运用状态转变。另外，也可以是，在由判定部103判定为通信判定数据113不符合通信许可规则141的情况下，即由判定部103判定为通信判定数据113异常的情况下，状

态管理部104使本装置的运用状态转变到异常状态。另外，也可以是，状态管理部104在判定为通信判定数据113正常的情况下，仅转变运用状态。如上所述，状态管理部104保有作为本装置的数据判定装置101的当前的运用状态121。

[0089] 操作部106由用户操作的按钮、触摸面板、键盘、鼠标等构成。操作部106在有来自用户的操作输入时，输出表示已受理针对本装置的操作的操作信号120。

[0090] 计时器108计测本装置的运用状态持续的时间。按照每个运用状态，预先设定有该运用状态持续的时间。在运用状态转变时，在计时器108中设定该运用状态的持续时间。计时器108在固定周期(例如1ms)内从已设定的持续时间的值中减去固定值，在值变为0的情况下结束减法运算，作为时限已到信号，输出值为“0”的计时器当前值117。另外，计时器108按照来自判定部103和状态管理部104的请求，输出当前的计时器108的值作为计时器当前值117。另外，不需要对全部运用状态预先设定持续时间，也可以仅对特定的运用状态设定持续时间。

[0091] 标志管理部107保持从判定部103输入的标志设定值116，对判定部103和状态管理部104输出标志当前值115。

[0092] 判定部103从通信部102取得接收数据112作为通信判定数据113，并且从应用310取得发送数据111。另外，判定部103取得状态管理部104保有的本装置的运用状态作为当前的运用状态121。另外，判定部103从计时器108取得计时器当前值117，进而从标志管理部107取得标志当前值115。判定部103使用当前的运用状态121、计时器当前值117、标志当前值115以及通信许可列表存储部109存储的通信许可列表119a～119d，判定通信判定数据113在当前的运用状态121下是否符合通信许可规则141。

[0093] 首先，判定部103从接收数据112或发送数据111中提取发送方信息和发送目的地信息。接着，判定部103使用提取出的发送方信息和发送目的地信息以及从状态管理部104取得的当前的运用状态121，根据图8的通信许可列表119d，计算索引开头编号和检索个数。判定部103根据计算出的索引开头编号和检索个数，基于图6的通信许可列表119b，确定应该参照的检索范围，提取符合该检索范围的规则编号。例如，在判定运用状态为停止中301的状态、发送方信息为192.168.0.50、发送目的地信息为192.168.0.10的通信判定数据113时，判定部103从图8的通信许可列表119d中提取索引开头编号“2”，并且提取检索个数“2”。这样，判定部103从图6的通信许可列表119b中，提取运用状态为停止中301、索引编号为从“2”开始的规则的规则编号为“2”的情况，进而根据检索个数“2”的信息，提取规则编号“2”和与其相邻的规则编号“4”。这样，判定部103判定通信判定数据113是否符合图5的通信许可列表119a的规则编号“2”或“4”中的任意一个的通信许可规则141。

[0094] 这样，判定部103判定通信判定数据113是否符合通信许可规则141。判定部103在判定为通信判定数据113符合通信许可规则141的情况下，判定为通信判定数据113正常，并且执行与符合的规则编号的通信许可规则141中记载的动作编号对应的动作。例如，在通信判定数据113符合规则编号9的通信许可规则141的情况下，根据图5的通信许可列表119a的规则编号9的通信许可规则141，提取动作编号“9”。这样，判定部103执行图7的通信许可列表119c的动作编号“9”中记载的动作。即，判定部103根据图7的通信许可列表119c的动作编号9的“计时器操作”的内容，将“0”代入到计时器108的计时器值T2中，根据动作编号9的“标志操作”的内容，对标志管理部107的标志F5设置“1”。

[0095] 另一方面，判定部103在判定为通信判定数据113不符合通信许可规则141的情况下，判定为通信判定数据113异常，切断控制器300与监视控制装置200之间的通信。另外，判定部103对警报部110输出表示通信判定数据113异常的判定结果122。

[0096] 警报部110在被判定部103输入表示通信判定数据113异常的判定结果122的情况下，向用户输出用于通知异常的警报。即，警报部110在判定结果122异常的情况下发出警报。警报部110发出的警报可以是视觉上的警报，或者也可以是听觉上的警报。在是视觉上的警报的情况下，可以是警报部110例如由灯构成，将该灯的点亮或闪烁动作作为“警报”。另外，在警报是听觉上的警报的情况下，可以是警报部110由蜂鸣器或扬声器构成，将蜂鸣音的发声或声音消息的发声作为“警报”。另外，作为“警报”，也可以是，警报部110例如经由网络400向其他服务器发送警报信号。另外，也可以是，警报部110由后述的图9的显示器908构成，在显示画面显示判定部103的判定结果122。在该情况下，在判定结果122正常的情况下，在显示画面上进行表示“判定结果122正常”的显示。另一方面，在判定结果122异常的情况下，在显示画面上进行表示“判定结果122异常”的显示，并且产生警报。

[0097] 接着，使用图2对图1的数据判定装置101的变形例进行说明。图2示出进行与图1的数据判定装置101不同的动作的数据判定装置101a的结构。

[0098] 在图1所示的数据判定装置101中，示出了在判定部103判定了通信判定数据113之后，对接收数据112或发送数据111进行通信的结构。

[0099] 另一方面，在图2所示的数据判定装置101a中，应用310和监视控制装置200不经由数据判定装置101a而直接进行发送数据111和接收数据112的通信。该通信可以使用网络400进行，或者也可以使用专用线路进行。此时，数据判定装置101a使用通信部102，捕捉监视控制装置200与应用310之间的通信而取得通信判定数据113，判定已取得的通信判定数据113。但是，在图2的数据判定装置101a中，即使在判定部103的判定结果122异常的情况下，判定部103也不能切断应用310与监视控制装置200之间的通信。另一方面，由于能够通过由警报部110发出的警报向用户通知异常，因此，接收到异常通知的用户能够针对第三者的非法攻击进行某种应对。

[0100] 另外，图2的数据判定装置101a的其他结构和动作与图1的数据判定装置101相同，因此这里省略其说明。

[0101] 接着，使用图9，对本实施方式的数据判定装置101的硬件结构的一例进行说明。

[0102] 如图9所示，数据判定装置101例如由计算机构成。

[0103] 构成数据判定装置101的计算机具有处理器901、辅助存储装置902、存储器903、通信装置904、输入接口905以及显示器接口906这样的硬件。

[0104] 处理器901经由信号线910而与其他硬件902～906连接，对这些其他硬件902～906进行控制。

[0105] 输入接口905与输入装置907连接。

[0106] 显示器接口906与显示器908连接。

[0107] 数据判定装置101中的作为输入部的通信部102和操作部106是输入装置907和输入接口905。另外，数据判定装置101的输出部是显示器908和显示器接口906。另外，在图9中，虽然省略图示，但在数据判定装置101中还设置有构成警报部110的硬件。

[0108] 处理器901由进行处理的IC(Integrated Circuit:集成电路)构成。处理器901例

如是CPU(Central Processing Unit:中央处理单元)、DSP(Digital Signal Processor:数字信号处理器)、GPU(Graphics Processing Unit:图形处理单元)。

[0109] 辅助存储装置902例如由ROM(Read Only Memory:只读存储器)、闪存、HDD(Hard Disk Drive:硬盘驱动器)构成。

[0110] 存储器903例如由RAM(Random Access Memory:随机存取存储器)构成。

[0111] 通信装置904包含接收数据的接收机9041和发送数据的发送机9042。通信装置904例如由通信芯片或NIC(Network Interface Card:网络接口卡)构成。

[0112] 输入接口905是连接输入装置907的电缆911的端口。输入接口905例如由USB(Universal Serial Bus:通用串行总线)端子构成。

[0113] 显示器接口906是连接显示器908的电缆912的端口。显示器接口906例如由USB端子或HDMI(注册商标)(High Definition Multimedia Interface:高清晰度多媒体接口)端子构成。

[0114] 输入装置907例如由鼠标、键盘或触摸面板构成。

[0115] 显示器908例如由LCD(Liquid Crystal Display:液晶显示器)构成。

[0116] 在辅助存储装置902中存储有实现图1所示的状态管理部104、判定部103、警报部110、标志管理部107、计时器108以及通信许可列表转换部123(以下将状态管理部104、判定部103、警报部110、标志管理部107、计时器108以及通信许可列表转换部123总记作“部”)的功能的程序。实现上述的数据判定装置101具有的“部”的功能的程序也被称作数据判定程序。实现“部”的功能的程序可以是1个程序,也可以由多个程序构成。该程序被加载到存储器903,被读入到处理器901,由处理器901执行。

[0117] 并且,在辅助存储装置902中还存储有OS(Operating System:操作系统)。并且,OS的至少一部分被加载到存储器903,处理器901一边执行OS,一边执行实现“部”的功能的程序。

