



(12)发明专利申请

(10)申请公布号 CN 106104497 A

(43)申请公布日 2016.11.09

(21)申请号 201580015248.8

小林佑嗣 矾山和彦

(22)申请日 2015.03.18

(74)专利代理机构 北京林达刘知识产权代理事务
所(普通合伙) 11277

(30)优先权数据

2014-058497 2014.03.20 JP

代理人 刘新宇

PCT/JP2014/003007 2014.06.05 JP

(51)Int.Cl.

(85)PCT国际申请进入国家阶段日

G06F 11/34(2006.01)

2016.09.20

(86)PCT国际申请的申请数据

PCT/JP2015/001500 2015.03.18

(87)PCT国际申请的公布数据

W02015/141221 JA 2015.09.24

(71)申请人 日本电气株式会社

地址 日本东京都

(72)发明人 野村崇志 喜田弘司 上村纯平

荣纯明 胜田悦子 山崎健太郎

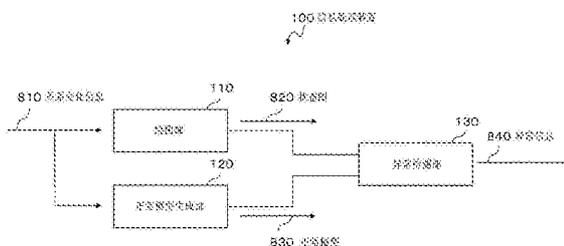
权利要求书2页 说明书14页 附图16页

(54)发明名称

信息处理装置和异常检测方法

(57)摘要

本发明提供一种提高系统异常的检测能力的信息处理装置。该信息处理装置包括：用于基于表示系统中所包括的多个要素之间的关系的变化的关系变化信息来生成状态图的部件，所述状态图包括所述要素作为所述状态图的顶点并且包括所述要素之间的关系作为所述状态图的边；用于基于所述关系变化信息来生成正常模型的部件，其中所述正常模型是所述系统的正常操作期间所述状态图所满足的条件的集合；以及用于基于所述状态图和所述正常模型来检测系统异常并且输出表示所检测到的异常的异常信息的部件。



1. 一种信息处理装置,包括:

绘图部,用于基于时间序列来获得表示系统中所包括的多个要素之间的关系的变化的关系变化信息,并且基于所述关系变化信息来生成状态图,其中所述状态图包括所述要素作为所述状态图的顶点并且包括所述要素之间的关系作为所述状态图的边;

正常模型生成部,用于基于所述关系变化信息来生成正常模型,其中所述正常模型是所述系统的正常操作期间所述状态图所满足的条件集合;以及

异常检测部,用于基于所述状态图和所述正常模型来检测与所述系统相关联的异常,并且输出表示所检测到的所述异常的第一异常信息。

2. 根据权利要求1所述的信息处理装置,其中,

所述系统包括经由网络彼此连接的多个主机,以及

所述主机上所运行的进程由所述顶点来定义。

3. 根据权利要求1或2所述的信息处理装置,其中,所述异常检测部计算与所检测到的所述异常相对应的表示所述状态图相对于所述正常模型的偏差程度的异常度,并且输出至少包括所计算出的所述异常度的所述第一异常信息。

4. 根据权利要求1~3中任一项所述的信息处理装置,其中,所述异常检测部输出至少包括与所检测到的所述异常相对应的用于识别所述要素的信息和与所述要素之间的关系有关的信息的所述第一异常信息。

5. 根据权利要求1~4中任一项所述的信息处理装置,其中,所述异常检测部输出基于所述状态图和所述第一异常信息所生成的包括用于表示异常的图表的第二异常信息。

6. 根据权利要求5所述的信息处理装置,其中,所述异常检测部在所述要素之间的所有关系中提取通过与所述正常模型进行对照而被视为正常的所述要素之间的关系,并且与所提取的所述要素之间的关系重叠地输出用于表示异常的图表。

7. 根据权利要求5或6所述的信息处理装置,其中,所述异常检测部独立地或彼此相关联地输出表示所述状态图、所述正常模型和所述第二异常信息各自的时间变化的显示信息。

8. 根据权利要求1~7中任一项所述的信息处理装置,其中,还包括:

历史累积部,用于存储状态图,

其中,所述绘图部将所述状态图记录在所述历史累积部中,以及

所述异常检测部进一步基于所述正常模型和所述历史累积部中所记录的历史状态图来检测与所述系统相关联的异常。

9. 根据权利要求1~8中任一项所述的信息处理装置,其中,所述关系变化信息包括表示所述要素之间的关系的的发生、消失和变化以及要素的的发生和消失中的至少一个的信息。

10. 根据权利要求1~9中任一项所述的信息处理装置,其中,所述正常模型中的所述条件包括以下内容中的至少一个的范围:所述顶点中的任一顶点的属性、与所述顶点中的任一顶点邻接的顶点的数量、与所述顶点中的任一顶点邻接的顶点的属性、所述边的属性、所述顶点之间的路线的有无、所述顶点之间的路线的数量、所述路线的距离、所述路线中的所述顶点的属性、所述路线中的所述边的属性、以及状态图的特性。

11. 一种信息处理系统,包括:

根据权利要求1~10中任一项所述的信息处理装置;以及

关系变化监视部,用于监视所述系统并发送关系变化信息。

12.一种异常检测方法,包括以下步骤:

基于时间序列来获得表示系统中所包括的多个要素之间的关系的变化的关系变化信息,并且基于所述关系变化信息来生成状态图,其中所述状态图包括所述要素作为所述状态图的顶点并且包括所述要素之间的关系作为所述状态图的边;

基于所述关系变化信息来生成正常模型,其中所述正常模型是所述系统的正常操作期间所述状态图所满足的条件的集合;

基于所述状态图和所述正常模型来检测与所述系统相关联的异常;以及

输出表示所检测到的所述异常的异常信息。

13.一种用于记录程序的非瞬态计算机可读记录介质,所述程序用于使计算机执行以下处理:

基于时间序列来获得表示系统中所包括的多个要素之间的关系的变化的关系变化信息,并且基于所述关系变化信息来生成状态图,其中所述状态图包括所述要素作为所述状态图的顶点并且包括所述要素之间的关系作为所述状态图的边;

基于所述关系变化信息来生成正常模型,其中所述正常模型是所述系统的正常操作期间所述状态图所满足的条件的集合;

基于所述状态图和所述正常模型来检测与所述系统相关联的异常;以及

输出表示所检测到的所述异常的异常信息。

信息处理装置和异常检测方法

技术领域

[0001] 本发明涉及用于检测系统异常的技术。

背景技术

[0002] 已知有用以检测系统异常的各种现有技术。

[0003] 例如,专利文献1公开了进程监视装置。专利文献1中所公开的该进程监视装置按以下方式进行工作。

[0004] 首先,进程监视装置基于进程的静态属性来提取需要注意进程。静态属性的示例包括进程名称、用于实现进程的程序的制造商名称、程序(软件)名称、版本、启动进程的父进程的名称、以及进程大小。进程监视装置在当前静态属性与过去的静态属性不同的情况下提取相关进程作为需要注意进程。进程监视装置在过去的静态属性不可用的情况下提取相关进程作为需要注意进程。进程监视装置在父进程不可识别的情况下提取相关进程作为需要注意进程。进程监视装置在外部进程用作父进程的情况下提取相关进程作为需要注意进程。

[0005] 其次,进程监视装置基于动态属性来针对需要注意进程发出警报。动态属性的示例包括动态专用存储器字节数、动态共享存储器字节数、重定向器发送、接收流量速率和硬盘访问速率。在可以通过使用任何统计方法来区分过去的动态属性和当前动态属性的情况下,进程监视装置例如针对相关的需要注意进程生成警告或者将相关的需要注意进程登记为要监视的进程。

[0006] 再次,进程监视装置提取与需要注意进程具有预定相关性的关联进程并且将该关联进程确定为要监视的进程。具有预定相关性的进程的示例包括具有明确父子关系的进程、以及尽管不具有明确父子关系但在要监视的进程进行工作的情况下始终启动的进程。

[0007] 专利文献2公开了与安全应用程序中的云计算的使用相关联的技术。专利文献2中所公开的系统按以下方式进行工作。

[0008] 首先,系统监视客户端的流量。

[0009] 其次,系统将所监视到的流量与同客户端的工作模式相对应的预测流量模式进行比较。

[0010] 再次,系统基于比较结果来判断是否发现了安全威胁。

[0011] 现有技术文献

[0012] 专利文献

[0013] 专利文献1:日本特开2008-021274

[0014] 专利文献2:日本特表2012-523159

发明内容

[0015] 发明要解决的问题

[0016] 然而,在上述的现有技术文献所公开的技术中,仅检测个别的要素单位的异常或

者由于预定义的攻击模式所引起的异常。换句话说,例如难以检测由于针对计算机系统的未知目标类型的攻击而引起的异常。

[0017] 这是因为,专利文献1中所公开的技术仅用于基于个别进程的预定义的静态和动态属性来检测异常。专利文献1中所公开的技术在相关进程提取方面仅考虑到父子关系和启动之间的同步性。

[0018] 专利文献2中所公开的技术仅用于基于预测流量模式来检测客户端的流量的异常。

[0019] 本发明的目的是提供用以解决上述问题的信息处理装置、监视方法及其程序或用于记录程序的非瞬态计算机可读记录介质。

[0020] 用于解决问题的方案

[0021] 根据本发明的一方面的信息处理装置,包括:绘图部,用于基于时间序列来获得表示系统中所包括的多个要素之间的关系的变化的关系变化信息,并且基于所述关系变化信息来生成状态图,其中所述状态图包括所述要素作为所述状态图的顶点并且包括所述要素之间的关系作为所述状态图的边;正常模型生成部,用于基于所述关系变化信息来生成正常模型,其中所述正常模型是所述系统的正常操作期间所述状态图所满足的条件的集合;以及异常检测部,用于基于所述状态图和所述正常模型来检测与所述系统相关联的异常,并且输出表示所检测到的所述异常的第一异常信息。

[0022] 根据本发明的一方面的异常检测方法,包括以下步骤:基于时间序列来获得表示系统中所包括的多个要素之间的关系的变化的关系变化信息,并且基于所述关系变化信息来生成状态图,其中所述状态图包括所述要素作为所述状态图的顶点并且包括所述要素之间的关系作为所述状态图的边;基于所述关系变化信息来生成正常模型,其中所述正常模型是所述系统的正常操作期间所述状态图所满足的条件的集合;基于所述状态图和所述正常模型来检测与所述系统相关联的异常;以及输出表示所检测到的所述异常的异常信息。

