



(12) 发明专利

(10) 授权公告号 CN 114073023 B

(45) 授权公告日 2024. 05. 31

(21) 申请号 202080044686.8

(22) 申请日 2020.04.24

(65) 同一申请的已公布的文献号
申请公布号 CN 114073023 A

(43) 申请公布日 2022.02.18

(30) 优先权数据
2019-086276 2019.04.26 JP
2019-165493 2019.09.11 JP

(85) PCT国际申请进入国家阶段日
2021.12.17

(86) PCT国际申请的申请数据
PCT/JP2020/017632 2020.04.24

(87) PCT国际申请的公布数据
W02020/218478 JA 2020.10.29

(73) 专利权人 株式会社赛斯
地址 日本东京
专利权人 长濑产业株式会社

(72) 发明人 伊东久雄

(74) 专利代理机构 北京柏杉松知识产权代理事
务所(普通合伙) 11413
专利代理师 袁波 刘继富

(51) Int.Cl.
H04L 1/00 (2006.01)
G06F 11/00 (2006.01)
G06F 11/07 (2006.01)

(56) 对比文件
JP 6494004 B1, 2019.04.03
CN 109491996 A, 2019.03.19
WO 2018/177264 X, 2018.10.04
US 2018/0342036 Y, 2018.11.29
CN 107885305 A, 2018.04.06
CN 108648084 A, 2018.10.12

审查员 刘梅

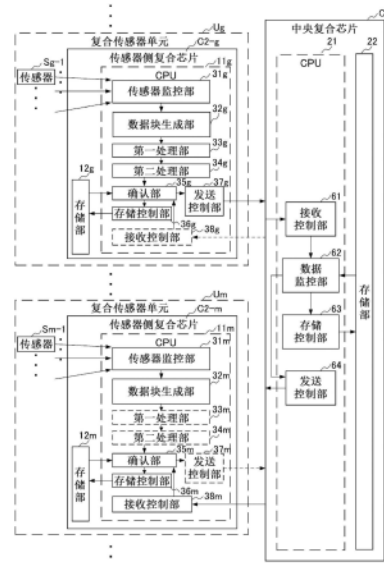
权利要求书1页 说明书16页 附图6页

(54) 发明名称

电子设备和信息处理系统

(57) 摘要

本发明提供一种能够进一步降低传输数据时的数据损坏风险的技术。数据块生成部(32g)基于传感器信息生成数据块(BD1)、数据块(BD2)、以及数据块(BD3)。第一处理部(33g)生成第二关联信息(FT1),并将其作为第一关联信息(HD2)附加在数据块(BD2)中。第二处理部(34g)生成至少包含根据数据块(BD2)得到的哈希值的第二关联信息(FT2),并附加在数据块(BD2)中。存储控制部(36g)执行以下控制:利用区块链技术将附加了第一关联信息(HD2)和第二关联信息(FT2)的数据块(BD2)与包含数据块(BD1)的一个以上的其他所述单位的数据进行关联,并存储在存储部(12g)中。由此,解决上述问题。



1. 一种电子设备,其具有:
 - 生成单元,其基于规定的信息,按每个规定的单位生成数据;
 - 第一处理单元,其将由所述生成单元生成的处理对象的所述单位的数据作为第一单位数据,将在此之前由所述生成单元生成的所述单位的数据作为第二单位数据,生成至少包含根据该第二单位数据得到的哈希值的信息作为第一关联信息,将该第一关联信息附加在处理对象的所述第一单位数据中;
 - 第二处理单元,其生成至少包含根据所述第一单位数据得到的哈希值的信息作为第二关联信息,将该第二关联信息附加在处理对象的所述第一单位数据中;
 - 存储控制单元,其执行以下控制,即,利用区块链技术,将附加了所述第一关联信息和所述第二关联信息的处理对象的所述第一单位数据与包含所述第二单位数据的一个以上的其他所述单位的数据进行关联,并存储在规定的存储介质中;以及
 - 确认部,其确认前一个由所述生成单元生成的单位的数据的哈希值与当前的单位的数据的第一关联信息是否为同一内容。
2. 根据权利要求1所述的电子设备,其中,
 - 具有发送控制单元,其执行将附加了所述第一关联信息和所述第二关联信息的所述第一单位数据发送至其他的电子设备的控制。
3. 根据权利要求1或2所述的电子设备,其中,
 - 还具有:
 - 获取单元,其从外部获取使所述第一处理单元、所述第二处理单元、以及所述存储控制单元发挥功能的程序;以及
 - 存储单元,其存储从外部获取的所述程序。
4. 根据权利要求1或2所述的电子设备,其中,
 - 还具有电力获取单元,其获取使本机驱动的电力。
5. 根据权利要求3所述的电子设备,其中,
 - 还具有电力获取单元,其获取使本机驱动的电力。
6. 一种信息处理系统,其构成为包含多个权利要求2至5中的任一项所述的电子设备。
7. 根据权利要求6所述的信息处理系统,其中,
 - 多个所述电子设备分别向其他的所述电子设备发送与车辆的操作相关的数据。
8. 根据权利要求6所述的信息处理系统,其中,
 - 多个所述电子设备分别向其他的所述电子设备发送所拍摄的图像的数据。

电子设备和信息处理系统

技术领域

[0001] 本发明涉及电子设备、信息处理系统。

背景技术

[0002] 以往,在进行信息的收发的情况下,涉及数据损坏的风险对策是很重要的。在这一点上,曾提出了一种降低在信息传输时的数据损坏风险的技术(例如参照专利文献1)。