[0118] 在图9中图示出1个处理器901,但数据判定装置101也可以具有多个处理器901。并且,也可以是,多个处理器901协作执行实现“部”的功能的程序。

[0119] 另外,表示“部”的处理结果的信息、数据、信号值、变量值等作为文件存储在存储器903、辅助存储装置902或者处理器901内的寄存器或高速缓冲存储器中。

[0120] 另外,也可以通过“处理线路”提供“部”。

[0121] 另外,也可以将“部”改写成“电路”或“工序”或“步骤”或“处理”。另外,也可以将“处理”改写成“电路”或“工序”或“步骤”或“部”。

[0122] “电路”和“处理线路”的概念不仅包含处理器901,而且包含逻辑IC或GA(Gate Array:门阵列)或ASIC(Application Specific Integrated Circuit:面向特定用途的集成电路)或FPGA(Field-Programmable Gate Array:现场可编程门阵列)这样的其他种类的处理电路。

[0123] 另外,被称作程序产品的是记录有实现作为“部”说明的功能的程序的存储介质、存储装置等,与外观的形式无关,加载有计算机能读取的程序。

[0124] 接着,使用图10,对作为本实施方式的数据判定装置101的数据判定方法的数据判定处理S100进行说明。

[0125] 如上所述,数据判定装置101具有存储状态转变模型114的状态转变模型存储部

105以及存储通信许可规则141作为通信许可列表119a～119d的通信许可列表存储部109。

[0126] 如图10所示，首先，在步骤S101的状态管理处理中，状态管理部104根据状态转变模型114执行保有本装置的运用状态的状态管理处理S101。即，状态管理部104根据操作信号120、接收数据112、发送数据111、来自标志管理部107的标志当前值115以及来自计时器108的计时器当前值117中的一个以上，按照状态转变模型114使本装置的运用状态转变而保有最新的运用状态。

[0127] 接着，在步骤S110的通信处理中，通信部102和判定部103取得通信判定数据113。具体而言，通信部102取得接收数据112，判定部103取得发送数据111。

[0128] 接着，在步骤S120的判定处理中，判定部103从通信部102取得通过步骤S110的通信处理而取得的接收数据112，并且从状态管理部104取得通过步骤S101的状态管理处理而保有的本装置的运用状态作为当前的运用状态121。另外，判定部103从计时器108取得计时器当前值117，从标志管理部107取得标志当前值115。判定部103使用当前的运用状态121、计时器当前值117、标志当前值115以及通信许可列表存储部109中存储的通信许可列表119a～119d，判定通信判定数据113在当前的运用状态121下是否符合通信许可规则141。判定部103输出判定结果122。

[0129] 接着，在步骤S130的分支处理中，判定判定结果122是否正常。在判定结果122正常即通信判定数据113符合通信许可规则141的情况下，进入步骤S140的正常处理。另一方面，在判定结果122异常即通信判定数据113不符合通信许可规则141的情况下，进入步骤S150的异常处理。

[0130] 在步骤S140的正常处理中，状态管理部104使用取得的通信判定数据113、计时器当前值117、标志当前值115以及操作信号120中的任意一个以上，按照状态转变模型114使本装置的运用状态转变。

[0131] 另一方面，在步骤S150的异常处理中，状态管理部104使本装置的运用状态转变成异常状态。另外，警报部110根据来自判定部103的判定结果122通知警报。

[0132] 接着，使用图11，对图10的步骤S120的判定部103的判定处理进行说明。

[0133] 首先，在步骤S121中，判定部103取得接收数据112或发送数据111作为通信判定数据113，对取得的通信判定数据113进行分析。判定部103通过该分析从通信判定数据113中提取判定所需的元素。提取出的元素是记载在图5的通信许可列表119a中的项目，即发送方信息、发送目的地信息、命令种类等。

[0134] 接着，在步骤S122中，判定部103从状态管理部104取得当前的运用状态121。另外，判定部103从通信许可列表存储部109取得通信许可列表119a～119d。

[0135] 在步骤S123中，判定部103根据在步骤S122中取得的当前的运用状态121和通信许可列表119a～119d，判定通信判定数据113是否是在当前的运用状态121下被许可的通信数据，即是否符合通信许可规则141。如果判定的结果是通信判定数据113符合通信许可规则141，则进入步骤S124。另一方面，如果通信判定数据113不符合通信许可规则141，即是通信判定数据113不被许可的通信，则进入步骤S125。

[0136] 在步骤S124中，判定部103输出表示“正常”的判定结果122。另外，执行与符合的通信许可规则141中记载的动作编号对应的动作。判定部103根据该动作编号，参照图7的通信许可列表119c，例如在标志管理部107中设置规定的标志，或者在计时器108中设置预定的

值。

[0137] 另一方面，在步骤S125中，判定部103将表示“异常”的判定结果122输出到警报部110，并且切断通信判定数据113的通信。或者，也可以是，判定部103仅输出表示“异常”的判定结果122而不切断通信判定数据113的通信。

[0138] 接着，使用图12，对本发明的通信许可列表转换部123的动作进行说明。

[0139] 首先，在步骤S201中，通信许可列表转换部123从检测规则存储部124取得图4的检测规则列表125。通信许可列表转换部123根据检测规则列表125分析每个规则的请求与响应之间的对应关系。分析结果为以下3种。

[0140] A)请求与响应1:1对应

[0141] B)请求与响应0:m对应(m≥1)

[0142] C)请求与响应1:n对应(n≥2)

[0143] A)是1个响应通信对应1个请求通信的关系。例如，可以是使用TCP的Read通信和Write通信。

[0144] B)是对应于请求通信存在多个响应通信，但响应通信之间不存在依存关系的关系。例如，可以是基于广播的保持活跃通信等。

[0145] C)是针对1个请求通信存在多个响应通信的候选，只要其中1个成立，则其他变为无效的关系。例如，可以是使用UDP的连接型的通信等。

[0146] 在步骤S201的分析中，在分析结果为A)的情况下进入步骤S202，在分析结果为B)的情况下进入步骤S205，在分析结果为C)的情况下进入步骤S208。以下，对各情况进行说明。

[0147] 在分析结果为A)的情况下，首先，在步骤S202中，按照图4的检测规则列表125的请求规则的每个规则编号定义1个标志，在与该规则编号的动作编号对应的图7的通信许可列表119c的动作的标志操作中，追加该标志的设定操作。接着，在步骤S203中，在图5的通信许可列表119a的响应规则中，追加判定在步骤S202中分配的标志是否被设置的标志条件。接着，在步骤S204中，在与响应规则的动作编号对应的通信许可列表119c的标志操作中，追加在步骤S202中分配的标志的重置操作。

[0148] 在分析结果为B)的情况下，首先，在步骤S205中，按照图4的检测规则列表125的请求规则的每个规则编号定义m个标志，在与该规则编号的动作编号对应的图7的通信许可列表119c的动作的标志操作中，追加该标志的设定操作。接着，在步骤S206中，在图5的通信许可列表119a的响应规则中，逐个分配在步骤S205中分配的m个标志，追加判定该标志是否被设置的标志条件。接着，在步骤S207中，在与响应规则的动作编号对应的通信许可列表119c的标志操作中，追加在步骤S206中分配的标志的重置操作。

[0149] 在分析结果为C)的情况下，首先，在步骤S208中，按照图4的检测规则列表125的请求规则的每个规则编号定义1个标志，在与该规则编号的动作编号对应的图7的通信许可列表119c的动作的标志操作中，追加该标志的设定操作。接着，在步骤S209中，对图5的通信许可列表119a的全部响应规则，追加判定在步骤S208中分配的标志是否被设置的标志条件。接着，在步骤S210中，在与响应规则的动作编号对应的通信许可列表119c的标志操作中，追加在步骤S208中分配的标志的重置操作。

[0150] 以上，关于本实施方式的数据判定装置101的数据判定方法和数据判定处理S100

的说明结束。

[0151] 如上所述，本实施方式的数据判定装置101具有以下的结构。

[0152] (A)标志管理部107，其存储针对本装置设定的标志的当前值。

[0153] (B)状态管理部104，其存储在多个运用状态之间转变的本装置的当前的运用状态121，并且根据来自外部的作为输入信号的例如通知数据以及标志管理部107存储的标志的当前值115中的任意一个以上，按照定义了运用状态之间的转变的状态转变模型114，使本装置的运用状态转变。

[0154] (C)通信许可列表转换部123，其将检测规则列表125转换成预先按照每个运用状态登记被许可通信的通信数据的通信许可列表119a、119b，该检测规则列表125记述有构成请求通信的通信数据与构成针对请求通信的响应通信的通信数据之间的对应关系。