[0023] 根据本发明的一方面的非瞬态计算机可读记录介质记录用于使计算机执行以下处理的程序:基于时间序列来获得表示系统中所包括的多个要素之间的关系的变化的关系变化信息,并且基于所述关系变化信息来生成状态图,其中所述状态图包括所述要素作为所述状态图的顶点并且包括所述要素之间的关系作为所述状态图的边;基于所述关系变化信息来生成正常模型,其中所述正常模型是所述系统的正常操作期间所述状态图所满足的条件的集合;基于所述状态图和所述正常模型来检测与所述系统相关联的异常;以及输出表示所检测到的所述异常的异常信息。

[0024] 发明的效果

[0025] 本发明可以提高系统异常的检测能力。

附图说明

[0026] 图1是示出根据本发明的第一实施例的信息处理装置的结构框图。

[0027] 图2是示出根据第一实施例的包括信息处理装置和要监视的系统的信息处理系统的结构的框图。

[0028] 图3是示出第一实施例中的示例性关系变化信息的图。

[0029] 图4是示出第一实施例中的示例性状态图的图。

- [0030] 图5是示出第一实施例中的状态图所表示的要素之间的关系的概念图。
- [0031] 图6是示出第一实施例中的示例性正常模型的图。
- [0032] 图7是示出第一实施例中的示例性异常信息的图。
- [0033] 图8是示出实现根据第一实施例的信息处理装置的计算机的硬件结构的框图。
- [0034] 图9是示出第一实施例中的信息处理装置的操作的流程图。
- [0035] 图10是示出第一实施例中的信息处理装置的操作的流程图。
- [0036] 图11是示出第一实施例中的示例性关系变化信息的图。
- [0037] 图12是示出第一实施例中的另一示例性状态图的图。
- [0038] 图13是示出根据本发明的第二实施例的信息处理装置的结构框图。
- [0039] 图14是示出第二实施例中的示例性异常信息的图。
- [0040] 图15是示出根据本发明的第三实施例的信息处理装置的结构框图。
- [0041] 图16是示出第三实施例中的示例性异常信息的图。
- [0042] 图17是示出根据本发明的第四实施例的信息处理装置的结构框图。
- [0043] 图18是示出第四实施例中的示例性异常信息的图。
- [0044] 图19是示出第四实施例中的另一示例性异常信息的图。
- [0045] 图20是示出根据本发明的第五实施例的信息处理装置的结构框图。

具体实施方式

[0046] 以下将参考附图来详细说明本发明的实施例。在本说明书所述的各附图和各实施例中,相同的附图标记表示相同的构成要素,并且将适当地省略对相同的构成要素的说明。

[0047] 第一实施例

[0048] 图1是示出根据本发明的第一实施例的信息处理装置100的结构框图。

[0049] 如图1所示,根据本实施例的信息处理装置100包括绘图部110、正常模型生成部120和异常检测部130。可以针对硬件单位的电路或计算机装置的功能单位来划分图1所示的构成要素。这里假定要针对计算机装置的功能单位来划分图1所示的构成要素。

[0050] 图2是示出包括信息处理装置100、要监视的系统(以下还简称为“系统”)900和关系变化监视部件930的信息处理系统的结构框图。

[0051] 要监视的系统900

[0052] 要监视的系统900包括多个要素920。各要素920具有与其它各要素920的特定关系。

[0053] 例如,要监视的系统900是包括经由网络彼此连接的多个主机(未示出)并且在这些主机上启动进程(未示出)的信息处理系统。

[0054] 要监视的系统900可以是社交网络。

[0055] 要监视的系统900可以是具有特定构造的数据项(要素920)的集合。具有特定构造的数据项的集合的示例包括具有超文本链接和超文本链接对象之间的关系的文件的集合。

[0056] 要监视的系统900可以是与上述的示例无关的任何系统。

[0057] 关系变化监视部件930

[0058] 关系变化监视部件930监视要监视的系统900中所包括的要素920之间的关系的變化。关系变化监视部件930将所检测到的关系的變化作为关系变化信息810发送至信息处理

装置100。关系变化监视部件930可以包括在要监视的系统900中。

[0059] 在要监视的系统900是信息处理系统的情况下,关系变化监视部件930例如可以是主机上所运行的代理。例如,代理监视主机上的启动的进程的行为并且将进程事件日志发送至信息处理装置100。

[0060] 在要监视的系统900是社交网络的情况下,关系变化监视部件930可以例如用作邮件服务器上所运行的邮件监视代理。这里,社交网络是指SNS(Social Networking Service,社交网络服务)所构建的网络。例如,邮件监视代理监视用户之间所交换的邮件消息,并且将邮件发送和接收日志发送至信息处理装置100。可选地,关系变化监视部件930可以是SNS服务器上所运行的代理。该代理例如监视SNS中的好友请求信息(消息信息)以及好友之间的联系(用户连接信息/联系数量的增加)及其变化。

[0061] 在要监视的系统900是网页的集合的情况下,关系变化监视部件930例如可以是web服务器上所运行的代理。例如,该代理监视网页的创建和删除以及网页之间的超文本链接关系的变化,并且将表示这些变化的详情的的事件日志发送至信息处理装置100。

[0062] 关系变化监视部件930可以与上述的示例无关地监视任意系统中的任意要素920之间的关系的变化,并且将任意关系变化信息810发送至信息处理装置100。

[0063] 信息处理装置100和关系变化监视部件930经由网络(未示出)彼此连接。用于监视相同或不同的要监视的系统900的多个关系变化监视部件930可以连接至信息处理装置100而不同于图2所示的示例。

[0064] 信息处理装置100的绘图部110

[0065] 绘图部110基于时间序列例如从关系变化监视部件930获取要监视的系统900的关系变化信息810。绘图部110基于所获得的关系变化信息810生成状态图820,并且将状态图820输出至异常检测部130。

[0066] 关系变化信息810

[0067] 关系变化信息810是表示要监视的系统900中所包括的要素920之间的关系的变化信息。更具体地,关系变化信息810如上所述包括从各种关系变化监视部件930发送来的信息。

[0068] 图3是示出作为关系变化信息810的具体示例的示例性关系变化信息811的图。图3所示的关系变化信息811表示“要素920“E2”和要素920“E3”之间发生了类型为“L2”的关系”的事件。注意,“E2”和“E3”是要素920的标识符。例如,要素920“E2”表示要素920具有标识符“E2”。此外,“L2”是要素920之间的关系的类型的标识符。例如,类型“L2”表示要素920之间的关系的类型具有标识符“L2”。

[0069] 状态图820

[0070] 状态图820具有各要素920作为该状态图820的顶点(也称为节或节点),并且具有要素920之间的关系作为该状态图820的边(也称为链、边或分支)。状态图820表示要监视的系统900中的要素920之间的关系。这里,该关系的示例包括“在特定时间段期间在要素之间传输数据”的数据传输关系以及“可以在特定时刻(或者在特定时间段期间)在要素之间发生数据传输”的数据传输关系。

[0071] 图4是示出作为状态图820的具体示例的状态图821的图。如图4所示,状态图821由包括顶点标识符和边的记录所定义。顶点标识符是形成顶点的要素920的标识符。边是表示

各顶点标识符所指定的顶点(要素920)和其它顶点(要素920)之间的关系的信息。

[0072] 例如,顶点标识符“E1”指定标识符为“E1”的要素920。与顶点标识符“E1”相对应的边“E2;L0,E3;L1;L1”表示以下信息。首先,要素920“E1”具有以要素920“E2”形成且具有属性“L0”的边。其次,要素920“E1”具有以要素920“E3”形成且均具有属性“L1”的两个边。

[0073] 例如,在顶点标识符为“E4”的记录中,边(Side)栏是空白的,这表示要素920“E4”不具有以任何其余的要素920形成的边。

[0074] 边例如表示具有该边的要素920已完成针对通信的准备。边的属性例如表示该边上所进行的通信的协议的类型。例如可以以表示要素920之间的关系而限于上述的示例的任何形式来定义边和边的属性(例如,类型)。

[0075] 例如,基于图3所示的关系变化信息811来定义顶点标识符为“E2”的记录中的边“E3;L2”和顶点标识符为“E3”的记录中的边“E2;L2”。

[0076] 状态图820可以采用任何形式而限于上述的示例。

[0077] 状态图820所表示的要素920之间的关系

[0078] 图5是示出状态图821所表示的要素920之间的关系的概念图。

[0079] 参考图5,以圆圈来表示顶点并且在圆圈内标记顶点标识符。通过使圆圈彼此连接的线段来表示边。例如,实线段表示类型为“L0”的边。交替的一长一短的虚线所表示的线段表示类型为“L1”的边。交替的一长两短的虚线所表示的线段表示类型为“L2”的边。箭头表示从关系生成边起的向外方向。

[0080] 信息处理装置100的正常模型生成部120

[0081] 正常模型生成部120基于关系变化信息810生成正常模型830,并且将正常模型830输出至异常检测部130。正常模型830是要监视的系统900的正常操作期间状态图820所满足的条件的集合。

[0082] 正常模型830

[0083] 图6是示出作为正常模型830的具体示例的示例性正常模型831的图。如图6所示,通过包括条件类型、条件值和有效标志的记录来定义正常模型831。

[0084] 例如,条件类型为“关系顶点数”的记录中的条件值“上限值2”表示“具有以一个顶点(要素920)形成的边的要素920的数量为两个以下”的条件。条件类型为“次数”的记录中的条件值“上限值6”表示“从一个顶点起延伸的边的数量为六个以下”的条件。条件类型为“边属性”的记录表示针对边的属性(例如,关系的类型、频率、关系的上下级方向或关系发生的时间等)的条件。有效标志表示记录中所包括的条件值是否有效。有效标志的初始值是“无效”。

[0085] 正常模型生成部120例如可以将如下值设置为针对条件类型为“关系顶点数”的记录的条件值,其中该值是通过将预定值与预定时间段期间针对所有顶点中的各顶点的“关系顶点数”的平均值相加所获得的。预定时间段例如被定义为从特定的过去时刻起直到当前时刻为止的时间段(以下被称为时间段Pa)。预定时间段还可以是由当前时刻之前的特定持续时间所定义的时间段(以下被称为时间段Pb)。预定时间段甚至可以是特定的第一过去时刻起直到特定的第二过去时刻为止的时间段(以下被称为时间段Pc)。预定时间段甚至可以是获得预定数量的关系变化信息810所花费的时间段。换句话说,预定时间段可以是相对于当前时刻或特定的过去时刻而言最近的、并且获得预定数量的关系变化信息810所经

历的时间段(以下被称为时间段Pd(相对于当前时刻)或时间段Pe(相对于过去时刻))。预定时间段甚至可以是时间段Pa、Pb、Pc或Pd期间的预定间歇时间段。如上所述,正常模型生成部120可以基于诸如过去的固定时间段(时间段Pc和Pe)或顺次变化的时间段(时间段Pa、Pb和Pd)等的任意时间段期间的关系变化信息810来生成正常模型830。在正常模型生成部120基于顺次变化的时间段期间的关系变化信息810生成正常模型830的情况下,根据关系变化信息810的顺次输入来顺次更新正常模型830。