[0003] 现有技术文献

[0004] 专利文献

[0005] 专利文献1:日本特开2017-026755号公报。

发明内容

[0006] 发明要解决的问题

[0007] 在此,仅在包括上述专利文献1的现有技术中,例如在构建从传感器经由通信线路传输数据的系统的情况下,通常由一个或少数的CPU(Central Processing Unit,中央处理器)集中管理来自传感器的所有的输出信息。

[0008] 但是,近年来,传感器的数量和种类有增加的趋势,管理输出信息的CPU的负荷日益增大。对此,如果在发生了雷电或静电的放电现象、来自其他电子设备的电磁波噪声等引起的传输数据的数据乱码等状况的情况下,需要时间进行CPU中的数据的安全性检查处理,则在CPU侧无法采取迅速的应对。

[0009] 因此,在当前状况下,在降低CPU的负荷的同时能够立即检测到使系统误动作的传输数据的异常、进而能够使传输数据的异常瞬间正常化的重要性逐渐增加。

[0010] 本发明是鉴于这样的情况而完成的,其目的在于提供一种能够进一步降低传输数据时的数据损坏风险的技术。

[0011] 用于解决问题的方案

[0012] 为了实现上述目的,本发明的一个方式的电子设备具有:

[0013] 生成单元,其基于规定的信息,按每个规定的单位生成数据;

[0014] 第一处理单元,其将由所述生成单元生成的处理对象的所述单位的数据作为第一单位数据,将在此之前由所述生成单元生成的所述单位的数据作为第二单位数据,生成至少包含根据该第二单位数据得到的哈希值的信息作为第一关联信息,将该第一关联信息附加在处理对象的所述第一单位数据中;

[0015] 第二处理单元,其生成至少包含根据所述第一单位数据得到的哈希值的信息作为第二关联信息,将该第二关联信息附加在处理对象的所述第一单位数据中;以及

[0016] 存储控制单元,其执行以下控制,即,利用区块链技术,将附加了所述第一关联信息和所述第二关联信息的处理对象的所述第一单位数据与包含所述第二单位数据的一个以上的其他所述单位的数据进行关联,并存储在规定的存储介质中。

[0017] 发明效果

[0018] 根据本发明,能够提供一种能够进一步降低传输数据时的数据损坏风险的技术。

附图说明

[0019] 图1是表示本发明的电子设备的一个实施方式涉及的区块链芯片的结构图。

[0020] 图2A是表示在通过连接多个图1的区块链芯片来构建LAN(Local Area Network, 局域网)的情况(有线LAN)的例子图。

[0021] 图2B是表示在通过连接多个图1的区块链芯片来构建LAN(Local Area Network, 局域网)的情况(无线LAN)的例子图。

[0022] 图3是通过连接多个图1的区块链芯片就能够实现的分布式AI(人工智能)系统的示意图。

[0023] 图4是表示本发明的信息处理系统的一个实施方式涉及的传感器系统的结构图。

[0024] 图5是表示在图4的传感器系统中的在中央复合芯片与传感器侧复合芯片之间传输的数据的结构的具体例子图。

[0025] 图6是表示图4的传感器系统中的中央复合芯片和传感器侧复合芯片的功能结构的一个例子图。

[0026] 图7A是表示将图4的传感器系统应用于汽车的控制的情况的例子示意图。

[0027] 图7B是表示将图4的传感器系统应用于汽车的控制的情况的例子示意图。与图7A不同。

具体实施方式

[0028] 以下,使用附图对本发明的实施方式进行说明。

[0029] 图1是表示本发明的电子设备的一个实施方式涉及的区块链芯片的结构图。

[0030] 图1所示的区块链芯片C是采用SIP(System in a Package,系统级封装)形式的半导体产品。

[0031] 区块链芯片C是在基板10搭载了CPU(Central Processing Unit,中央处理器)11、存储部12、复位按钮13、通信部14、指示器15、标识器16、以及电力获取部17的结构。

[0032] 基板10是尺寸为20mm×40mm左右的小型基板。但是,基板10的形式没有特别限定,能够按照用途采用各种各样的形式。

[0033] CPU11是采用组装有外围电路的SoC(System on Chip,片上系统)形式的复合型CPU。

[0034] CPU11根据预先记录在后述的非易失性存储器(高速缓冲存储器)121的程序和被加载的程序来执行各种处理。

[0035] 存储部12构成为包含非易失性存储器(高速缓冲存储器)121和易失性存储器(RAM/Random Access Memory,随机存取存储器)122。

[0036] 非易失性存储器(高速缓冲存储器)121由作为工作基础的软件(以下称为“基础软件”)、IPL(Initial Program Loader,初始程序加载器)、以及IOCS(Input-Output Control System,输入输出控制系统)构成。

[0037] IPL是用于将区块链主体加载到非易失性存储器(高速缓冲存储器)121的程序。

[0038] IOCS是执行外围设备的控制的程序,由基础软件和IOCS构成了用于使区块链芯片C工作的基础程序。

[0039] 像这样,非易失性存储器(高速缓冲存储器)121能够采用简单的结构。

[0040] 这里,区块链芯片C在出厂时没有装载区块链主体。由此,能够总是加载最新版本的区块链主体并使其工作。

[0041] 此外,即使区块链芯片C在工作中,只要按下后述的复位按钮13而将区块链芯片C复位,就能够容易地进行区块链主体的升级。

[0042] 易失性存储器(RAM)122是用于CPU11控制各种处理的执行的主存储器,适当地存储CPU11控制各种处理的执行时所需要的数据等。

[0043] 复位按钮13是用于使区块链芯片C恢复到初始状态的按钮。

[0044] 通信部14经由包含互联网的网络N在与其他装置(例如云服务器300、其他区块链芯片C等)之间进行通信。通信部14从外部接收例如规定的程序(例如区块链主体)。