[0155] (D)判定部103，其使用状态管理部104存储的本装置的当前的运用状态121、通信许可列表119a、119c以及标志管理部107存储的标志的当前值115中的任意一个以上，判定被输入到本装置的通信数据113是否是通信许可列表119a、119c中登记的当前的运用状态121下的通信数据，由此判定被输入到本装置的通信数据113正常还是异常。

[0156] 通信许可列表转换部123在将检测规则转换成通信许可列表119a、119c时，针对在检测规则中记述有对应关系的请求通信和响应通信分配1个以上的标志，使指定了针对该标志应该设定的值的标志操作的内容与用于判定在所述标志中是否设定有该值的标志条件之间的对应关系记述在所述通信许可列表中，

[0157] 判定部103判定作为请求通信的通信数据，在判定为该通信数据正常的情况下，作为该请求通信的动作，根据通信许可列表中记述的标志操作的内容，更新标志管理部107的标志的当前值。这里，例如在标志F1中设定1。

[0158] 判定部103在判定与该请求通信对应的响应通信的通信数据时，根据通信许可列表中记述的标志条件，判定标志F1的当前值与作为请求通信的动作而被更新后的标志F1的值即“1”是否一致，由此判定该响应通信是否与之前的请求通信正确地对应，判定该响应通信是否正常。

[0159] 判定部103在判定为响应通信正常的情况下，作为该响应通信的动作，按照通信许可列表中记述的标志操作的内容，重置标志管理部107的标志的当前值。即，这里例如在标志F1中设定0。

[0160] 这样，判定部103在判定数据时，根据标志的当前值的ON/OFF，确认请求与响应之间的对应关系，在不能取得请求与响应之间的对应关系的情况下，判定为通信数据是由非法攻击引起的，因此，能够更高度地进行攻击的检测。

[0161] 另外，判定部103在判定为通信数据异常的情况下，切断该通信数据的通信。

[0162] 根据以上的结构，在本实施方式的数据判定装置中，在通信许可列表中定义正常的通信时，记述请求通信与响应通信之间的对应关系，因此，能够在不引起组合爆炸的情况下记述全部通信数据。另外，使其可以通过标志的设置/重置来判定请求通信与响应通信之间的对应关系，使其还考虑请求通信与响应通信之间的对应关系来判定通信数据正常还是异常，因此，即使在由第三者侵占服务器而被该服务器进行了网络攻击的情况下，也能够检测出通信数据是非法的。另外，通过定义请求通信与响应通信之间的对应关系，能够高速地进行增大的检测规则的检索。

[0163] 另外，通信许可列表转换部123也可以还生成通信许可列表119b、119d。

[0164] 即，通信许可列表转换部123按照运用状态、发送方、发送目的地的优先顺序或者运用状态、发送目的地、发送方的优先顺序对通信许可列表的通信数据进行排序，将排序后的顺位作为索引赋予给各所述通信数据，从而生成通信许可列表119b。

[0165] 另外，通信许可列表转换部123根据运用状态、发送方的信息以及发送目的地的信息，生成表示索引开头编号和检索个数的通信许可列表119d，该索引开头编号表示指定应该参照的排序后的通信许可列表119b的检索范围的开头指针。

[0166] 此时，判定部103从状态管理部104取得本装置的当前的运用状态121，并且从作为判定对象的通信数据113取得发送方的信息和发送目的地的信息，根据当前的运用状态121、发送方的信息以及发送目的地的信息，从通信许可列表119d中提取索引开头编号和检索个数，根据提取出的索引开头编号和检索个数来确定排序后的通信许可列表119b中应参照的检索范围，通过对符合该检索范围的通信许可列表119a的通信数据与作为判定对象的通信数据113进行比较，判定作为判定对象的通信数据113正常还是异常。

[0167] 另外，根据需要，本实施方式的数据判定装置101还可以具有以下的结构。

[0168] (E)计时器108，其计测在多个运用状态之间转变的本装置的当前的运用状态的持续时间。

[0169] (F)通信许可列表存储部109，其存储通信许可列表119a～119d。

[0170] (G)警报部110，其在判定部103判定为通信数据异常的情况下，发出警报。

[0171] (H)检测规则存储部124，其存储检测规则。

[0172] 根据本实施方式1，如上所述，判定部103根据标志的当前值的ON/OFF，确认请求与响应之间的对应关系，在无法取得请求与响应之间的对应关系的情况下，能够检测出通信数据是由非法攻击引起的。使用图13对其中一例进行说明。图13以BACnet通信为例进行说明。图13中的装置1和装置2相当于控制器300和监视控制装置200。在图13中，省略数据判定装置101的图示。

[0173] 在图13中，设(A)是正常时的序列，设(B)是攻击时的序列。在(A)、(B)中，通信数据T1的请求与通信数据T2的响应相对应，通信数据T3、T5、T7的请求与通信数据T4、T6的响应相对应。针对各个对应分配标志。

[0174] 在(A)中，针对来自装置1的“Confirmed Request”请求，装置2返回“Complex Ack”或“Abort”。

[0175] 即，在图13的(A)中，针对通信数据T1的“Confirmed Request”请求，返回通信数据T2的“Abort”，针对通信数据T3的“Confirmed Request”请求，返回通信数据T4的“Complex Ack”。

[0176] 另外，在如通信数据T4那样，装置2对装置1响应“Complex Ack”的情况下，装置1返回“Segment Ack”，进行2次该交换，结束通信。即，在装置2响应通信数据T4的“Complex Ack”的情况下，装置1返回通信数据T5的“Segment Ack”。这是第1次交换。之后，装置2再次响应通信数据T6的“Complex Ack”，装置1返回通信数据T7的“Segment Ack”。这是第2次交换。这样，结束通信。

[0177] 以上是正常时的序列(A)。此时，数据判定装置101的判定部103根据标志的值，判定请求与响应之间的对应关系是否成立。

[0178] 对此，在(B)中，示出在装置2中安装有非法程序的情况。(B)中的标号T3～T6与(A)中的标号T3～T6相对应。在(B)中，设由于装置2的非法程序，在从装置2向装置1第2次发送“Complex Ack”之前，进行了从装置2流出“Abort”这样的攻击。在这种情况下，由于从装置2发送给装置1的不是“Complex Ack”并且标志的值不一致，因此，数据判定装置101的判定部103判定为请求通信与响应通信之间的对应关系不成立，判断为通信异常，不进行更多的通信。即使装置2上的正规程序随后流出“Complex Ack”，也无法完成通信。

[0179] 另外，由于来自装置2的“Abort”本身是正常的通信，因此，如果是现有的数据判定装置，则有可能漏掉这种情况，但是，在本实施方式1的数据判定装置中，由于在数据判定中使用请求通信与响应通信之间的对应关系，因此，即使在这样的装置2被第三者侵占的情况下，也能够检测来自第三者的攻击。

[0180] 并且，根据本实施方式1的数据判定装置，即使检测规则增大，由于根据发送方/发送目的地制作索引，缩小检索范围，因此，能够高速地进行通信许可列表与判定对象数据的匹配。

[0181] 并且，根据本实施方式1的数据判定装置，除了基于频度的再排序以外，都能够通过事前计算来执行，因此，能够在对判定处理不造成影响的情况下实现。

[0182] 标号说明

[0183] 101:数据判定装置;102:通信部;103:判定部;104:状态管理部;105:状态转变模型存储部;106:操作部;107:标志管理部;108:计时器;109:通信许可列表存储部;110:警报部;111:发送数据;112:接收数据;113:通信判定数据;114:状态转变模型;115:标志当前值;116:标志设定值;117:计时器当前值;118:计时器设定值;119a、119b、119c、119d:通信许可列表;200:监视控制装置;300:控制器;310:应用。