[0086] 正常模型生成部120可以基于关系变化信息810使用任何技术来计算任意条件类型的条件值,而限于上述示例。

[0087] 例如在基于预定数量的关系变化信息810来生成或更新条件值的情况下,正常模型生成部120将有效标志设置为“有效”。在基于预定时间段期间的关系变化信息810来生成或更新条件值的情况下,正常模型生成部120也可以将有效标志设置为“有效”。

[0088] 正常模型830可以与上述示例无关地包括表示以下条件类型的记录。

[0089] 正常模型830可以包括表示针对顶点的属性(例如,要素920的类型或顶点的发生时刻等)的条件的记录。

[0090] 正常模型830可以包括表示针对邻接顶点的属性的条件的记录。

[0091] 正常模型830可以包括表示针对以下内容的任意条件的记录:顶点之间的路径的有无、数量和距离、路线中的顶点和边的属性等。

[0092] 正常模型830甚至可以包括表示针对图特性(例如,直径、中心性或子构造等)的条件的记录。

[0093] 信息处理装置100的异常检测部130

[0094] 异常检测部130基于状态图820和正常模型830检测与要监视的系统900相关联的异常,并且输出表示所检测到的异常的异常信息840。

[0095] 异常信息840例如表示已检测到要监视的系统900的任何异常。异常信息840还可以包括与异常相关联的任意信息。

[0096] 异常检测部130可以在任意时刻输出异常信息840。例如,异常检测部130在检测到异常时输出表示该异常的异常信息840。异常检测部130还可以保持所检测到的异常,并且响应于请求(预定时刻或管理者的指示)而输出表示所保持的异常的异常信息840。异常检测部130甚至可以请求中所包括的时刻(时间范围)相对应地针对状态图820检测异常。

[0097] 图7是示出作为异常信息840的具体示例的示例性异常信息841的图。如图7所示,异常信息841表示关系顶点数已超过关系顶点数的上限值。

[0098] 以上已经说明了信息处理装置100的功能单位的构成要素。

[0099] 接着,以下将说明信息处理装置100的硬件单位的构成要素。

[0100] 图8是示出实现根据本实施例的信息处理装置100的计算机700的硬件结构的图。

[0101] 如图8所示,计算机700包括CPU(中央处理单元)701、存储部702、存储装置703、输入部704、输出部705和通信部706。计算机700还包括从外部供给的记录介质(或存储介质)707。例如,记录介质707是非瞬态地存储信息的非易失性记录介质(非瞬态记录介质)。记录介质707可以是将信息作为信号来保持的瞬态记录介质。

[0102] CPU 701运行操作系统(未示出)以控制计算机700整体的操作。例如,CPU 701从存储装置703中所安装的记录介质707读取程序或数据,并且将所读取的程序或数据写入存储

部702。该程序的示例包括用于使计算机700执行(后面要说明的)图9和10所示的流程图中的操作的程序。

[0103] CPU 701根据所读取的程序和所读取的数据来执行各种类型的处理作为图1所示的绘图部110、正常模型生成部120和异常检测部130。

[0104] CPU 701可以从连接至通信网络(未示出)的外部计算机(未示出)将程序或数据下载至存储部702。

[0105] 存储部702存储程序和数据。存储部702例如可以存储关系变化信息810、状态图820、正常模型830和异常信息840。

[0106] 存储装置703例如以任意的光盘、软盘、磁光盘、外部硬盘或半导体存储器中的任一类型来实现,并且包括记录介质707。存储装置703(记录介质707)以计算机可读的方式来存储程序。存储装置703还可以存储数据。存储装置703例如可以存储关系变化信息810、状态图820、正常模型830和异常信息840。

[0107] 输入部704接收操作员的操作输入和外部信息输入。输入操作所使用的装置的示例包括任意的鼠标、键盘、内部键钮和触摸面板中的任一类型。

[0108] 输出部705例如以显示器来实现。输出部705例如用于经由GUI(图形用户界面)向操作员的输入请求和向操作员的输出呈现。

[0109] 通信部706实现与关系变化监视部件930的接口。通信部706可以被包括作为绘图部110、正常模型生成部120和异常检测部130的一部分。

[0110] 如上所述,图1所示的信息处理装置100的功能单位的块是通过具有图8所示的硬件结构的计算机700来实现的。然而,注意,用于实现计算机700的各部的部件不限于上述说明。换句话说,可以以单个物理上结合的装置或者以有线或无线的方式相连接的两个以上物理上分离的装置来实现计算机700。

[0111] 在将用于记录上述程序的代码的记录介质707供给至计算机700的情况下,CPU 701可以读取并执行记录介质707中所存储的程序代码。可选地,CPU 701可以将记录介质707中所存储的程序代码存储在存储部702和/或存储装置703中。换句话说,本实施例包括瞬态或非瞬态地存储由计算机700(CPU 701)所执行的程序(软件)的记录介质707的实施例。非瞬态地存储信息的存储介质还被称为非易失性存储介质。

[0112] 以上已经说明了实现本实施例中的信息处理装置100的计算机700的硬件单位的各构成要素。

[0113] 以下将参考附图来详细说明本实施例中的操作。

[0114] 图9和10是示出本实施例中的操作的流程图。可以基于上述的CPU 701所进行的程序控制来执行基于流程图的处理。处理步骤由诸如S610等的附图标记来表示。

[0115] 绘图部110在接收到关系变化信息810时根据图9所示的流程图来开始操作。绘图部110例如经由图8所示的通信部706从要监视的系统900接收关系变化信息810。

[0116] 绘图部110基于所接收到的关系变化信息810生成状态图820(新生成状态图820或者通过更新来生成状态图820)(步骤S601)。绘图部110将状态图820保持在例如图8所示的存储部702或存储装置703中。

[0117] 正常模型生成部120基于所接收到的关系变化信息810来生成正常模型830的内容(新生成正常模型830的内容或者通过更新来生成正常模型830的内容)(步骤S602)。换句话

说,首先,正常模型生成部120生成或更新包括与所接收到的关系变化信息810相关联的条件类型的记录的条件值。该记录是正常模型830的记录。其次,正常模型生成部120在针对该记录满足预定条件(例如,条件值的给定更新次数)的情况下将该记录中的有效标志的设置改变为“有效”。正常模型生成部120将正常模型830保持在例如图8所示的存储部702或存储装置703中。

[0118] 异常检测部130基于状态图820和正常模型830来进行与要监视的系统900相关联的异常的检测处理(步骤S603)。然后,处理结束。

[0119] 在图9所示的流程图中,绘图部110、正常模型生成部120和异常检测部130按该顺序串行工作。然而,绘图部110、正常模型生成部120和异常检测部130可以并行工作。

[0120] 在图9的流程图中所示的操作中,每当正常模型生成部120更新正常模型830的内容时,异常检测部130进行异常检测处理。然而,异常检测部130可以在任意时间(例如,在特定时刻或者在从管理者接收到指示的情况下)进行异常检测处理。

[0121] 在图9的流程图中所示的操作中,绘图部110和正常模型生成部120每次接收到关系变化信息810时分别更新状态图820和正常模型830。然而,绘图部110和正常模型生成部120可以累积所接收到的关系变化信息810并且在特定时间基于所累积的关系变化信息810分别生成或更新状态图810和正常模型830。该特定时间例如可以是紧挨在异常检测部130生成异常信息840之前。

[0122] 在图9的步骤S603中,异常检测部130按照图10所示的流程图中进行以下操作。

[0123] 异常检测部130针对正常模型830的所有记录执行步骤S630~S638之间的处理。

[0124] 异常检测部130从正常模型830获得记录(步骤S631)。

[0125] 异常检测部130基于有效标志来判断该记录是否有效(步骤S632)。如果有效标志为“无效”(步骤S632为否),则处理进入步骤S638。

[0126] 如果有效标志为“有效”(步骤S632为是),则异常检测部130针对可从状态图820提取的要确认的所有值执行步骤S633~S637之间的处理。

[0127] 异常检测部130从状态图820提取与该记录中所包括的条件类型相对应的要确认的值(步骤S634)。

[0128] 异常检测部130判断该要确认的值是否符合该记录中所包括的条件值(步骤S635)。

[0129] 如果要确认的值符合该条件值(步骤S635为是),则处理进入步骤S637。

[0130] 如果要确认的值不符合该条件值(步骤S635为否),则异常检测部130判断为发生了异常,并且生成或更新异常信息840以包括表示异常的详情的信息(步骤S636)。

[0131] 如果处理了可提取的要确认的所有值,则处理进入步骤S638。如果要确认的任何值仍待处理,则处理返回至步骤S634(步骤S637)。

[0132] 如果处理了正常模型830的所有记录,则处理进入步骤S639。如果任何记录仍待处理,则处理返回至步骤S631(步骤S638)。

[0133] 异常检测部130输出异常信息840(步骤S639)。

[0134] 例如,异常检测部130经由图8所示的输出部705输出异常信息840。异常检测部130可以将异常信息840经由图8所示的通信部706发送至装置(未示出)。异常检测部130可以经由图8所示的存储装置703将异常信息840记录在记录介质707上。

[0135] 接着,以下将参考具体数据来说明从关系变化信息810的接收到异常信息840的输出的处理序列。

[0136] 绘图部110例如在接收到如图11所示的关系变化信息811时,根据图9所示的流程图开始操作。图11示出表示要素920“E3”和要素920“E4”之间发生了关系“L0”的关系变化信息810的具体示例。

[0137] 在图9的步骤S601中,绘图部110基于所接收到的图11所示的关系变化信息811来更新状态图820(例如,从图4所示的状态图821更新为图12所示的状态图821)。

[0138] 在图9的步骤S602中,正常模型生成部120基于所接收到的关系变化信息811来更新正常模型830(例如,图6所示的正常模型831)的内容。然而,在这种情况下,没有必要更新正常模型830(例如,正常模型831)的内容。

[0139] 在图10的步骤S631中,异常检测部130从正常模型830(例如,正常模型831)提取条件类型为“关系顶点数”的记录。

[0140] 在图10的步骤S632中,异常检测部130判断为该记录的有效标志为“有效”。

[0141] 在图10的步骤S634中,异常检测部130从状态图820(例如,图12所示的状态图821)顺次提取要确认的值。

[0142] 在图10的步骤S635中,异常检测部130顺次判断要确认的值是否符合该记录中所包括的条件值(上限值2)。在这种情况下,异常检测部130判断为要通过边链接至顶点标识符为“E4”的记录的要素920的数量(即,顶点关系数)为“3”,这不符合“上限值2”。

[0143] 在图10的步骤S636中,异常检测部130生成表示顶点关系数已超过顶点关系数的上限值的异常信息840(例如,图7所示的异常信息841)。

[0144] 异常检测部130甚至处理条件类型为“边数”和“边属性”的记录。然而,在这种情况下,针对条件类型为“边数”和“边属性”的记录,没有向异常信息840(例如,异常信息841)添加信息。