[0045] 通信部14能够构成为包含LAN端子141、输入输出(I/O)端口142、蓝牙(Bluetooth(注册商标))天线143。

[0046] 指示器15是表示区块链芯片C的状态的显示器。具体而言,例如指示器15可识别地显示区块链芯片C的初始状态、正常状态、程序和数据的收发中、或异常状态等。指示器15由例如LED(Light Emitting Diode,发光二极管)等构成。

[0047] 标识器16是能够使唯一能够确定区块链芯片C的标识号(例如ID号)可见的机构。

[0048] 电力获取部17获取来自电源的电力,并提供至区块链芯片C。由此,能够单独地驱动区块链芯片C。此外,也能够搭载在组装有外围电路的控制基板来使用。

[0049] 图2A和图2B是表示通过连接多个图1的区块链芯片来构建LAN的情况的例子图。

[0050] 图2A示出了通过连接多个图1的区块链芯片C来构建有线LAN100的情况的例子。

[0051] 在该情况下,如图2A所示,例如能够通过使HUB71连接多个区块链芯片C来构建有线LAN100。

[0052] 图2B示出了通过连接多个图1的区块链芯片C来构建无线LAN200的情况的例子。

[0053] 如图2B所示,例如能够通过利用能够进行多个设备彼此之间的通信的蓝牙网状网络(Bluetooth-Mesh(注册商标))的技术来构建无线LAN200。在该情况下,例如,使作为主设备的一个区块链芯片C连接在网络N,使其他的一个以上的区块链芯片C作为从设备发挥功能。

[0054] 图3是表示通过连接多个图1的区块链芯片就能够实现的分布式AI(人工智能)系统的示意图。

[0055] 根据图1所示的区块链芯片C,能够实现分布式AI(人工智能)系统。

[0056] 现有技术中的AI(人工智能)系统是基于在进行中央处理的单独的服务器等中储存的信息来分析其倾向、并进行各种各样的推测的系统。但是,在使信息储存在单独的服务器等中的情况下,会伴随数据损坏的风险、数据篡改的风险。

[0057] 与此相对,在将图1的区块链芯片C应用到AI(人工智能)系统的情况下,由于多个区块链芯片C分别作为节点发挥功能,所以不需要采用进行中央处理的服务器等。在该情况下,通过增加区块链芯片C的数量,也能够进行超出大型服务器的处理。

[0058] 在此,在AI(人工智能)系统中,被输入的数据本身的准确性是重要的。在现有技术

的AI(人工智能)系统中,通过对储存在单独的服务器等中的数据的数据的后处理来细查可靠性。因此,由于用单独的服务器等处理所输入的多种多样的信息,所以服务器等的负荷变大,有时无法利用CPU进行实时处理。

[0059] 与此相对,根据应用了区块链芯片C的AI(人工智能)系统,能够在区块链芯片C获取数据的感测(sensing)的时刻保证数据的准确性。

[0060] 接下来,参照图4,对应用了图1的区块链芯片C的传感器系统进行说明。

[0061] 图4是表示本发明的信息处理系统的一个实施方式涉及的传感器系统的结构的图。

[0062] 图4所示的传感器系统构成为包含中央复合芯片C1和n个(n为1以上的任意的整数)复合传感器单元U1至Un。

[0063] 在图4的传感器系统中,复合传感器单元U1至Un分别与中央复合芯片C1有线连接。

[0064] 复合传感器单元U1构成为包含传感器侧复合芯片C2-1和m个(m为与n独立的1以上的任意的整数)传感器S1-1至S1-m。

[0065] 复合传感器单元U2构成为包含传感器侧复合芯片C2-2和q个(q为与n、m独立的1以上的任意的整数)传感器S2-1至S2-q。

[0066] 复合传感器单元Un构成为包含传感器侧复合芯片C2-n和r个(r为与n、m、q独立的1以上的任意的整数)的传感器Sn-1至Sn-r。

[0067] 另外,为便于说明,在图4的例子中,中央复合芯片C1设为一个,但是不特别限定于一个,也可以是多个。

[0068] 同样地,为便于说明,在图4的例子中,传感器侧复合芯片C2-1至C2-n设为在复合传感器单元U1至Un中各具有1个,但是不特别限定于各一个,也可以是多个。

[0069] 此外,在不特别需要单独区分各复合传感器单元U1至Un的情况下,将它们统称为“复合传感器单元U”。在称为复合传感器单元U的情况下,将各传感器侧复合芯片C2-1至C2-n统称为“传感器侧复合芯片C2”。

[0070] 此外,在不特别需要单独区分各传感器S1-1至S1-m的情况下,将它们统称为“传感器S1”。

[0071] 同样地,在不特别需要单独区分各传感器S2-1至S2-q的情况下,将它们统称为“传感器S2”。

[0072] 同样地,在不特别需要单独区分各传感器Sn-1至Sn-r的情况下,将它们统称为“传感器Sn”。

[0073] 进而,在不特别需要单独区分各传感器S1至Sn的情况下,将它们统称为“传感器S”。

[0074] 中央复合芯片C1是应用了图1的区块链芯片C的电子设备,其执行作为图4的传感器系统整体的处理。

[0075] 复合传感器单元U是例如具有传感器侧复合芯片C2和传感器S的电路基板。

[0076] 传感器侧复合芯片C2与中央复合芯片C1相同,是应用了图1的区块链芯片C的电子设备,其执行作为复合传感器单元U整体的处理。

[0077] 传感器S是收集某个对象的信息并替换为机器能够处理的信号的元件等,例如是向外部输出对温度、湿度、压力、电流、电压等进行数值化后的数据、或者如图像数据、声音