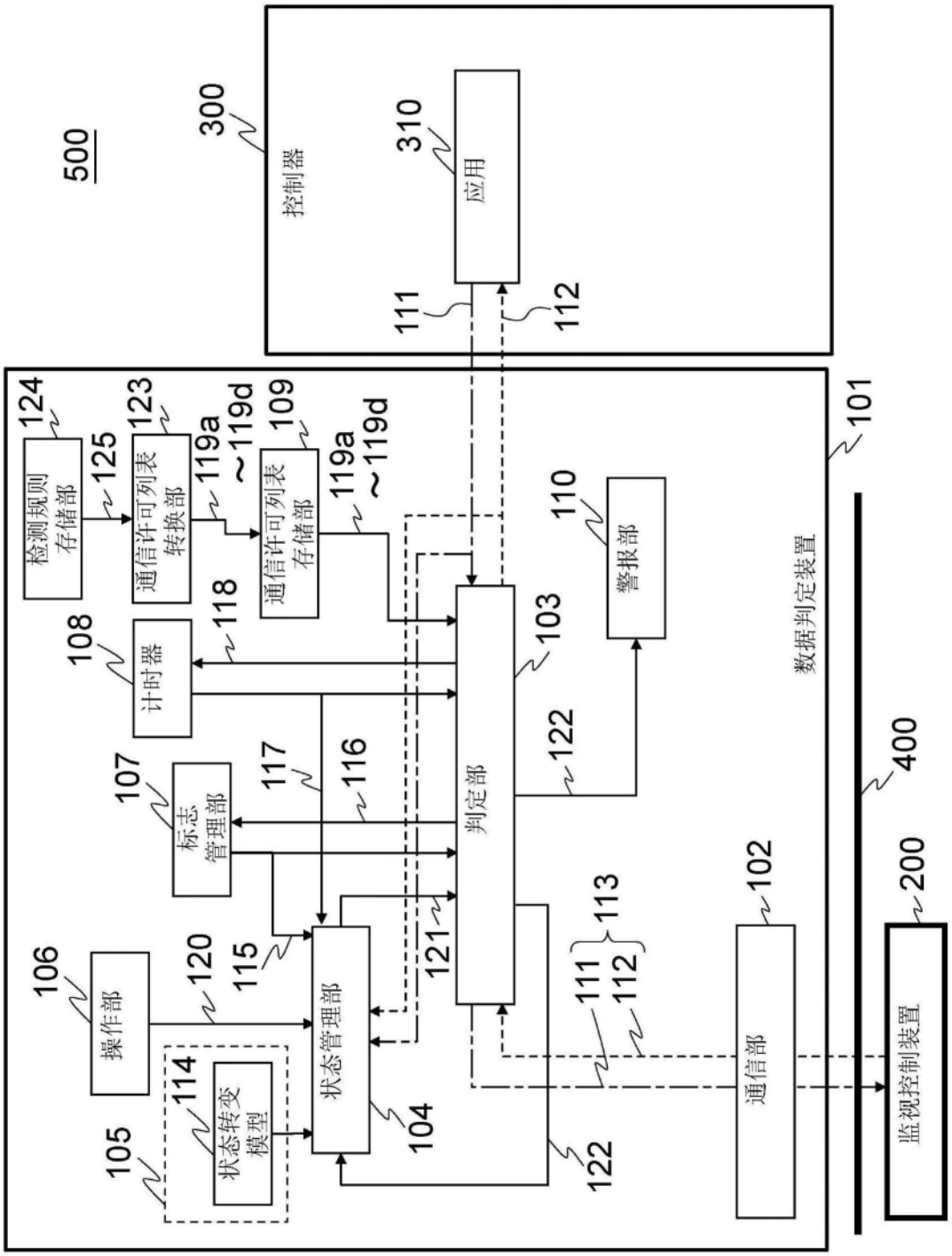

500
300
控制器
310
应用
111
112
101
数据判定装置
124
检测规则存储部
125
123
通信许可列表转换部
119a ~119d
109
通信许可列表存储部
119a ~119d
110
警报部
108
计时器
118
103
判定部
122
107
标志管理部
117
116
400
106
操作部
120
115
状态管理部
121
113
111
112
102
通信部
200
监视控制装置
114
状态转变模型
105
104
122

图1

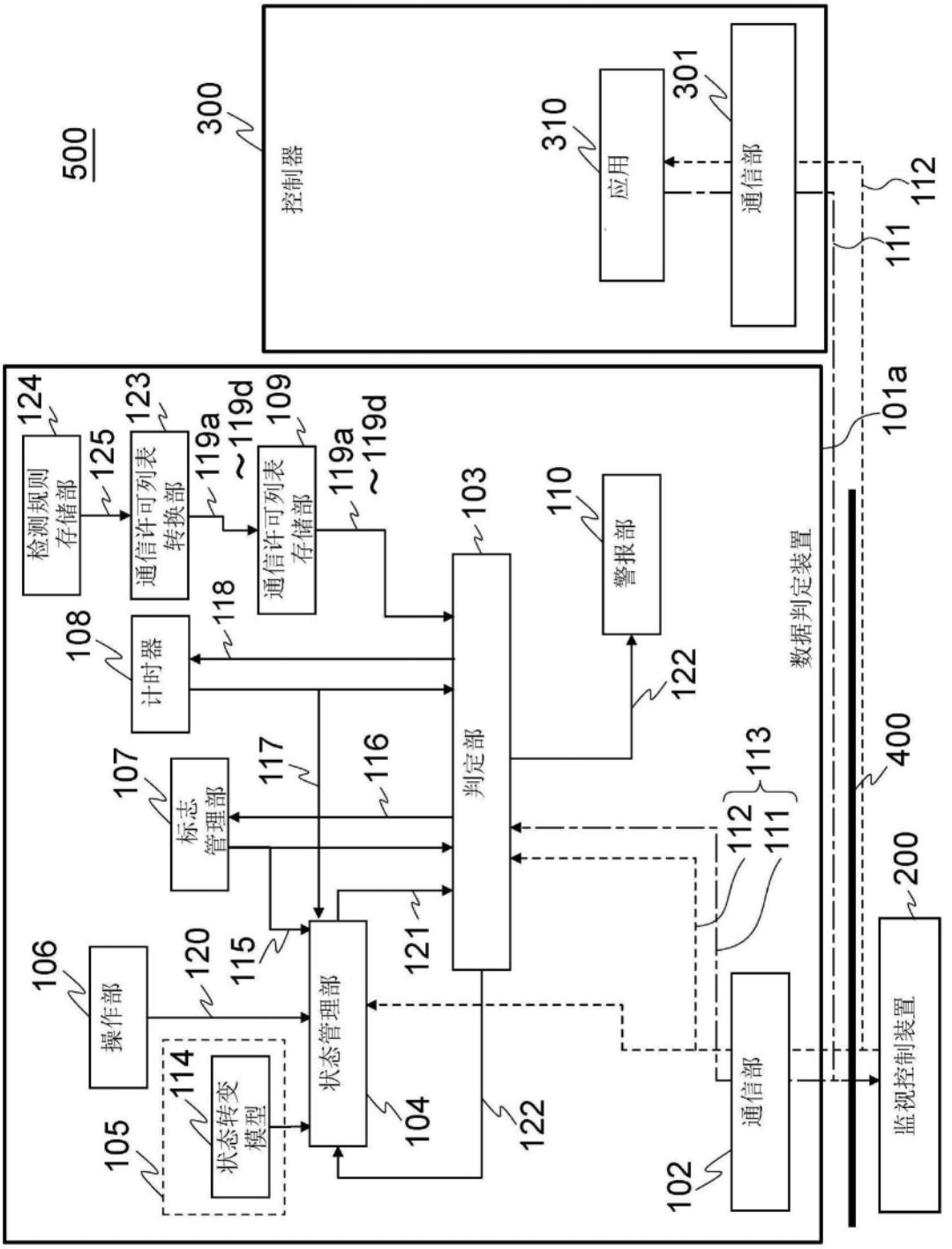

500
300
控制器
310
应用
301
通信部
112
111
101a
数据判定装置
124
检测规则存储部
125
123
通信许可列表转换部
119a ~119d
109
通信许可列表存储部
119a ~119d
103
110
警报部
108
计时器
118
122
107
标志管理部
117
116
判定部
113
112
111
400
106
操作部
120
115
121
200
114
状态转变模型
状态管理部
105
104
122
102
通信部
监视控制装置