[0145] 在图10的步骤S639中,异常检测部130输出异常信息840(例如,图7所示的异常信息841)。

[0146] 作为上述的本实施例的有利效果,可以提高系统异常的检测能力。例如,可以检测由于未知目标类型的攻击而引起的系统异常。

[0147] 这是由于包含了以下结构。首先,绘图部110基于关系变化信息810生成状态图820。其次,正常模型生成部120基于关系变化信息810来生成正常模型830。再次,异常检测部130基于状态图820和正常模型830来生成异常信息840。

[0148] 第二实施例

[0149] 以下将参考附图详细说明本发明的第二实施例。以下将在不会使本实施例的说明变得不清楚的范围内省略与上述说明相同的详细说明。

[0150] 图13是示出根据本发明的第二实施例的信息处理装置200的结构的框图。

[0151] 本实施例中的信息处理装置200与第一实施例中的信息处理装置100的不同之处在于:如图13所示,代替异常检测部130,前者包括异常检测部230。

[0152] 异常检测部230

[0153] 异常检测部230计算与所检测到的异常相对应的表示状态图820相对于正常模型830的偏差程度的异常度,并且输出包括异常度的异常信息840。

[0154] 除了上述的方面以外,异常检测部230与图1所示的异常检测部130相同。

[0155] 例如,基于图6所示的正常模型831和图12所示的状态图821,异常检测部230输出表示如下内容的异常信息840:要确认的值“3”相对于记录中所包括的条件值(上限值“2”)表示50%的偏差。

[0156] 图14是示出作为从异常检测部230输出的异常信息840的具体示例的示例性异常信息842的图。

[0157] 作为上述的本实施例的第一个有利效果,除第一实施例的有利效果之外,可以更详细地向用户呈现系统异常的检测结果。

[0158] 这是由于异常检测部230输出包括异常度的异常信息840。

[0159] 第三实施例

[0160] 以下将参考附图详细说明本发明的第三实施例。以下将在不会使本实施例的说明变得不清楚的范围内省略与上述说明相同的详细说明。

[0161] 图15是示出根据本发明的第三实施例的信息处理装置300的结构的框图。

[0162] 本实施例中的信息处理装置300与第一实施例中的信息处理装置100的不同之处在于:如图15所示,代替异常检测部130,前者包括异常检测部330。

[0163] 异常检测部330

[0164] 异常检测部330输出与所检测到的异常相关联的包括表示顶点(要素920)和边(要素920之间的关系)的信息的异常信息840。

[0165] 除上述的方面以外,异常检测部330与图1所示的异常检测部130相同。

[0166] 例如,基于图6所示的正常模型831和图12所示的状态图821,异常检测部330输出包括以下内容的异常信息840:关系顶点数已超过关系顶点数的上限值的顶点的标识符“E3”以及关系顶点的标识符“E1”、“E2”和“E3”。

[0167] 图16是示出作为从异常检测部330输出的异常信息840的具体示例的示例性异常信息843的图。

[0168] 异常检测部330可以包括根据第二实施例的异常检测部230的功能。在这种情况下,包括异常检测部230的功能的异常检测部330可以计算与所检测到的异常相关联的针对任意的边和顶点的异常度。

[0169] 作为上述的本实施例的第一个有利效果,除第一实施例的有利效果以外,可以更详细地向用户呈现系统异常的检测结果。

[0170] 这是由于异常检测部330输出与所检测到的异常相关联的包括表示顶点和边的信息的异常信息840。例如在检测到一个计算机A的异常的情况下,异常检测部330输出“计算机A与计算机B的通信存在异常”作为异常信息840。换句话说,与仅输出“计算机A存在异常”的情况相比,可以知晓与同计算机B的通信相关联的计算机A的内部存在异常这一事实。

[0171] 第四实施例

[0172] 以下将参考附图详细说明本发明的第四实施例。以下将在不会使本实施例的说明变得不清楚的范围内省略与上述说明相同的详细说明。

[0173] 图17是示出根据本发明的第四实施例的信息处理装置400的结构的框图。

[0174] 本实施例中的信息处理装置400与第一实施例中的信息处理装置100的不同之处在于:如图17所示,代替异常检测部130,前者包括异常检测部430。

[0175] 异常检测部430

[0176] 异常检测部430输出基于状态图820和正常模型830所生成的包括用于表示异常的图表的异常信息840。用于表示异常的图表包括网络图(后面更详细地说明)、矩阵(后面更详细地说明)和其它任意图表。

[0177] 异常检测部430按照以下方式来输出表示异常的异常信息840。异常检测部430例如在与状态图820上的异常相对应的部分中利用增加的线宽来表示图形的线或字符等。异常检测部430还可以在与状态图820上的异常相对应的部分中利用增加的大小来表示图形的线或字符等。异常检测部430甚至可以在与状态图820上的异常相对应的部分中利用颜色的变化来显示图形的线或字符等。异常检测部430甚至可以在与状态图上的异常相对应的部分中利用背景颜色的变化来显示图形的线或字符等。

[0178] 异常检测部430可以根据异常信息840中的图形、字符或矩阵单元的配置来强调与状态图820上的异常相对应的部分。更具体地,异常检测部430可以使与状态图820上的异常相对应的部分的图形集中在网络图的预定区域中(例如,网络图的左侧或靠近网络图的中心)。此外,异常检测部430可以通过列表排序来生成矩阵以使得在矩阵内按预定的顺序(例如,按从最左列和最上行起的顺序)来配置与状态图820上的异常相对应的单元。

[0179] 异常检测部430可以与上述的示例无关地,使用任何技术来强调与状态图820上的异常相对应的部分并且输出表示异常的异常信息840。

[0180] 异常检测部430还可以输出基于正常模型的图表(以下称为正常模型图表)。例如,异常检测部430输出正常模型图表以使得用户能够将正常模型图表和用于表示异常的图表进行比较并参考。异常检测部430可以独立地或者通过将正常模型图表包括在异常信息840中来输出该正常模型图表。

[0181] 异常检测部430可以基于例如正常模型生成部120所生成的正常模型830来生成正常模型图表。

[0182] 异常检测部430可以获得正常模型生成部120所生成的正常模型图表。在这种情况下,正常模型生成部120基于例如来自异常检测部430的请求而根据正常模型830生成正常模型图表并输出该正常模型图表。

[0183] 正常模型生成部120例如可以基于来自异常检测部430的请求来将正常模型830传送到绘图部110并请求绘图部110生成正常模型图表。绘图部110或正常模型生成部120所生成的正常模型图表可以直接或经由异常检测部430来输出。

[0184] 可以例如根据以下过程通过异常检测部430或正常模型生成部120来生成正常模型图表。作为该过程中的第一处理,将顶点的所有组合(要素920之间的关系)与正常模型830对照以提取被判断为正常的顶点的组合。作为该过程中的第二处理,将所提取到的顶点的组合包括在正常模型图表中。

[0185] 除上述的方面以外,异常检测部430与图1所示的异常检测部130相同。

[0186] 以下将给出基于图6所示的正常模型831和图12所示的状态图821从异常检测部430输出的异常信息840的示例。

[0187] 图18是示出作为从异常检测部430输出的异常信息840的具体示例的以网络图表示的示例性异常信息844的图。

[0188] 参考图18,圆圈表示顶点并且圆圈内所标记的字符串表示顶点标识符。使圆圈彼

此连接的线段表示边。例如,双圆圈和双线段强调被判断为存在异常的顶点(要素920)和边(要素920之间的关系)。

[0189] 网络图可以是任意类型并且以任意形式来表示异常而限于图18所示的示例。

[0190] 图19是示出作为从异常检测部430输出的异常信息840的具体示例的以矩阵表示的示例性异常信息845的图。

[0191] 异常信息845是如下的矩阵,其中该矩阵具有由纵轴上的顶点标识符(最左顶点标识符)的列表所指定的作为边的from(始端)侧顶点的顶点以及由横轴上的顶点标识符(最上行的顶点标识符)的列表所指定的作为边的to(终端)侧顶点的顶点。矩阵的单元中的字符串(例如,“L0”)表示从from侧顶点到to侧顶点的边的有无(NL表示边不存在,其它表示边存在)以及属性(L0、L1和L2)。参考图19,与异常相关联的顶点和边由斜体字符表示。

[0192] 与图19所示的示例无关地,矩阵可以是任意类型并且以任意形式表示异常。

[0193] 异常检测部430可以与上述的示例无关地,以彼此自由组合的方式或者作为异常信息840独立地输出通过以任意类型的图而使用任何技术表示异常所获得的任意异常图表以及基于正常模型830所生成的任意类型的正常图表。例如,异常检测部430可以与正常模型图表重叠地输出异常图表。

[0194] 异常检测部430可以包括根据第二实施例的异常检测部230和根据第三实施例的异常检测部330的功能。

[0195] 第四实施例的变形例

[0196] 异常检测部430可以独立地或彼此相关联地输出表示状态图820、正常模型830和异常信息840各自的时间变化的显示信息。时间变化是指随着时间的经过的变化。

[0197] 显示信息可以是表示例如状态图820、正常模型830和异常信息840中任何之一的状态的变化了的运动图像的信息。显示信息还可以是表示状态图820、正常模型830和异常信息840中任何之一在多个时间点处可用的状态的特定配置的信息。

[0198] 可以与当前时刻相对应地实时更新显示信息。

[0199] 作为上述的本实施例的第一个有利效果,除第一实施例的有利效果以外,可以以更易于人理解的形式向用户呈现系统异常的检测结果。

[0200] 原因如下。异常检测部430输出包括用于表示异常的图表的异常信息840。异常检测部430还输出正常模型图表。异常检测部430甚至输出表示状态图820、正常模型830和异常信息840各自的时间变化的显示信息。

[0201] 作为上述的实施例的第二个有利效果,即使在系统中实际上没有发生异常的情况下,使通信被视为正常的顶点之间的间隔也可以与使通信被视为异常的顶点之间的间隔区分开来。此外,能够进行该区分,这使得可以例如通过仅允许被视为通信正常的发生的顶点之间的通信来防止异常通信。

[0202] 这是由于包含了以下结构。首先,异常检测部430或正常模型生成部120将顶点的所有组合与正常模型830进行对照以提取被判断为正常的顶点的组合,并且将所提取的顶点的组合包括在正常模型图表中。其次,异常检测部430与正常模型图表重叠地输出用于表示异常的图表。

[0203] 第五实施例

[0204] 以下将参考附图详细说明本发明的第五实施例。以下将在不会使本实施例的说明

变得不清楚的范围内省略与上述说明相同的详细说明。

[0205] 图20是示出根据本发明的第五实施例的信息处理装置500的结构的框图。

[0206] 本实施例中的信息处理装置500与第一实施例中的信息处理装置100的不同之处在于:如图20所示,代替绘图部110和异常检测部130,前者包括绘图部510和异常检测部530,并且还包括历史累积部540。