数据这样的非数值的数据等的各种传感器等。

[0078] 具体而言,例如,传感器侧复合芯片C2执行监控同一复合传感器单元U内所具有的各个传感器S的处理。此外,传感器侧复合芯片C2例如执行对被传感器S检测出的数据进行传输、加工等的处理。

[0079] 在此,图4的数据异常Dm是由于图4的传感器系统受到雷电或静电的放电现象、来自其他电子设备的电磁波噪声等的影响而产生的。在图4的传感器系统中,特别是引发系统的误动作的数据乱码成为问题。

[0080] 在此,所谓“数据乱码”是指在数据传输路径或存储器等中因某种原因导致比特位从原始值反转的现象。

[0081] 但是,引发系统的误动作的原因不限于此。即,例如,除了由于电源电压下降或脉冲噪声、太阳风耀斑等磁暴等引起的数据损坏之外,由传感器S的故障等引起的异常信号输出等也可能引发系统的误动作。本发明的实施方式涉及的图4的传感器系统在针对上述不同的可能成为误动作原因的各种情形防止数据乱码这一方面是非常有效的。

[0082] 而且,在图4的例子中,例如考虑传感器S2-2发生故障的情况。在该情况下,发生故障的传感器S2-2输出异常数据。

[0083] 在这方面,例如,在图4的传感器系统的结构中不具有传感器侧复合芯片C2,仅由中央复合芯片C1管理所有传感器的输入输出等信息的情况下,当传感器S2-2发生故障时,在由于中央复合芯片C1的CPU针对所有的输入输出等信息进行其数据的正确性检查处理,所以导致负荷变大的情况下,多数时候无法迅速地处理传感器S2-2输出的异常数据,无法应对。

[0084] 另一方面,在图4的传感器系统的结构中具有传感器S2、传感器侧复合芯片C2的情况下,当传感器侧复合芯片C2-2检测到传感器S2-2的故障时,通过阻断来自传感器S2-2的异常数据的外部输出等,从而能够防止传感器系统整体的误动作。

[0085] 但是,像这样仅进行数据的分布管理,会产生不具有对雷电或静电的放电现象、来自其他电子设备的电磁波噪声等进行防御的策略的问题。

[0086] 因此,为了解决这样的问题,例如利用区块链技术,采用图5所示的结构的数据作为中央复合芯片C1和传感器侧复合芯片C2之间的传输数据。

[0087] 由此,即使是传感器侧复合芯片C2也能够进行与数据乱码、损坏相关的检查,此外,在实际发现了数据乱码、损坏等情况下能够立即向中央复合芯片C1通知该信息,因此能够防止传感器系统整体的误动作。

[0088] 图5是表示在图4的传感器系统中的中央复合芯片与传感器侧复合芯片之间传输的数据的结构的具体例子的图。

[0089] 从一个传感器侧复合芯片C2向中央复合芯片C1传输的数据的单位是图5所示的传输块B1至B3的每个传输块。

[0090] 在此,在图5中,为便于说明,仅描绘了三个传输块B1至B3,但是实际上存在n个(n为1以上的任意的整数值,理论上不存在其上限)传输块B1至Bn。因此,以下,着眼于第p个(p为1至n中的任意的整数值)传输块Bp进行说明。

[0091] 传输块Bp采用了以下结构:具有包含与传输单位的量对应的实际内容的数据块BDp,在该数据块BDp之前附加第一关联信息HDp,并且在数据块BDp之后附加第二关联信

息FT_p。

[0092] 第一关联信息HD_p是通过利用区块链技术,基于之前收发的前一次的数据块BD(p-1)而生成的。具体而言,例如,第一关联信息HD_p为例如数据块BD(p-1)的哈希值。

[0093] 第二关联信息FT_p是通过利用区块链技术,基于发送对象的本次的数据块BD_p而生成的。具体而言,例如,第二关联信息FT_p为例如数据块BD_p的哈希值。

[0094] 在复合传感器单元U₂中,将本次向复合传感器单元U₁发送的对象的传输块B_p与前一次发送的传输块B(p-1)利用区块链技术进行关联,并存储在规定的存储介质(后述的图6的存储部12等)进行管理。

[0095] 即,在规定的存储介质中,存储各传输块B₁至B_p被连成一串的数据组并进行管理。

[0096] 更具体而言,当着眼于连续的两个传输块B(p-1)、B_p时,根据使前一个传输块B(p-1)所包含的第二关联信息FT(p-1)与本次发送对象的传输块B_p所包含的第一关联信息HD_p一致的规则,传输块B₁至B_p被连成一串。

[0097] 即,传输块B_p的第一关联信息HD_p与前一个传输块B(p-1)的第二关联信息FT(p-1)为同一内容的数据。此外,传输块B_p的第二关联信息FT_p与下一个传输块B(p+1)的第一关联信息HD(p+1)为同一内容的数据。

[0098] 图6是表示图4的传感器系统中的中央复合芯片和传感器侧复合芯片的功能结构的一个例子的图。

[0099] 复合传感器单元U_g(g为1至n中的任意整数)具有传感器S_{g-1}至传感器S_{g-t}(t为与n独立的1以上的任意的整数)和传感器侧复合芯片C_{2-g}。

[0100] 另外,在不特别需要单独区分各个传感器S_{g-1}至传感器S_{g-t}的情况下,将它们统称为“传感器S_g”。

[0101] 传感器侧复合芯片C_{2-g}具有CPU_{1g}和存储部12_g。

[0102] 如图6所示,在传感器侧复合芯片C_{2-g}的CPU_{1g}中,传感器监控部31_g、数据块生成部32_g、第一处理部33_g、第二处理部34_g、确认部35_g、存储控制部36_g、发送控制部37_g、以及接收控制部38_g发挥功能。