图2

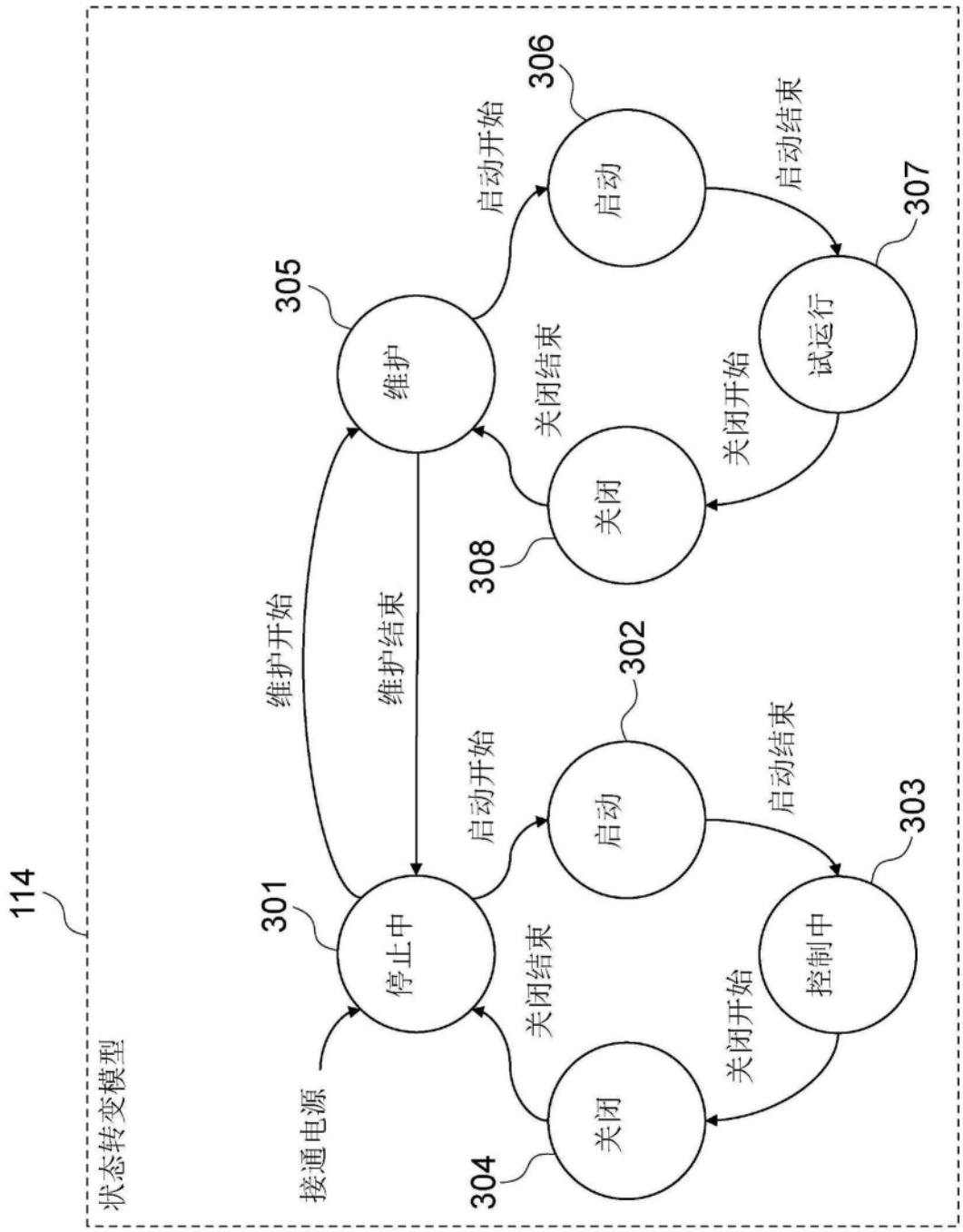
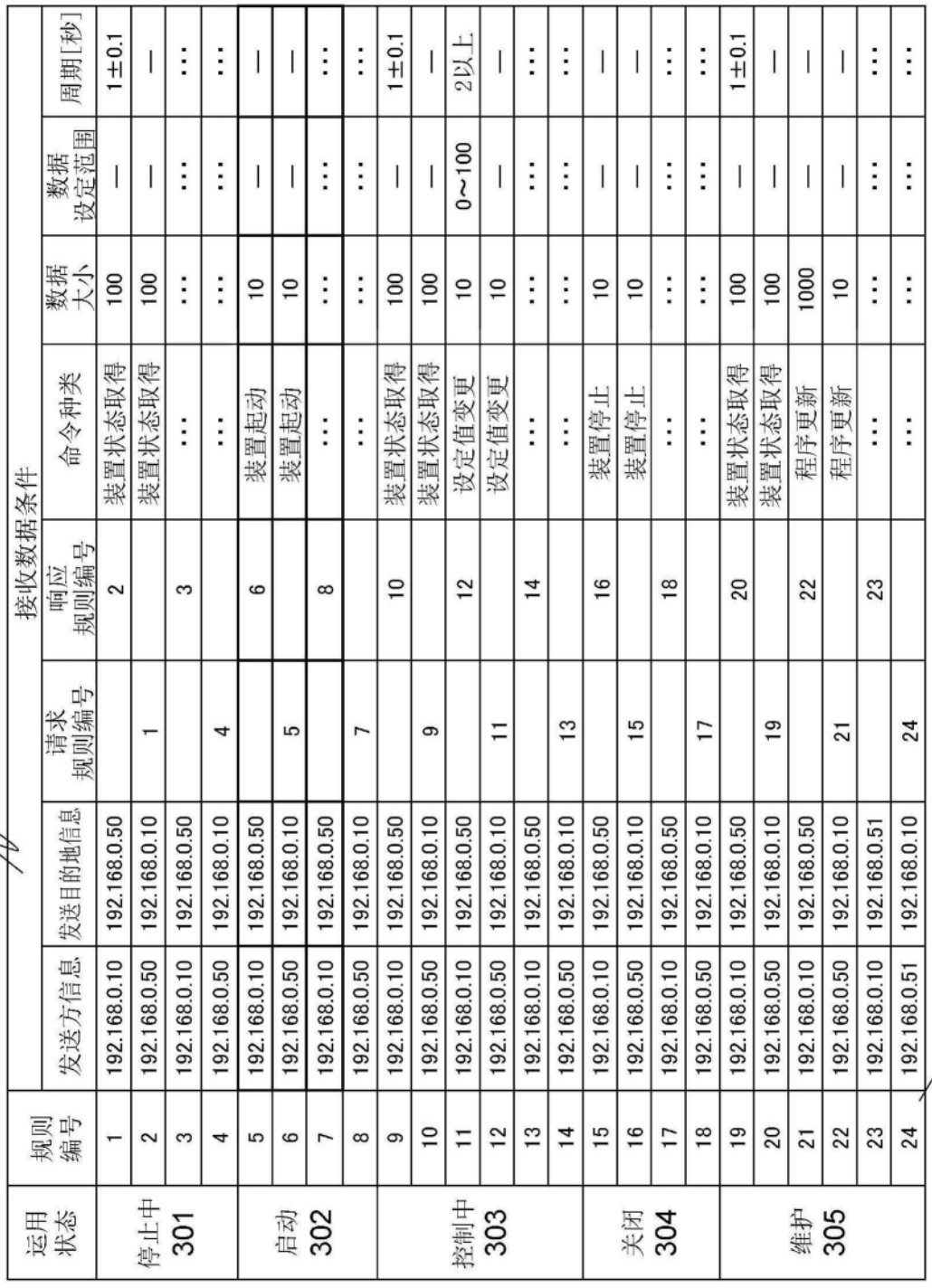
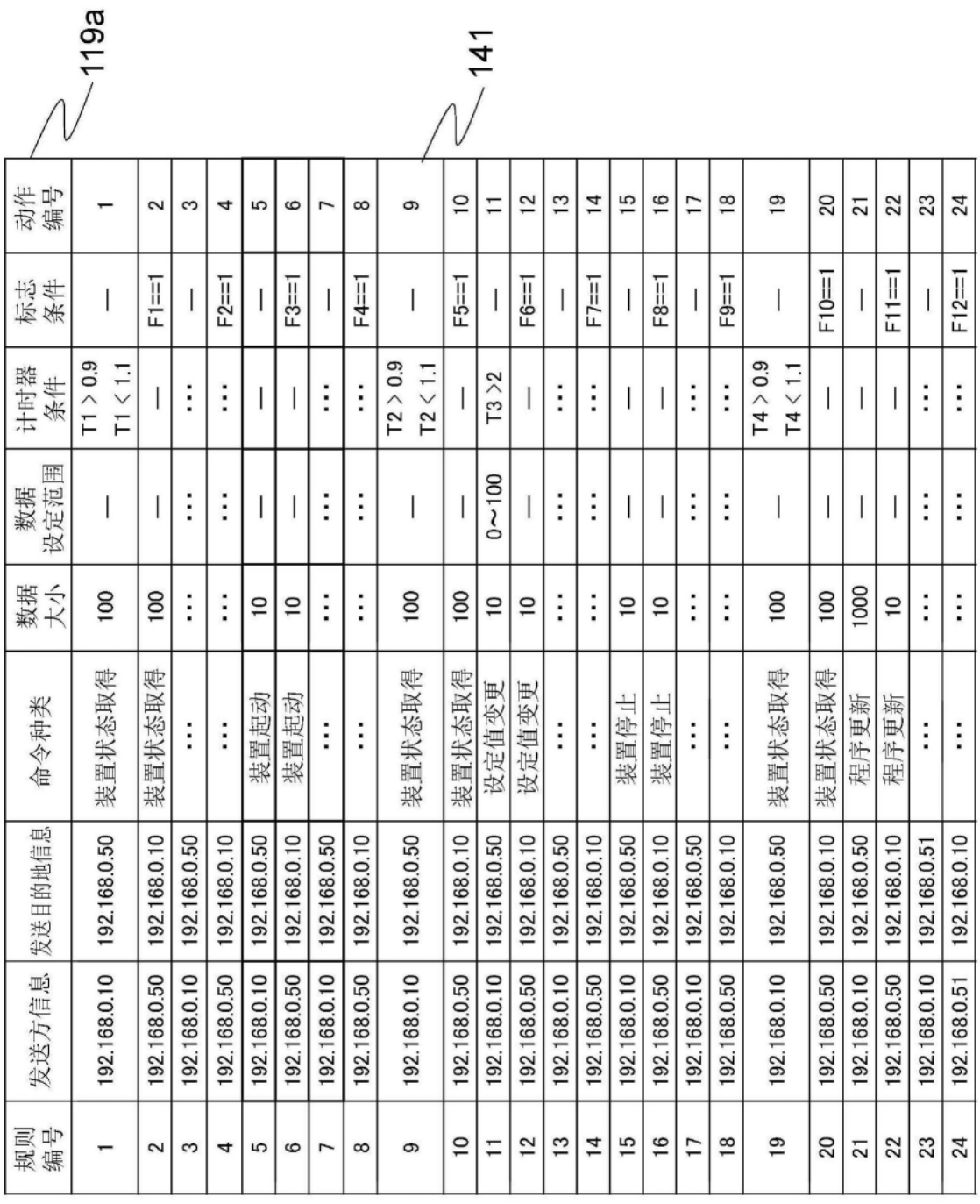