[0207] 绘图部510

[0208] 绘图部510在预定时间将能够恢复该时间点可用的状态图820的信息与例如该时间点的时刻相关联地记录在历史累积部540中。预定时间的示例包括预定的时刻。预定时间可以是关系变化信息810的处理数量达到预定阈值的时刻。预定时间可以是与上述的示例无关的任意时刻。能够恢复该时间点可用的状态图820的信息的示例包括与任意先前时间点(例如,预定时间点之前的时间点)处可用的状态图820的差异。能够恢复该时间点可用的状态图820的信息甚至可以是该时间点处可用的状态图820自身。

[0209] 绘图部510还可以将最新的状态图820作为暂时状态图记录在历史累积部540中,并且每当获得关系变化信息810时更新该暂时状态图及其相关联的时刻。在这种情况下,绘图部510可以在预定时间停止更新暂时状态图并且将暂时状态图确定为最终状态图820。

[0210] 除上述的方面以外,绘图部510与图1所示的绘图部110相同。

[0211] 历史累积部540

[0212] 历史累积部540存储状态图820。历史累积部540还可以存储上述的暂时状态图。

[0213] 异常检测部530

[0214] 异常检测部530基于正常模型830和历史累积部540中所存储的状态图820来检测与要监视的系统900相关联的异常。异常检测部530还可以基于历史累积部540中所存储的暂时状态图来检测与要检测的系统900相关联的异常。除上述的方面以外,异常检测部530与图1所示的异常检测部130等同。

[0215] 异常检测部530可以包括根据第一实施例的异常检测部130、根据第二实施例的异常检测部230、根据第三实施例的异常检测部330和根据第四实施例的异常检测部430的任何功能。

[0216] 例如在异常检测部530包括异常检测部430的功能的情况下,第四实施例的变形例中的显示信息可以与所要求的时间范围相关联。

[0217] 作为上述的本实施例的有利效果,除第一实施例的有利效果以外,可以向用户提供过去状态图820相对于当前正常模型830的异常信息840。

[0218] 这是由于包含了以下结构。首先,绘图部510在预定时间将状态图820记录在历史累积部540中,并且历史累积部540存储状态图820。其次,异常检测部530基于正常模型830和历史累积部540中所存储的状态图820来检测与要监视的系统900相关联的异常。

[0219] 尽管以上已经参考各实施例说明了本发明,但本发明不限于上述实施例。可以在本发明的范围内对本发明的结构或详情作出本领域技术人员将理解的各种变化。

[0220] 本申请基于并要求2014年3月20日提交的日本专利申请2014-058497和2014年6月6日提交的PCT国际申请PCT/JP2014/003014的优先权,它们全部内容通过引用包含于此。

[0221] 附图标记说明

[0222] 100 信息处理装置

- [0223] 110 绘图部
- [0224] 120 正常模型生成部
- [0225] 130 异常检测部
- [0226] 200 信息处理装置
- [0227] 230 异常检测部
- [0228] 300 信息处理装置
- [0229] 330 异常检测部
- [0230] 400 信息处理装置
- [0231] 430 异常检测部
- [0232] 500 信息处理装置
- [0233] 510 绘图部
- [0234] 530 异常检测部
- [0235] 540 历史累积部
- [0236] 700 计算机
- [0237] 701 CPU
- [0238] 702 存储部
- [0239] 703 存储装置
- [0240] 704 输入部
- [0241] 705 输出部
- [0242] 706 通信部
- [0243] 707 记录介质
- [0244] 810 关系变化信息
- [0245] 811 关系变化信息
- [0246] 820 状态图
- [0247] 821 状态图
- [0248] 830 正常模型
- [0249] 831 正常模型
- [0250] 840 异常信息
- [0251] 841 异常信息
- [0252] 842 异常信息
- [0253] 843 异常信息
- [0254] 844 异常信息
- [0255] 845 异常信息
- [0256] 900 要监视的系统
- [0257] 920 要素
- [0258] 930 关系变化监视部件