[0103] 传感器监控部31_g监控传感器S_g。即,传感器监控部31_g获取与传感器S_g的工作状态相关的数据,基于该数据判断有无异常,在判断为有异常的情况下,生成表示该意思的数据。

[0104] 此外,传感器监控部31_g在判断为传感器S_g的工作状态有异常的情况下,阻断该传感器S_g检测出的信号。

[0105] 数据块生成部32_g生成本次(1至k中的第k次)发送对象的数据(例如从传感器监控部31_g输出的数据)作为数据块BD_k。

[0106] 第一处理部33_g通过利用区块链技术,基于前一次的传输块B(k-1)所包含的数据块BD(k-1)生成第一关联信息HD_k,在数据块BD_k中附加该第一关联信息HD_k。

[0107] 另外,在本实施方式中,第一关联信息HD_k被附加在数据块BD_k的头部的位,但是这仅为示例。即,第一关联信息HD_k的附加位置是任意的,例如也可以采用数据块BD_k的尾部的位置。

[0108] 第二处理部34_g通过利用区块链技术,基于本次的传输块B_k所包含的数据块BD_k生成第二关联信息FT_k,在数据块BD_k中附加该第二关联信息FT_k。

[0109] 另外,在本实施方式中,第二关联信息FTk被附加在数据块BDk的尾部的的位置,但是这仅为示例。即,第二关联信息FTk的附加位置是任意的,例如也可以采用数据块BDk的头部的的位置。

[0110] 确认部35g确认基于数据块BD(k-1)生成的哈希值与第一关联信息HDk是否为同一内容。

[0111] 即,在确认部35g中,如果基于存储在存储部12g的数据块BD(k-1)生成的哈希值与作为数据块BDk的头部而附加的第一关联信息HDk一致,则可知存储在存储部12g的数据块BD(k-1)没有问题。另一方面,在它们不一致的情况下,可以说存储在存储部12g的数据块BD(k-1)产生一些问题的可能性高,在基于此生成了数据块BDk的情况下,数据块BDk也有问题的可能性高。

[0112] 存储控制部36g执行以下控制:将附加了第一关联信息HDk和第二关联信息FTk的数据块BDk作为传输块,利用了区块链技术与包含数据块BD(k-1)的其他传输块进行关联,并存储在规定的存储介质中。

[0113] 即,存储控制部36g执行以下控制:将附加了第一关联信息HDk和第二关联信息FTk的数据块BDk作为传输块,将其与包含数据块BD(k-1)的其他传输块的关联在能够检测到数据乱码的状况下存储在规定的存储介质中。

[0114] 发送控制部37g执行将附加了第一关联信息HDk和第二关联信息FTk的数据块BDk作为利用了区块链技术的传输块来发送的控制。

[0115] 接收控制部38g执行接收从各种硬件(例如、中央复合芯片C1等)发送来的各种信息的控制。

[0116] 接着,对中央复合芯片C1的功能结构的一个例子进行说明。

[0117] 如图6所示,在中央复合芯片C1的CPU21中,接收控制部61、数据监控部62、存储控制部63、以及发送控制部64发挥功能。

[0118] 接收控制部61执行接收从各种硬件(例如传感器侧复合芯片C2等)发送来的各种信息的控制。

[0119] 数据监控部62确认在规定的存储介质(存储部22等)存储的第二关联信息FT(k-1)与第一关联信息HDk是否为同一内容。

[0120] 即,在数据监控部62中,如果在规定的存储介质(存储部22等)存储的第二关联信息FT(k-1)与由接收控制部61接收到的作为数据块BDk的头部而附加的第一关联信息HDk一致,则可知被传输的数据块BDk没有问题。另一方面,在它们不一致的情况下,可以说被传输的数据块BDk产生了一些问题的可能性高。

[0121] 此外,数据监控部62确认基于数据块BDk生成的哈希值与第二关联信息FTk是否为同一内容。

[0122] 即,在数据监控部62中,如果基于数据块BDk生成的哈希值与作为尾部附加在数据块BDk的第二关联信息FTk一致,则可知发送信息没有问题。另一方面,在它们不一致的情况下,可以说发送信息产生了一些问题的可能性高。

[0123] 存储控制部63执行以下控制:将附加了第一关联信息HDk和第二关联信息FTk的数据块BDk作为传输块,利用了区块链技术与包含数据块BD(k-1)的其他传输块进行关联,使其存储在规定的存储介质中。

[0124] 即,存储控制部63执行以下控制:将附加了第一关联信息HDk和第二关联信息FTk的数据块BDk作为传输块,将其与包含数据块BD(k-1)的其他传输块的关联在能够检测到数据乱码的状况下存储在存储部22中。

[0125] 发送控制部64执行将附加了第一关联信息HDk和第二关联信息FTk的数据块BDk作为利用了区块链技术的传输块来发送的控制。

[0126] 在此,以下对上述的实施方式中的传感器系统的具体的应用例进行说明。

[0127] [第一应用例]

[0128] 图4的传感器系统例如能够应用于工厂内的机器人管理。

[0129] 具体而言,例如在复合传感器单元U中设置有检测工厂内的制造机器人的各部位的压力、温度的各种传感器S。

[0130] 该复合传感器单元U内的传感器侧复合芯片C2将这些各种传感器S的检测结果、即工厂内的制造机器人的各部位的压力、温度进行数值化,并生成数据块BDk。

[0131] 传感器侧复合芯片C2通过利用区块链技术,基于前一次的传输块B(k-1)的数据块BD(k-1)生成第一关联信息HDk,在数据块BDk中附加该第一关联信息HDk。