114
状态转变模型
301
停止中
305
维护
306
启动
302
启动
307
试运行
303
控制中
304
关闭
308
关闭
接通电源
维护开始
维护结束
启动开始
关闭结束
启动开始
启动结束
关闭开始
关闭结束
启动开始
启动结束
关闭开始

图3



运用状态	规则编号	接收数据条件							
		发送方信息	发送目的地信息	请求规则编号	响应规则编号	命令种类	数据大小	数据设定范围	周期[秒]
停止中 301	1	192.168.0.10	192.168.0.50		2	装置状态取得	100	—	1±0.1
	2	192.168.0.50	192.168.0.10	1		装置状态取得	100	—	—
	3	192.168.0.10	192.168.0.50		3	…	…	…	…
	4	192.168.0.50	192.168.0.10	4		…	…	…	…
启动 302	5	192.168.0.10	192.168.0.50		6	装置起动	10	—	—
	6	192.168.0.50	192.168.0.10	5		装置起动	10	—	—
	7	192.168.0.10	192.168.0.50		8	…	…	…	…
	8	192.168.0.50	192.168.0.10	7		…	…	…	…
控制中 303	9	192.168.0.10	192.168.0.50		10	装置状态取得	100	—	1±0.1
	10	192.168.0.50	192.168.0.10	9		装置状态取得	100	—	—
	11	192.168.0.10	192.168.0.50		12	设定值变更	10	0~100	2以上
	12	192.168.0.50	192.168.0.10	11		设定值变更	10	—	—
	13	192.168.0.10	192.168.0.50		14	…	…	…	…
	14	192.168.0.50	192.168.0.10	13		…	…	…	…
关闭 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		…	…	…	…
维护 305	19	192.168.0.10	192.168.0.50		20	装置状态取得	100	—	1±0.1
	20	192.168.0.50	192.168.0.10	19		装置状态取得	100	—	—
	21	192.168.0.10	192.168.0.50		22	程序更新	1000	—	—
	22	192.168.0.50	192.168.0.10	21		程序更新	10	—	—
	23	192.168.0.10	192.168.0.51		23	…	…	…	…
	24	192.168.0.51	192.168.0.10	24		…	…	…	…

图4



规则编号	发送方信息	发送目的地信息	命令种类	数据大小	数据设定范围	计时器条件	标志条件	动作编号
1	192.168.0.10	192.168.0.50	装置状态取得	100	—	T1 > 0.9 T1 < 1.1	—	1
2	192.168.0.50	192.168.0.10	装置状态取得	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	装置起动	10	—	—	—	5
6	192.168.0.50	192.168.0.10	装置起动	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	装置状态取得	100	—	T2 > 0.9 T2 < 1.1	—	9
10	192.168.0.50	192.168.0.10	装置状态取得	100	—	—	F5==1	10
11	192.168.0.10	192.168.0.50	设定值变更	10	0~100	T3 >2	—	11
12	192.168.0.50	192.168.0.10	设定值变更	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	装置状态取得	100	—	T4 > 0.9 T4 < 1.1	—	19
20	192.168.0.50	192.168.0.10	装置状态取得	100	—	—	F10==1	20
21	192.168.0.10	192.168.0.50	程序更新	1000	—	—	—	21
22	192.168.0.50	192.168.0.10	程序更新	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

图5

119b

运用状态	规则个数	索引					
		规则编号					
停止中301	4	0	1	2	3		
		1	3	2	4		
启动 302	4	0	1	2	3		
		5	7	6	8		
控制中303	6	0	1	2	3	4	5
		9	11	13	10	12	14
关闭 304	4	0	1	2	3		
		15	17	16	18		
维护305	6	0	1	2	3	4	5
		19	21	23	20	22	24

图6

119c

动作编号	计时器操作	标志操作
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

图7

119d

运用状态	发送方	发送目的地	索引开头编码	检索个数
停止中301	192.168.0.10	192.168.0.50	0	2
	192.168.0.50	192.168.0.10	2	2
启动302	192.168.0.10	192.168.0.50	0	2
	192.168.0.50	192.168.0.10	2	2
控制中303	192.168.0.10	192.168.0.50	0	3
	192.168.0.50	192.168.0.10	3	3
关闭304	192.168.0.10	192.168.0.50	0	2
	192.168.0.50	192.168.0.10	2	2
维护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

图8

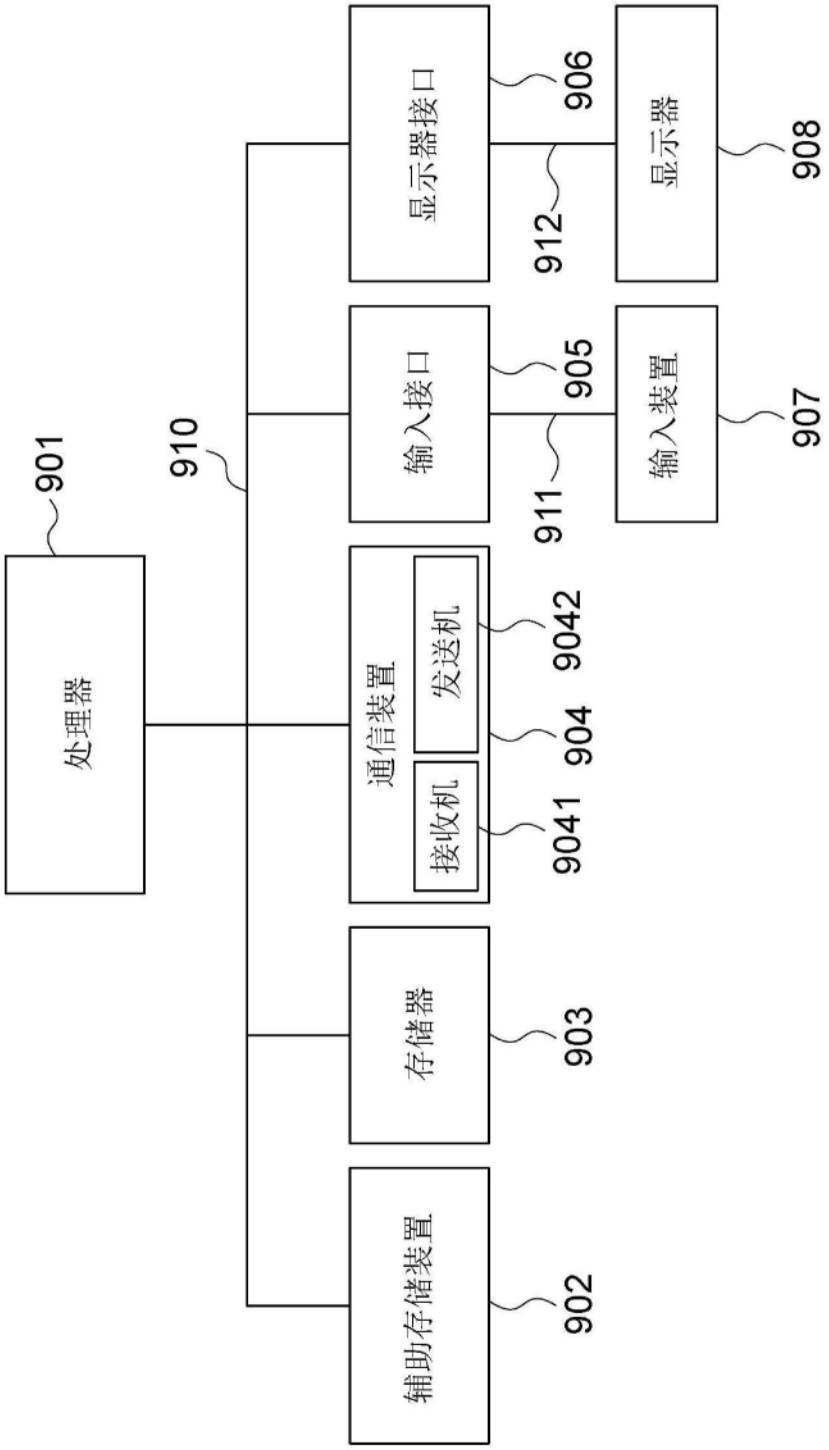

处理器
901
910
辅助存储装置
902
存储器
903
通信装置
接收机
9041
发送机
9042
904
输入接口
905
911
输入装置
907
显示器接口
906
912
显示器
908