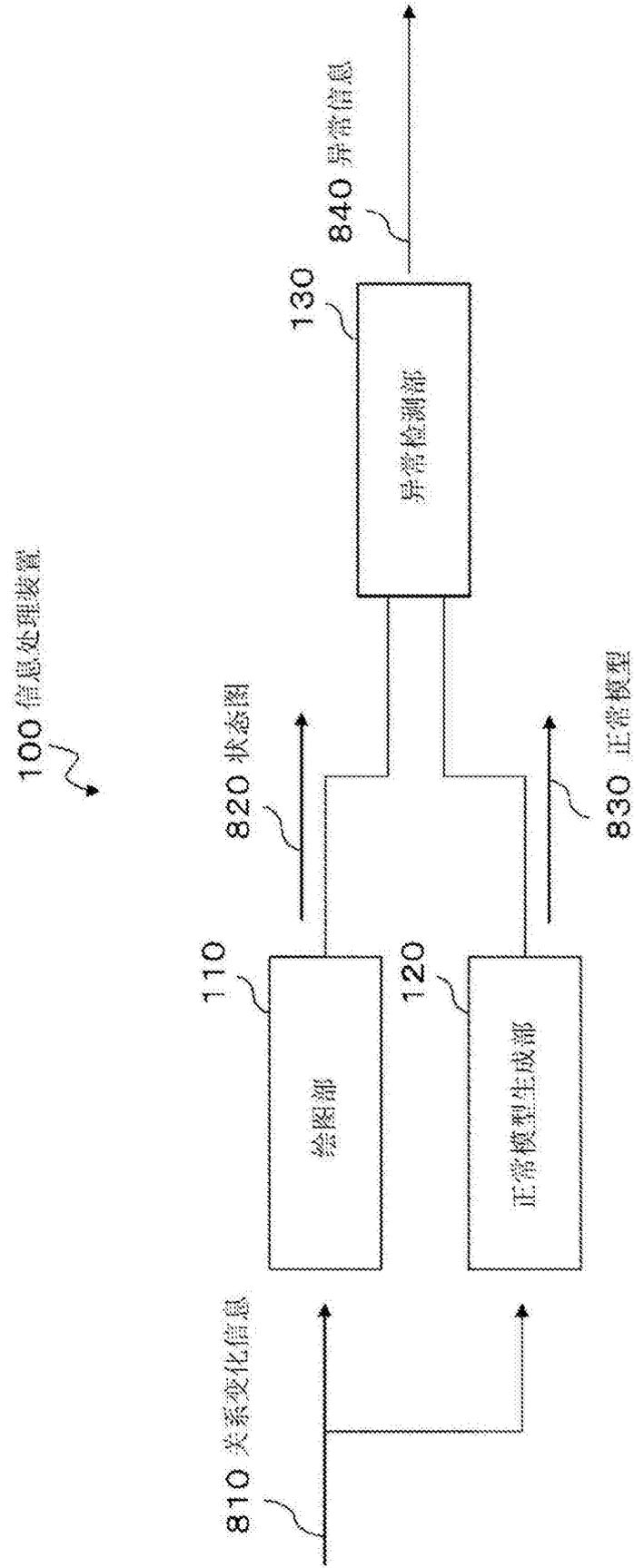


图1

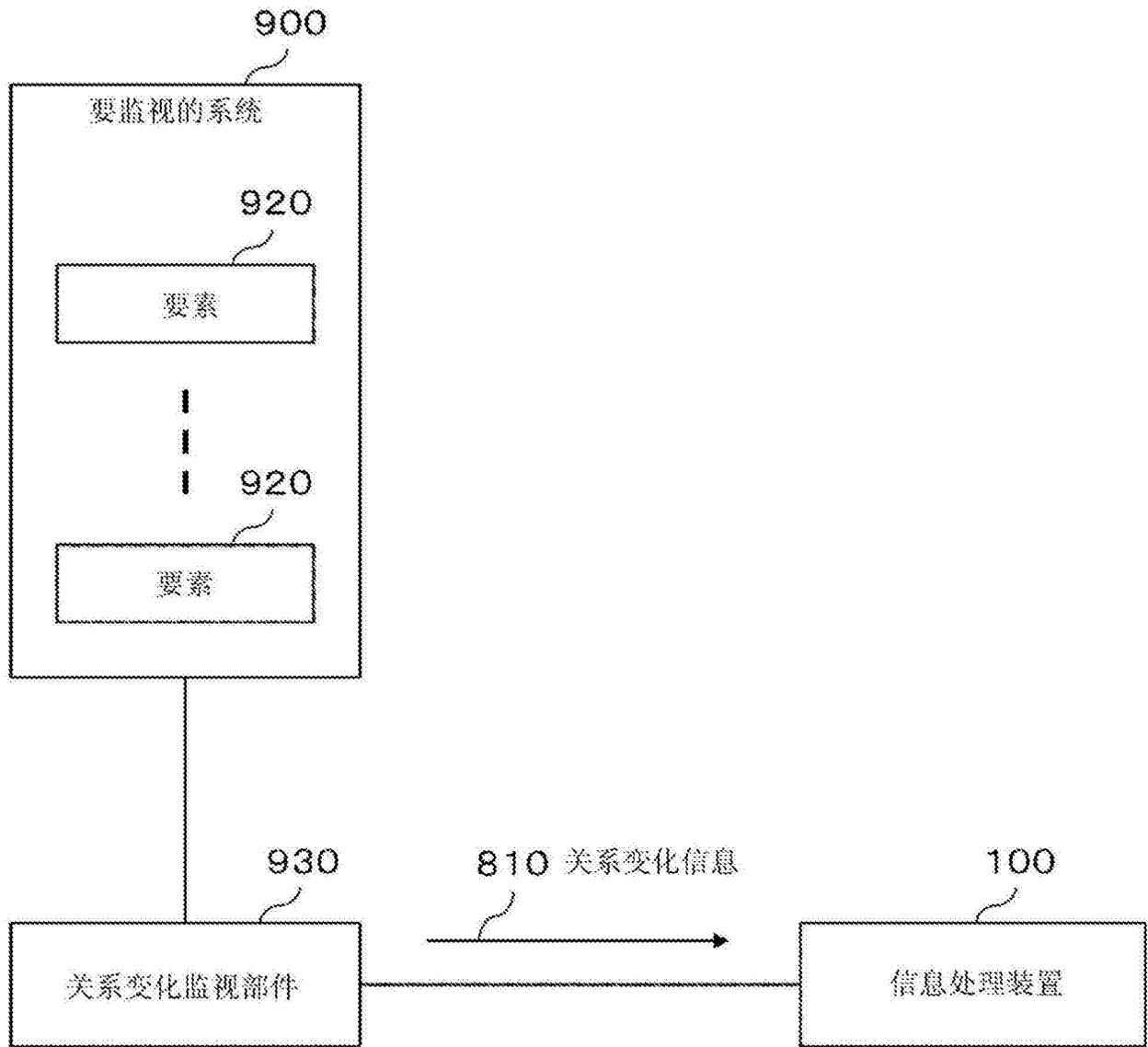


图2

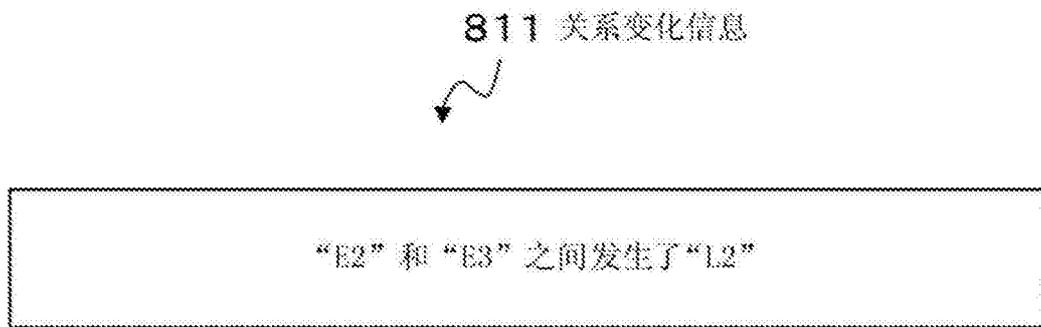


图3

821 状态图



顶点标识符	边
E1	E2;L0、 E3;L1;L1
E2	E1;L0、 E3;L2
E3	E1;L1;L1、 E2;L2
E4	

图4

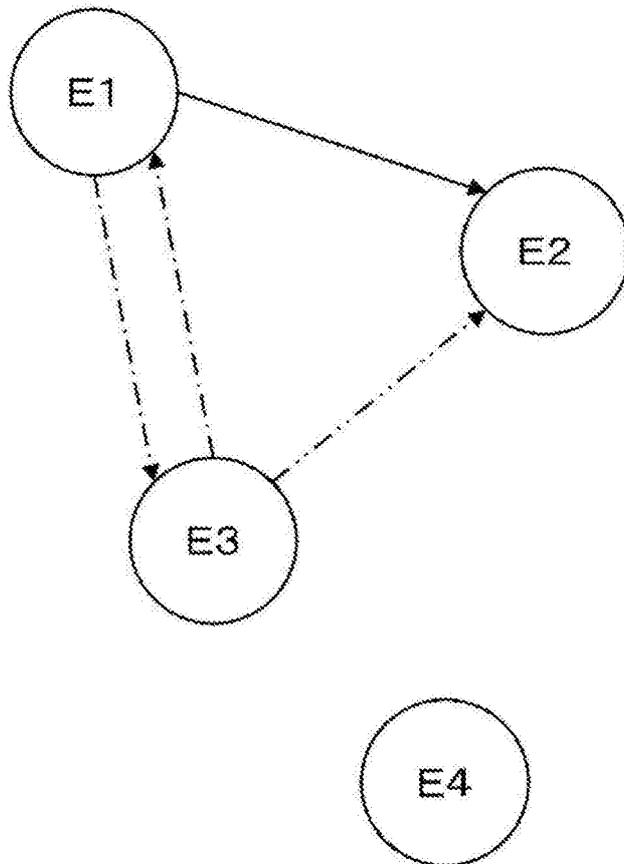


图5

831 正常模型



条件类型	条件值	有效标志
关系顶点数	上限值2	有效
次数	上限值6	有效
边属性		无效

图6

841 异常信息



关系顶点数已超过关系顶点数的上限值