[0132] 传感器侧复合芯片C2通过利用区块链技术,基于本次的数据块BDk来生成第二关联信息FTk,在数据块BDk中附加该第二关联信息FTk。

[0133] 传感器侧复合芯片C2将附加了第一关联信息HDk和第二关联信息FTk的传输块Bk与前一次的传输块B(k-1)利用区块链技术进行关联,使其存储在存储部12等规定的存储介质中。

[0134] 此外,传感器侧复合芯片C2向中央复合芯片C1发送传输块Bk。

[0135] 中央复合芯片C1根据传输块Bk识别将各部位的压力、温度进行了数值化的记录。然后,中央复合芯片C1判断工厂内的制造机器人是否正确地工作。

[0136] 图4的传感器系统通过如这种第一应用例那样应用于工厂内的机器人管理,能够获得如下的第一效果和第二效果。

[0137] 第一效果是指传感器侧复合芯片C2和中央复合芯片C1能够应对制造机器人和传感器的工作不良的效果。

[0138] 第二效果是指传感器侧复合芯片C2和中央复合芯片C1能够检测制造机器人内部的数值的数据乱码或数据损坏,防止工厂内的制造机器人的误动作的效果。

[0139] [第二应用例]

[0140] 图4的传感器系统例如能够应用于例如可使用的空间有限的车辆控制系统、火车控制系统、船舶控制系统等。

[0141] 具体而言,例如在复合传感器单元U中设置有检测对车辆控制系统、火车控制系统、船舶控制系统的车体或船体的振动、倾斜的推定有用的加速度等的各种传感器S。

[0142] 该复合传感器单元U内的传感器侧复合芯片C2将这些各种传感器S的检测结果、即车辆控制系统、火车控制系统、船舶控制系统的加速度等进行数值化,并生成数据块BDk。

[0143] 传感器侧复合芯片C2通过利用区块链技术,基于前一次的传输块B(k-1)的数据块BD(k-1)生成第一关联信息HDk,在数据块BDk中附加该第一关联信息HDk。

[0144] 传感器侧复合芯片C2通过利用区块链技术,基于本次的数据块BDk生成第二关联信息FTk,在数据块BDk中附加该第二关联信息FTk。

[0145] 传感器侧复合芯片C2将附加了第一关联信息HDk和第二关联信息FTk的传输块Bk与前一次的传输块B(k-1)利用区块链技术进行关联,并使其存储在存储部12等规定的存储介质中。

[0146] 此外,传感器侧复合芯片C2向中央复合芯片C1发送传输块Bk。

[0147] 中央复合芯片C1根据传输块Bk来识别工作时的传感器的数值的变化的记录。然后,中央复合芯片C1能够基于传感器S的数值的记录来确认是否正常工作。

[0148] 图4的传感器系统通过如这种第二应用例那样应用于车辆控制系统、火车控制系统、船舶控制系统,能够获得如下效果。

[0149] 该效果是指通过传感器侧复合芯片C2和中央复合芯片C1记录车辆、火车、船舶在工作时的数值的变化来确认数据,并能够运用最合适的控制系统的效果。

[0150] [第三应用例]

[0151] 图4的传感器系统例如能够应用于无人机的数据管理。

[0152] 具体而言,例如在复合传感器单元U中设置有检测GPS坐标、高度等的各种传感器S。

[0153] 该复合传感器单元U内的传感器侧复合芯片C2根据这些各种传感器S的检测结果、即GPS坐标、高度等生成数据块BDk。

[0154] 传感器侧复合芯片C2通过利用区块链技术,基于前一次的传输块B(k-1)的数据块BD(k-1)生成第一关联信息HDk,在数据块BDk附加该第一关联信息HDk。

[0155] 传感器侧复合芯片C2通过利用区块链技术,基于本次的数据块BDk生成第二关联信息FTk,在数据块BDk附加该第二关联信息FTk。

[0156] 传感器侧复合芯片C2将附加了第一关联信息HDk和第二关联信息FTk的传输块Bk与前一次的传输块B(k-1)利用区块链技术进行关联,并使其存储在存储部12等规定的存储介质中。

[0157] 此外,传感器侧复合芯片C2向中央复合芯片C1发送传输块Bk。

[0158] 中央复合芯片C1根据传输块Bk识别GPS坐标、高度等。然后,中央复合芯片C1记录由无人机得到的各种数据,能够进行数据的管理。

[0159] 图4的传感器系统通过如这种第三应用例那样应用于无人机,能够获得如下效果。

[0160] 该效果是指能够基于由传感器侧复合芯片C2和中央复合芯片C1记录的各种数据来进行无人机的搜索、检查。

[0161] [第四应用例]

[0162] 图4的传感器系统例如能够应用于租赁商品的远程操作管理。

[0163] 具体而言,例如在复合传感器单元U中设置有检测操作历史等或故障的征兆的各种传感器S。

[0164] 该复合传感器单元U内的传感器侧复合芯片C2将这些各种传感器S的检测结果、即操作历史等或故障的征兆的数据进行数值化,并生成数据块BDk。

[0165] 传感器侧复合芯片C2通过利用区块链技术,基于前一次的传输块B(k-1)的数据块BD(k-1)生成第一关联信息HDk,在数据块BDk中附加该第一关联信息HDk。