图9

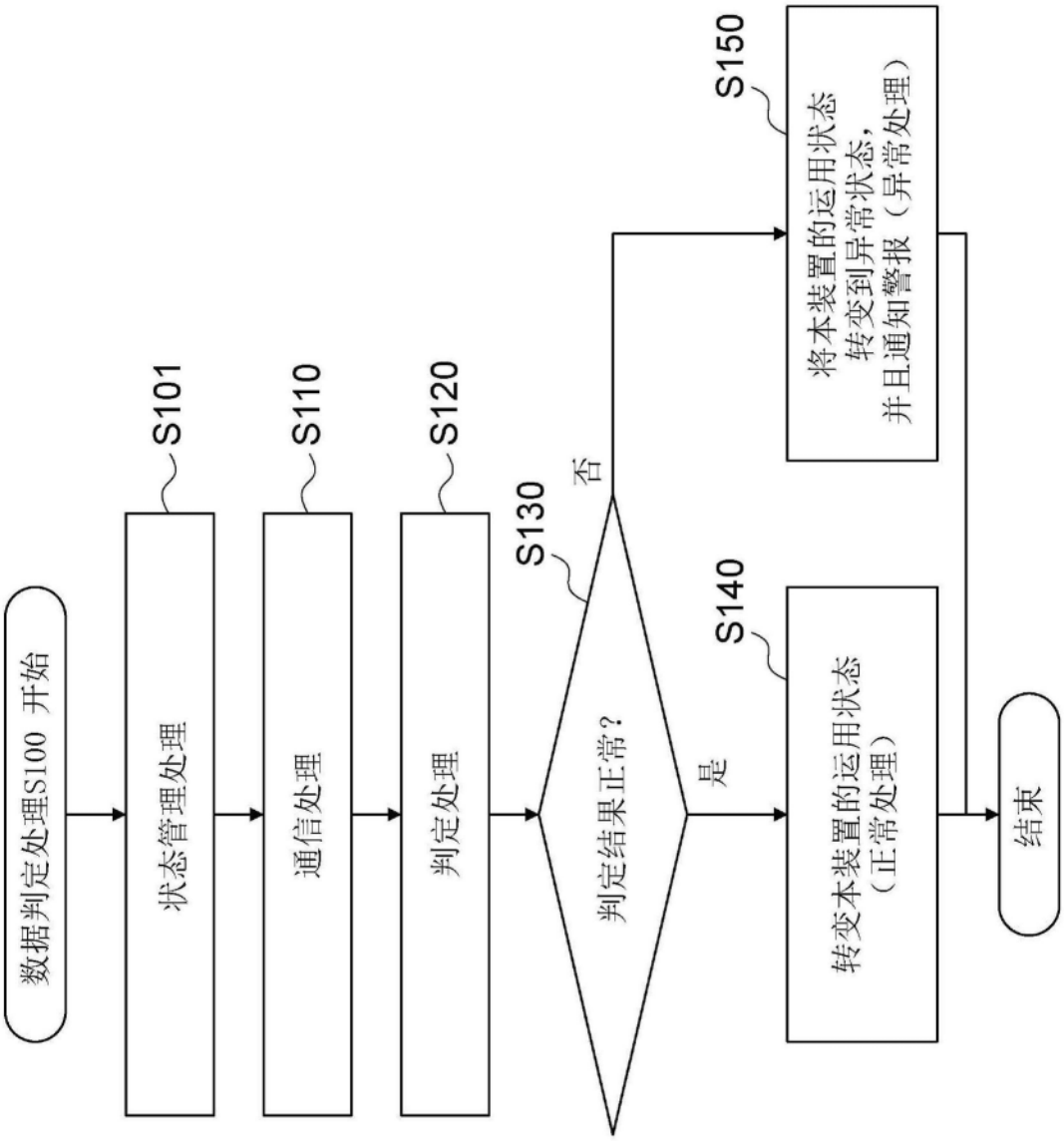

数据判定处理S100 开始
S101
状态管理处理
S110
通信处理
S120
判定处理
S130
判定结果正常？
否
是
S140
转变本装置的运用状态
（正常处理）
S150
将本装置的运用状态
转变到异常状态，
并且通知警报（异常处理）
结束

图10

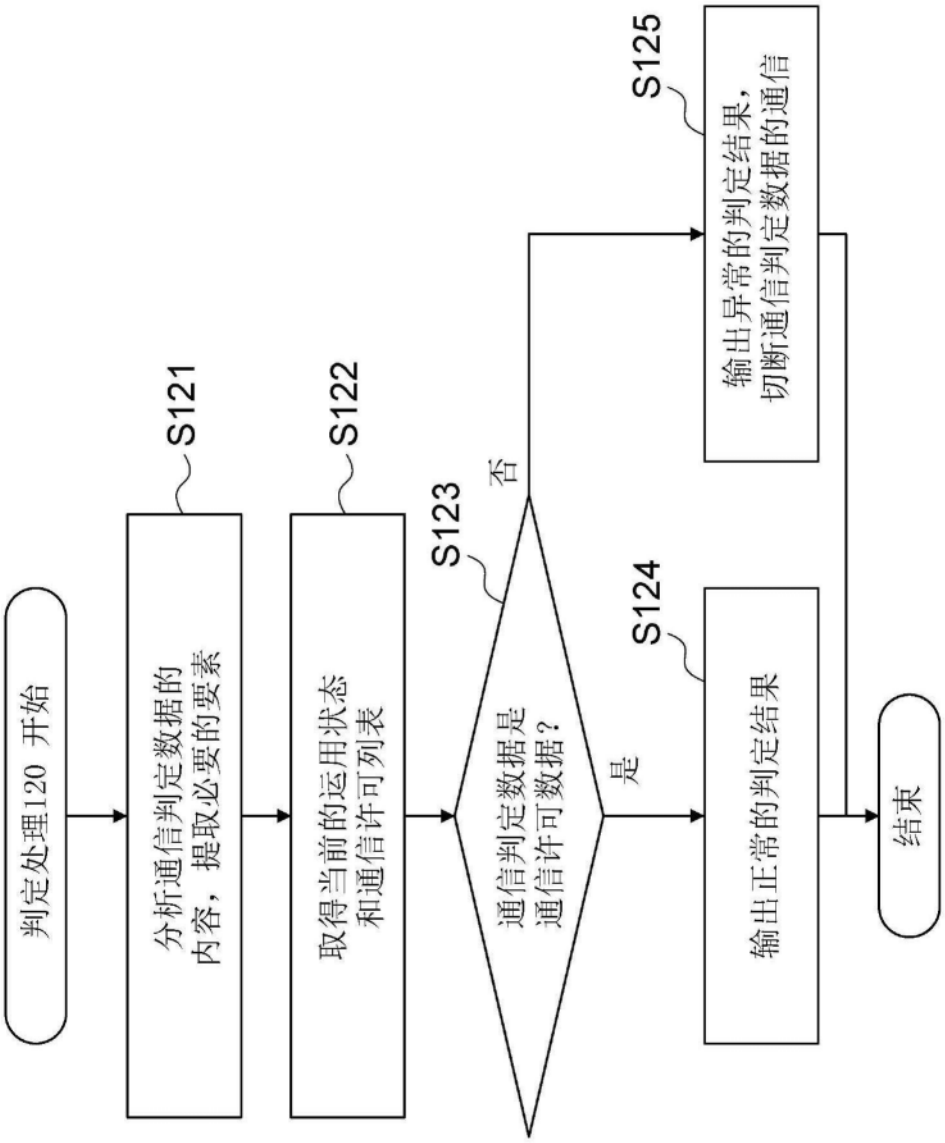

判定处理120 开始
S121
分析通信判定数据的内容，提取必要的要素
S122
取得当前的运用状态和通信许可列表
S123
通信判定数据是通信许可数据？
否
是
S124
输出正常的判定结果
S125
输出异常的判定结果，切断通信判定数据的通信
结束