图7

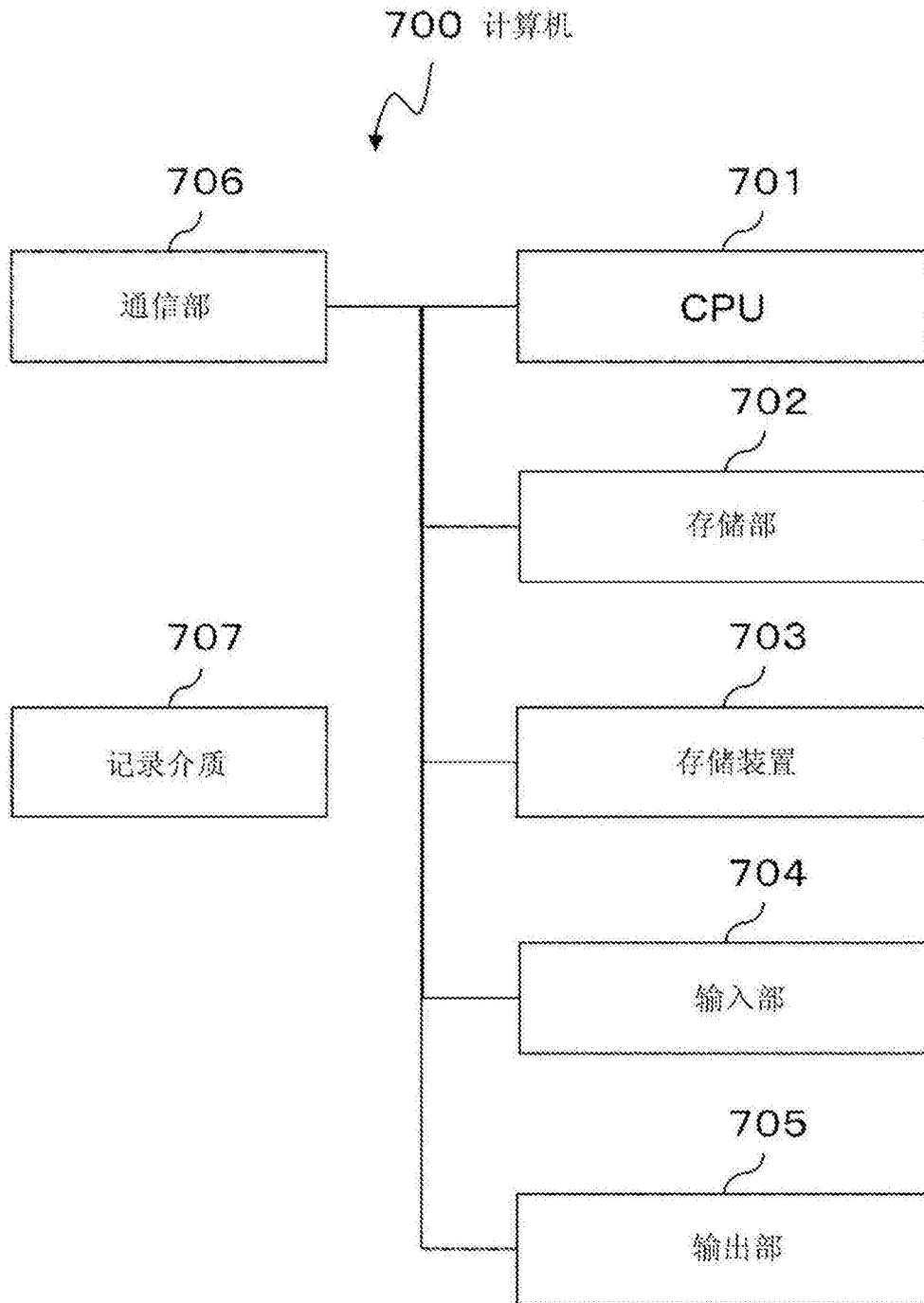


图8

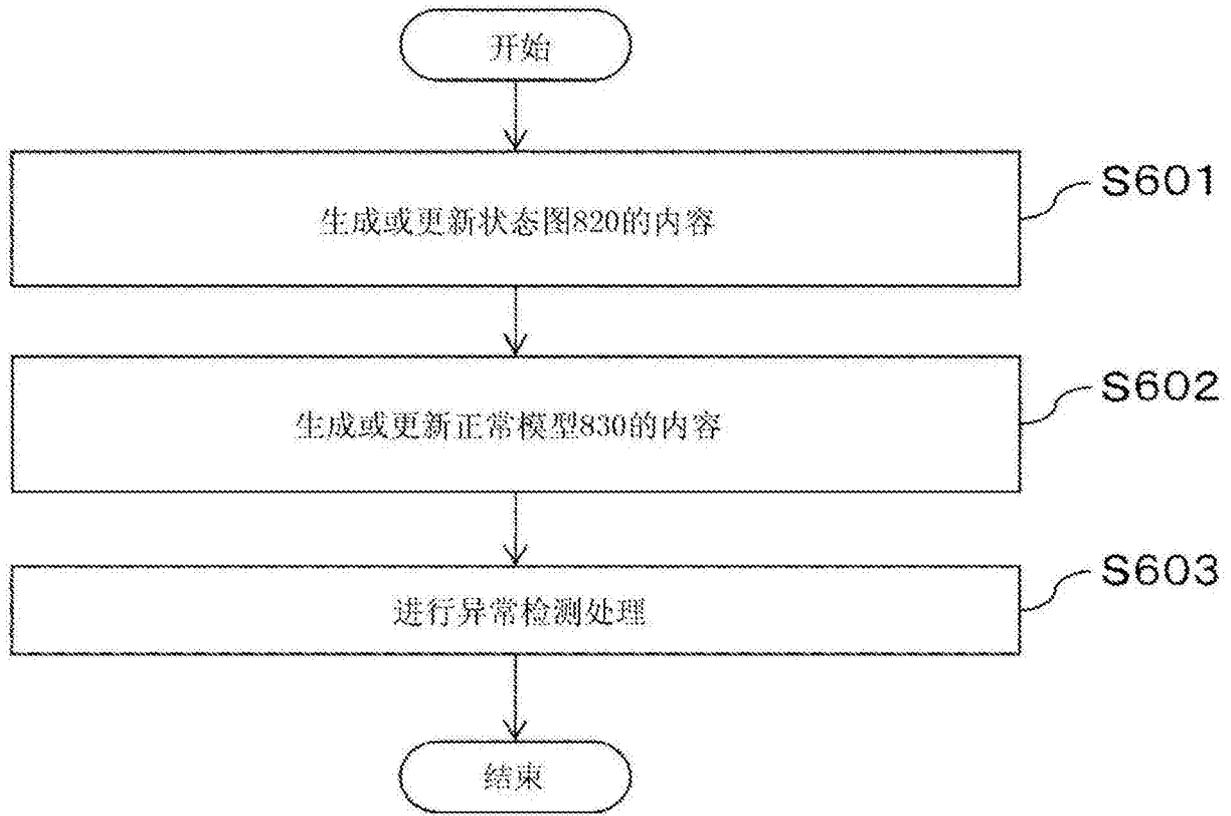


图9

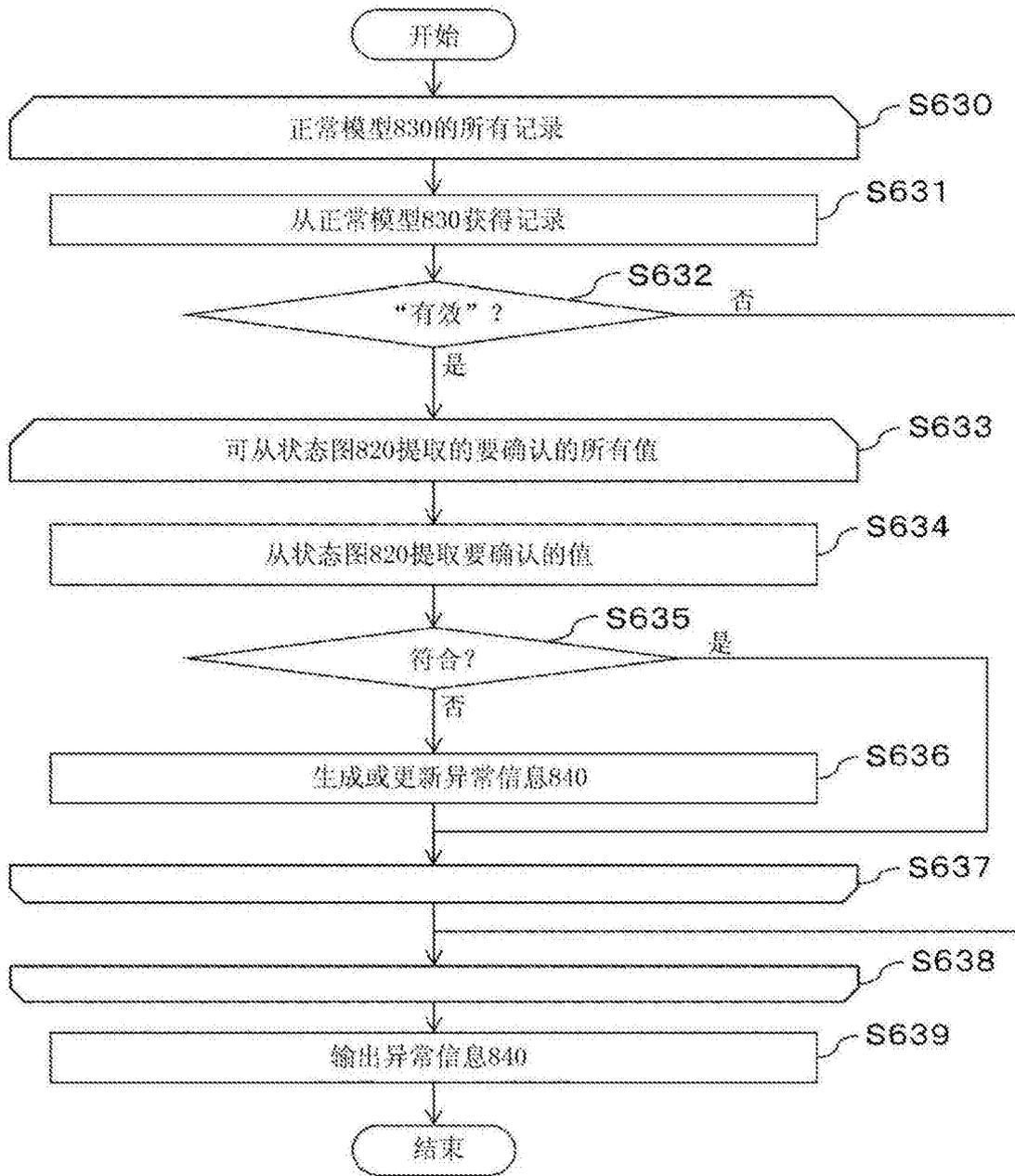


图10

811 关系变化信息

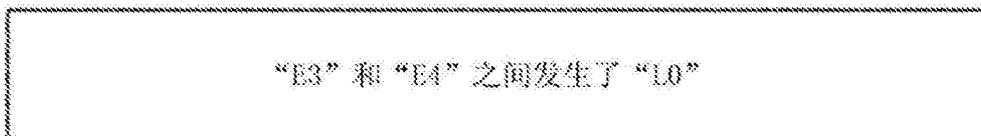


图11

821 状态图



顶点标识符	边
E1	E2;L0, E3;L1;L1
E2	E1;L0, E3;L2
E3	E1;L1;L1、E2;L2、E4;L0
E4	E3;L0

图12

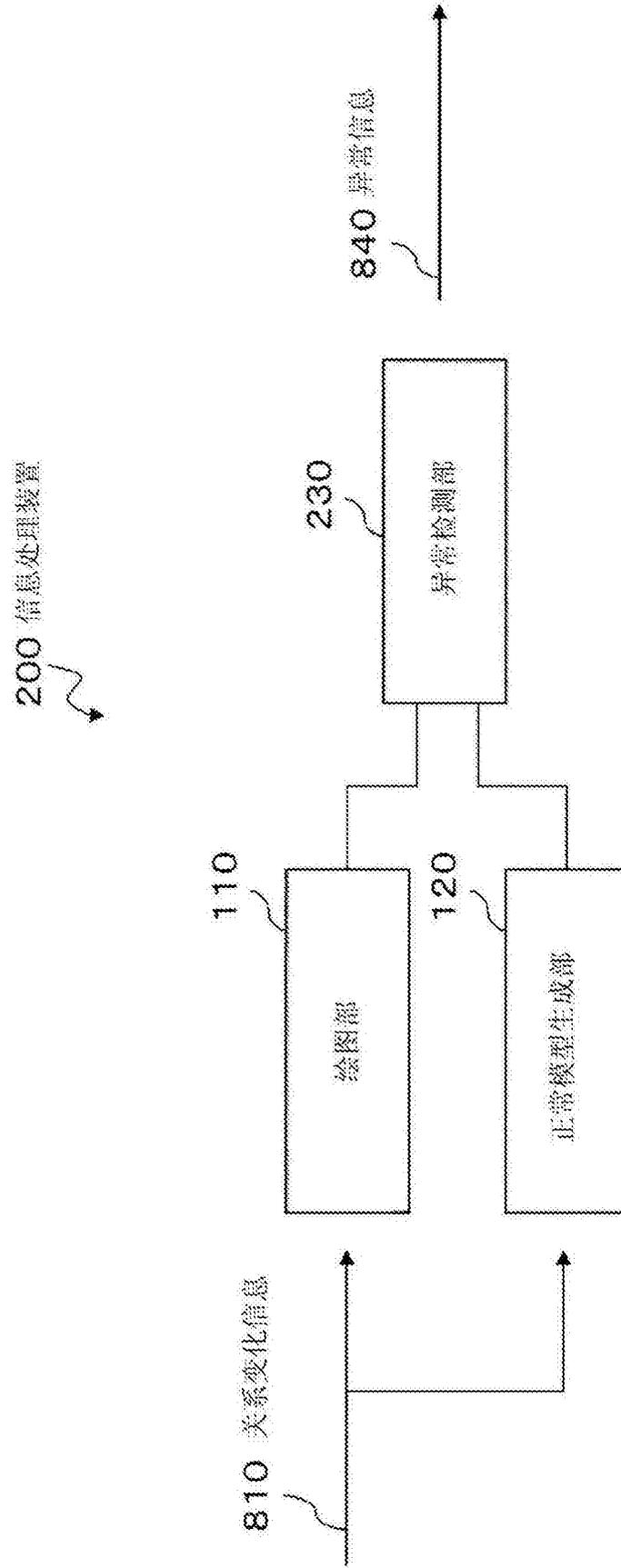


图13

842 异常信息