[0166] 传感器侧复合芯片C2通过利用区块链技术,基于本次的数据块BDk来生成第二关联信息FTk,在数据块BDk中附加该第二关联信息FTk。

[0167] 传感器侧复合芯片C2将附加了第一关联信息HDk和第二关联信息FTk的传输块Bk与前一次的传输块B(k-1)利用区块链技术进行关联,并使其存储在存储部12等规定的存储介质中。

[0168] 此外,传感器侧复合芯片C2向中央复合芯片C1发送传输块Bk。

[0169] 中央复合芯片C1根据传输块Bk识别租赁商品的各种数值数据。然后,中央复合芯片C1记录租赁商品的各种数值数据,成为能够远程进行租赁商品的操作管理的状态。

[0170] 图4的传感器系统通过如这种第四应用例那样应用于租赁商品的远程操作管理,能够获得如下效果。

[0171] 该效果是指能够远程地对租赁商品进行操作管理,并能够省去定期点检的麻烦等的效果。

[0172] [第五应用例]

[0173] 图4的传感器系统例如能够应用于游戏机(例如弹球机、街机游戏机)的系统管理。

[0174] 具体而言,例如在复合传感器单元U中设置有获取系统的运行信息的各种传感器S。

[0175] 该复合传感器单元U内的传感器侧复合芯片C2根据这些各种传感器S的检测结果、即游戏机的系统的运行信息来生成数据块BDk。

[0176] 传感器侧复合芯片C2通过利用区块链技术,基于前一次的传输块B(k-1)的数据块BD(k-1)生成第一关联信息HDk,在数据块BDk中附加该第一关联信息HDk。

[0177] 传感器侧复合芯片C2通过利用区块链技术,基于本次的数据块BDk生成第二关联信息FTk,在数据块BDk中附加该第二关联信息FTk。

[0178] 传感器侧复合芯片C2将附加了第一关联信息HDk和第二关联信息FTk的传输块Bk与前一次的传输块B(k-1)利用区块链技术进行关联,并使其存储在存储部12等规定的存储介质中。

[0179] 此外,传感器侧复合芯片C2向中央复合芯片C1发送传输块Bk。

[0180] 中央复合芯片C1根据传输块Bk识别游戏机的系统的运行信息。然后,中央复合芯片C1在区块链记录系统的运行信息,成为能够掌握机体状态的状态。

[0181] 图4的传感器系统通过如这种第五应用例那样应用于游戏机,能够获得如下效果。

[0182] 该效果是指通过在区块链记录系统的运行信息从而保证信用的效果。

[0183] [第六应用例]

[0184] 图7A和图7B是表示将图4的传感器系统应用于汽车的控制的情况的例子的示意图。

[0185] 图7A是表示将图4的传感器系统搭载于汽车M的情况的例子的示意图。

[0186] 像上述的第二应用例那样,在将图4的传感器系统应用于车辆控制、特别是汽车M的控制的情况下,除了上述的效果以外,还能够期待获得例如以下的效果。

[0187] 在现有技术中,作为控制汽车的技术,存在自主型的自动驾驶技术、或通过多个CPU处理从各传感器得到的数据从而执行各种动作的控制的技术。

[0188] 具体而言,例如存在执行汽车的发动机、变速器、动力转向这样的系统的工作的控制的技术、或者执行ABS(Anti-lock Brake System,防抱死制动系统)、汽车间距调整、自动停车这样的辅助用户的工作的控制的技术。此外,也存在像所谓的联网汽车(connected

car)那样通过使汽车作为ICT(信息通信技术)的终端发挥功能从而将各种数据收集在云端进行处理的技术。

[0189] 但是,在与云服务器连接的联网汽车的情况下,由于恶意的第三方从外部入侵(破解),驾驶本身有可能被操控。

[0190] 与此相对,在将使用了区块链芯片C的图4的传感器系统搭载于汽车M的情况下,由于确认来自搭载于汽车M的各传感器的数据的联动性,因此迅速地检测数据的准确性。

[0191] 此外,能够针对每个传感器环境以传感器为单位事先推测或选择数据,因此能够减轻CPU的负荷。其结果,能够实现实时处理。

[0192] 图7B是表示将图4的传感器系统搭载于多辆汽车M的情况的例子的示意图。

[0193] 即,如图7B所示,通过使以区块链芯片C作为节点的云服务器300进行区块链化,能够在所有汽车M中共享地使用通过分布处理而保证了准确性的数据。

[0194] [第七应用例]

[0195] 图4的传感器系统例如能够应用于网络监控摄像机。

[0196] 在现有技术中,存在网络监控摄像机。根据现有技术中存在的网络监控摄像机,能够远程地进行所拍摄的图像的数据的确认、动作检测、面部识别等。

[0197] 但是,由网络监控摄像机拍摄到的图像的数据存在由于恶意的第三方从外部入侵(破解)而导致的数据损坏的风险或数据篡改的风险。

[0198] 与此相对,在将使用了区块链芯片C的图4的传感器系统应用于网络监控摄像机的情况下,能够利用多个网络摄像机进行分布处理化,因此能够实现确保可信赖的数据和数据共享化。也就是说,即使是其他监控摄像机也能够共享某个监控摄像机检测到的数据,因此能够容易地追踪特定的人物。

[0199] 以上对本发明的信息处理系统的各实施方式进行了说明,但本发明不限于上述的本实施方式。此外,本实施方式所记载的效果仅列举了由本发明产生的最优选的效果,本发明的效果并不限于本实施方式所记载的效果。

[0200] 在此,对本发明进行简单的补充。

[0201] 如上所述,在现有的涉及传感器与CPU的信息传输等的系统中,通常由一个或少数的CPU集中管理来自传感器的全部的输出信息。

[0202] 与此相对,为了减少CPU中的数据的正确性检查的处理负荷,例如实施将传感器的管理分成各个部分的分布处理是有效的,但其前提是当前状况下例如在传感器与CPU的信息传输中,存在数据损坏风险严峻的问题。