图11

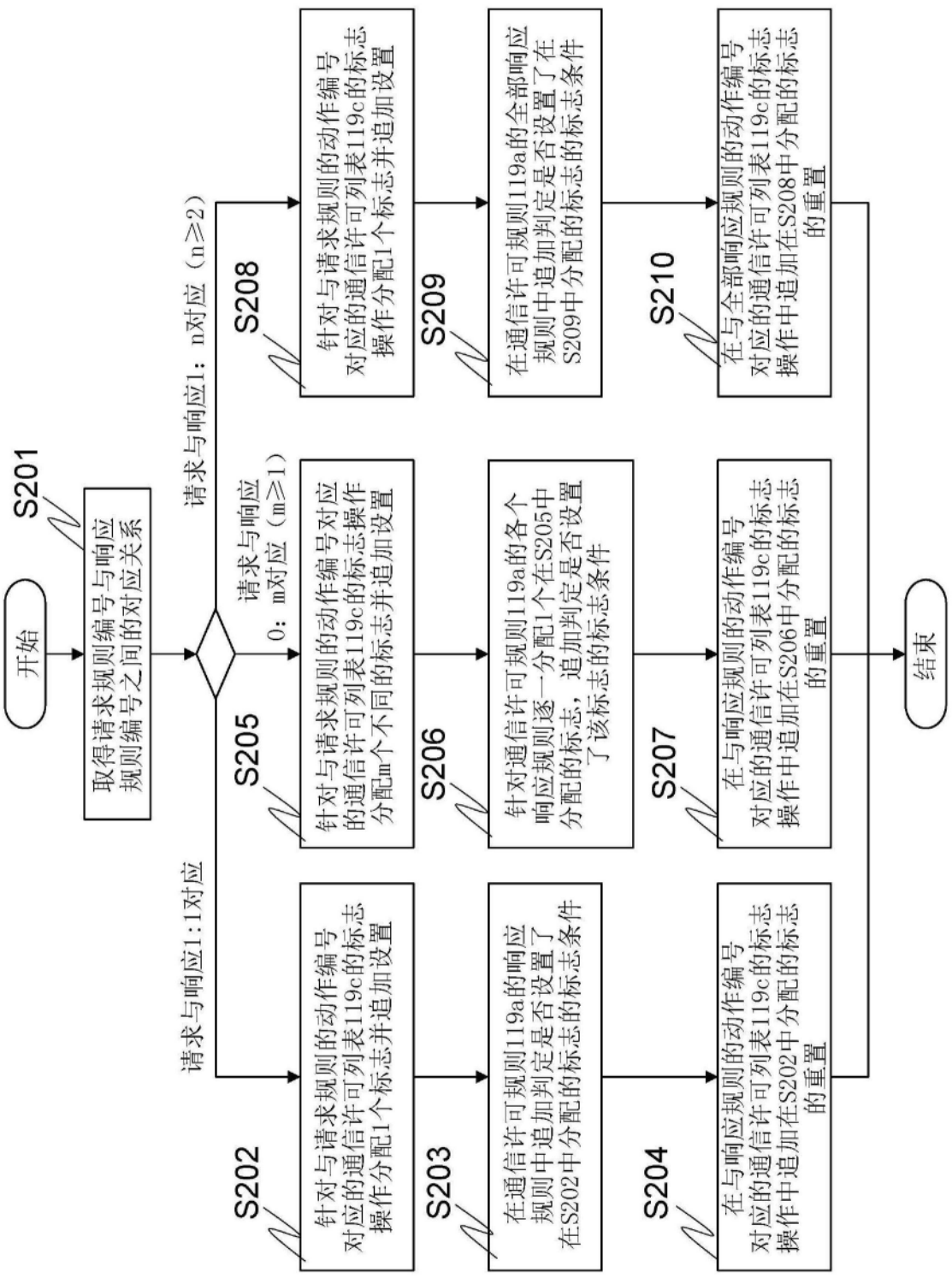

开始
S201
取得请求规则编号与响应规则编号之间的对应关系
请求与响应1：n对应（n≥2）
请求与响应1:1对应
请求与响应0：m对应（m≥1）
S202
针对与请求规则的动作编号对应的通信许可列表119c的标志操作分配1个标志并追加设置
S203
在通信许可规则119a的响应规则中追加判定是否设置了在S202中分配的标志的标志条件
S204
在与响应规则的动作编号对应的通信许可列表119c的标志操作中追加在S202中分配的标志的重置
S205
针对与请求规则的动作编号对应的通信许可列表119c的标志操作分配m个不同的标志并追加设置
S206
针对通信许可规则119a的各个响应规则逐一分配1个在S205中分配的标志，追加判定是否设置了该标志的标志条件
S207
在与响应规则的动作编号对应的通信许可列表119c的标志操作中追加在S206中分配的标志的重置
S208
针对与请求规则的动作编号对应的通信许可列表119c的标志操作分配1个标志并追加设置
S209
在通信许可规则119a的全部响应规则中追加判定是否设置了在S209中分配的标志的标志条件
S210
在与全部响应规则的动作编号对应的通信许可列表119c的标志操作中追加在S208中分配的标志的重置
结束

图12

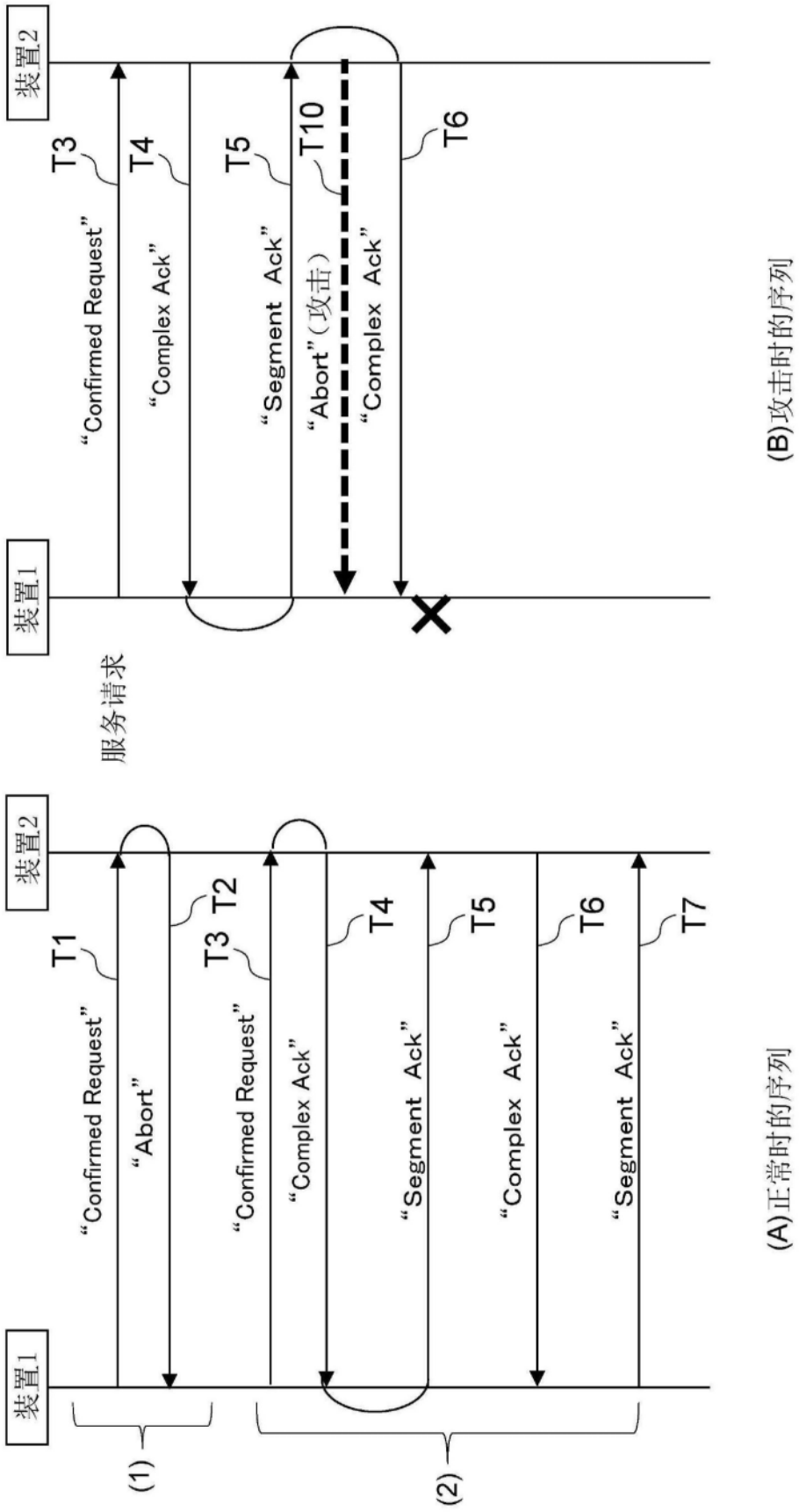

装置2
装置1
T3
T4
T5
T10
T6
“Confirmed Request”
“Complex Ack”
“Segment Ack”
“Abort”（攻击）
“Complex Ack”
服务请求
(B)攻击时的序列
装置2
装置1
T1
T2
T3
T4
T5
T6
T7
“Confirmed Request”
“Abort”
“Confirmed Request”
“Complex Ack”
“Segment Ack”
“Complex Ack”
“Segment Ack”
(1)
(2)
(A)正常时的序列

图13