关系顶点数已超过关系顶点数的上限值50%

图14

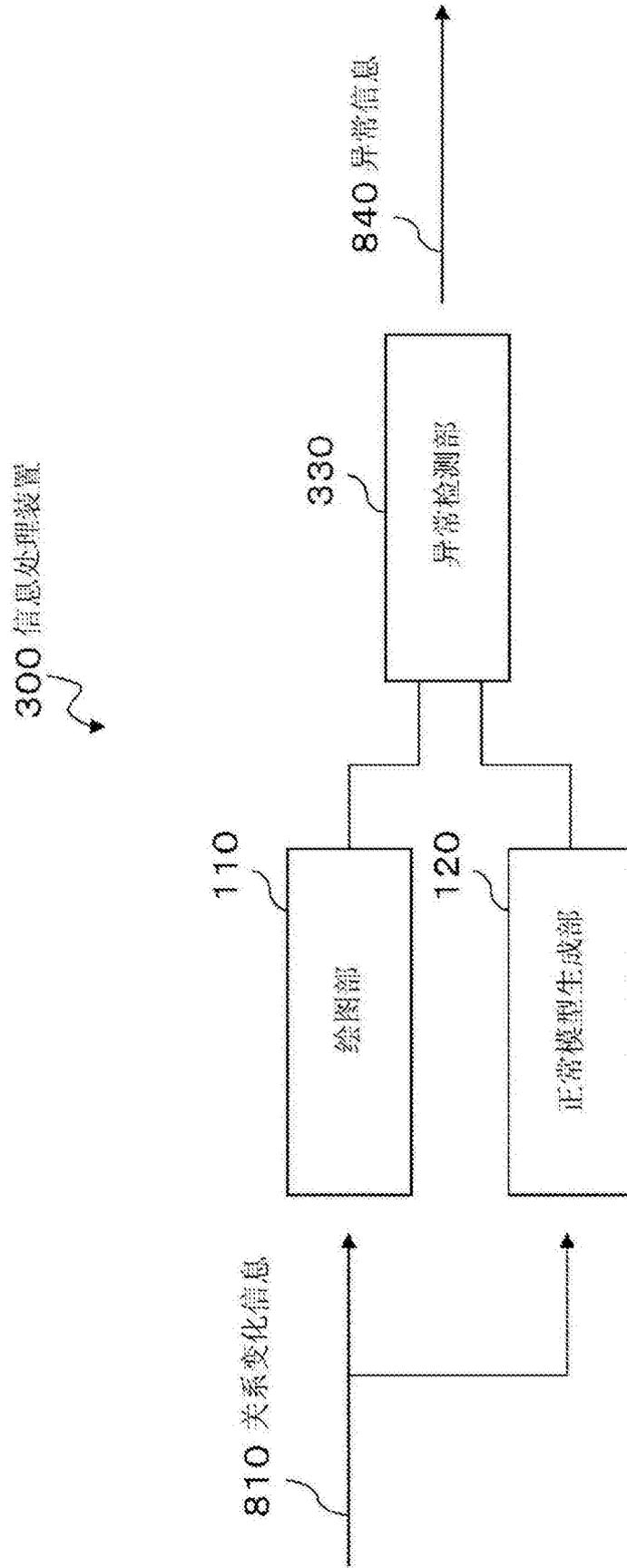


图15

843 异常信息



在“E3”中，关系顶点(“E1”、“E2”和“E4”)数已超过关系顶点数的上限值

图16

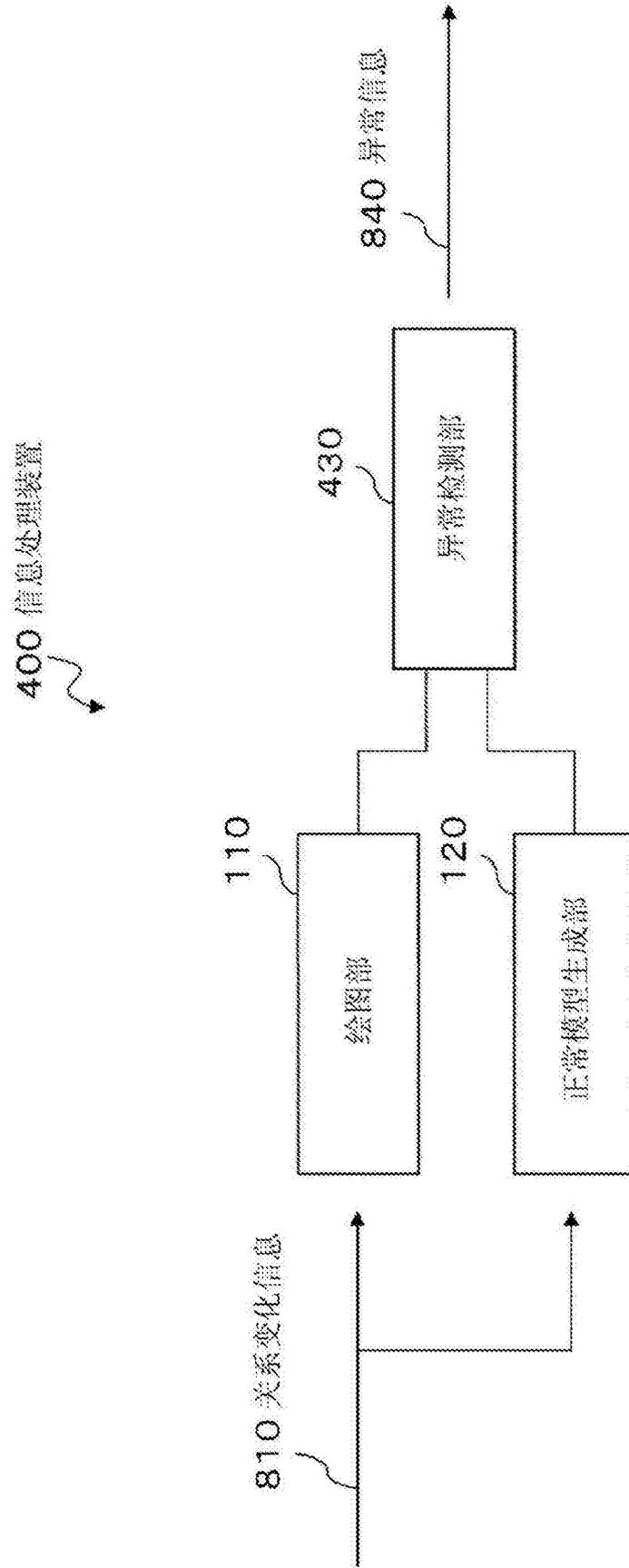


图17

844 异常信息

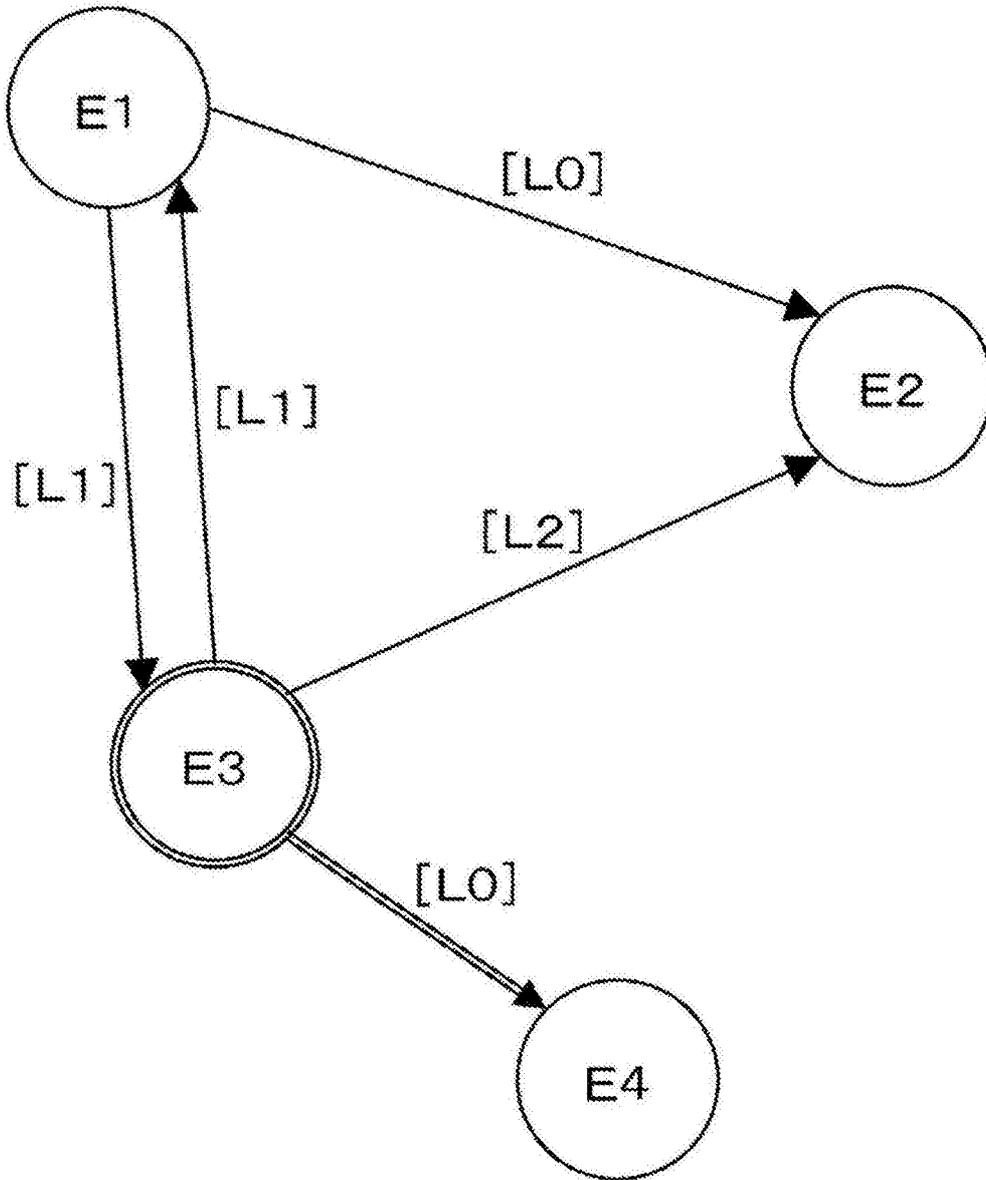


图18

845 异常信息



	E1	E2	E3	E4
E1	NL	L0	L1	NL
E2	NL	NL	NL	NL
E3	L1	L2	NL	L0
E4	NL	NL	NL	NL

图19

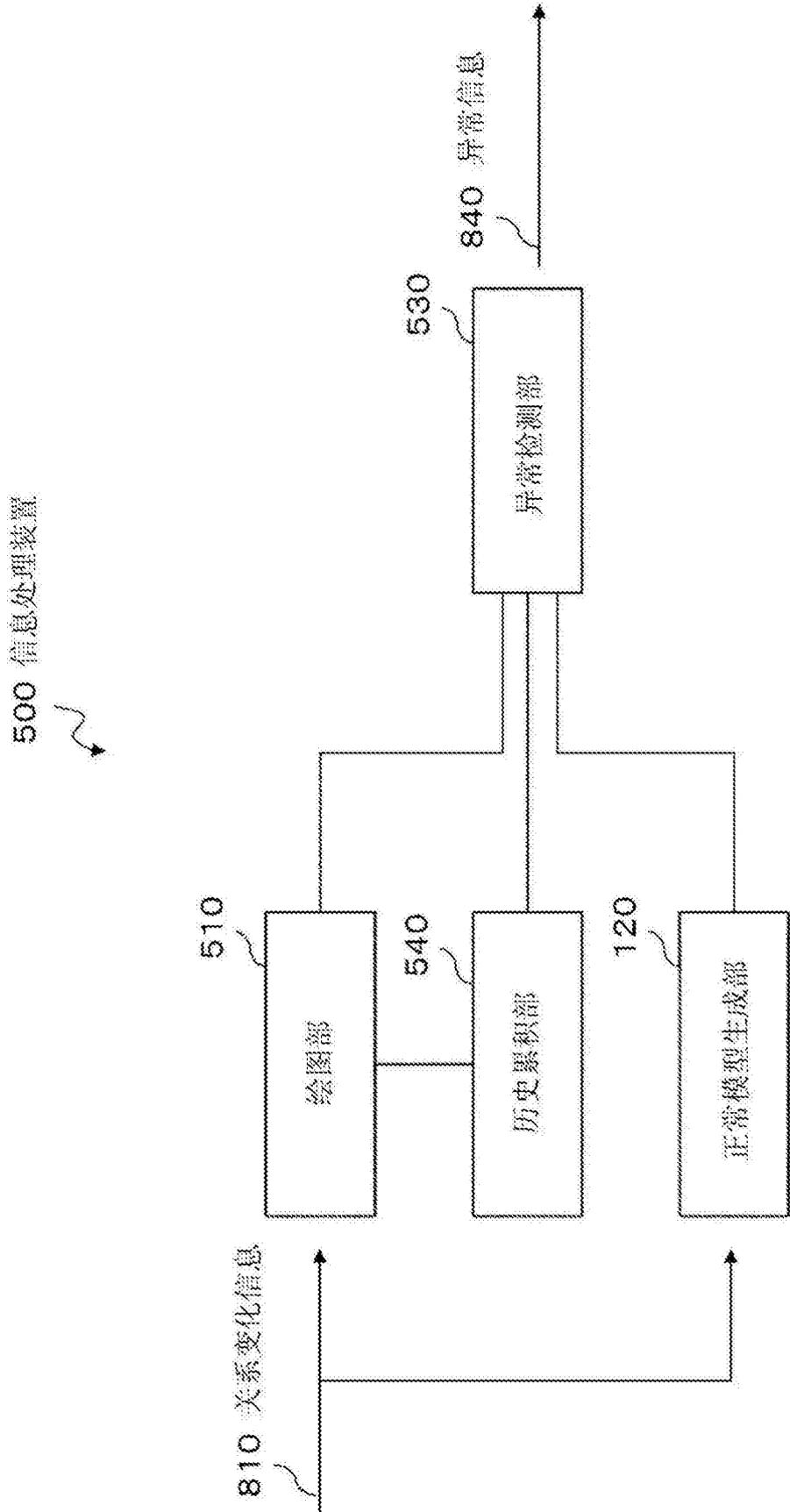


图20