[0203] 换言之,在当前状况下,在现有的涉及传感器与CPU的信息传输等的系统中,防御由于静电的放电等引起的数据损坏或数据乱码是非常困难的。

[0204] 鉴于像这样的状况,本发明的目的之一在于,为了实现例如计算机中的分布式自治组织(DAO:Distributed Autonomous Organization),提供一种数据的传输和保存的形式,其用于在IoT(Internet of Things,物联网)中使用的传感器等的数据传输中加强数据保护。

[0205] 也就是说,像上述的实施方式那样,在引入了区块链技术的复合芯片中,在具有CPU的中央复合芯片等与一个以上的传感器侧复合芯片之间分布地共享数据的全部或一部分。因此,成为能够迅速地检测由于上述静电的放电现象等引起的数据损坏或数据乱码等

的有力的防御手段,并且能够大幅度降低控制CPU的负荷。

[0206] 另外,作为进一步的应用,例如,通过将DSP(Digital Signal Processor,数字信号处理器)用于芯片,也能够实现低价且大量地生产。

[0207] 例如,在上述的实施方式中,说明了第一关联信息HD可以是块的头部,但是不限于此,能够附加在块的任意位置。

[0208] 同样地,例如,虽然说明了第二关联信息FT可以是块的尾部,但是不限于此,能够附加在块的任意位置。

[0209] 此外,例如,在上述的实施方式中,说明了第一关联信息HD_p为数据块BD(p-1)的哈希值,但是不限于此,只要是基于任意的数据而再现生成的难以预测的值,则能够应用任意的值。

[0210] 同样地,例如,虽然说明了第二关联信息FT_p为数据块BD_p的哈希值,但是不限于此,只要是基于任意的数据而再现地生成的难以预测的值,则能够应用任意的值。

[0211] 此外,例如,在上述的实施方式中,设为传感器侧复合芯片C2和中央复合芯片C1具有CPU,但是能够在CPU中采用能够进行信息处理运算的任意的处理器,除了上述的DSP之外,也可以是GPU(Graphics Processing Unit,图形处理器)等。

[0212] 此外,例如,一般来说在传感器系统等中,由于静电的放电等引起的数据损坏是日常常见的威胁,希望采取一些对策。

[0213] 对于这样的问题,像上述的实施方式那样,通过将传输单位的数据块(例如数据块B_k)进行传输,从而在各种设备等中分布地共享数据,这能够成为有效的对策。也就是说,这是因为,如果能够检测到在各种设备间持有的数据的不匹配,并以一定的准确度推测其是否是真正的数据,则能够使系统整体立即从数据的损坏中恢复。

[0214] 这样的分布共享是在上述的实施方式的传感器系统中,在传感器系统内的所有的中央复合芯片C1和传感器侧复合芯片C2中分布共享数据。

[0215] 通过这样,即使是服务器为一台的系统结构,也能够使数据分布共享,能够降低系统整体进行误动作的风险。

[0216] 进一步而言,通过在传输单位的数据块中附加生成值难以预测的哈希值等,并按照时序进行添加,从而使数据篡改更加困难的区块链的方法对于数据损坏或数据乱码也是有效的。

[0217] 在图4的传感器系统中,因为是传输来自传感器S的数据的元件,所以传感器侧复合芯片C2作为传输源的情况较多。

[0218] 在此,当传感器侧复合芯片C2传输数据时,通过根据前一次发送的或前一次接收到的块即区块链的最末尾的块B(k-1)的数据来生成哈希值,并与作为第二关联信息FT(k-1)附加在该块的哈希值进行对照,从而能够检测是否存在数据损坏或数据乱码。

[0219] 在图4的传感器系统中,可以存在基于前一个数据块BD(k-1)的内容而加上差分来决定最新的数据块BD_k的内容的累积数据。

[0220] 在此情况下,当然,确保在前一个数据块中没有数据损坏或数据乱码是重要的。

[0221] 但是,与此同时,存在即使前两个以上的数据块B(1至k-2)发生数据损坏或数据乱码也没有不妥的情况。

[0222] 在该情况下,仅对一个数据块进行哈希值的对照即可,因此可以认为即使传感器

侧复合芯片C2不具有高运算能力也不成问题。

[0223] 另一方面,对于检测到前一个数据的损坏或数据乱码的情况,可以通过利用区块链技术恢复数据的真正性。

[0224] 具体而言,用分布共享的所有区块链来生成前一个数据块B(k-1)的哈希值并进行对照,发现没有数据损坏或数据乱码的数据块,基于此来覆盖数据被损坏的数据块。

[0225] 在上述的图4的传感器系统的一个实施方式中,优选采用图5所示的数据结构。

[0226] 此外,例如在上述的实施方式中,说明了数据块生成部32g将本次的发送对象的数据作为数据块BDk来生成,但是不特别限定。即,数据块生成部32g也可以在任意时刻生成数据块BDk。

[0227] 具体而言,例如,数据块生成部32g既可以在获取到由传感器监控部31g取得的数据的时刻生成数据块BDk,也可以按每个规定的时间生成数据块BDk。

[0228] 由此,数据块生成部32g能够在任意时刻生成数据块BDk,因此能够减轻CPU11g的负荷。

[0229] 另外,对于数据块生成部32m,也是一样的。

[0230] 此外,图1和图4所示的系统结构和硬件结构仅为用于达到本发明的目的的示例,不特别限定。

[0231] 此外,图5所示的数据结构仅为用于达到本发明的目的的示例,不特别限定。

[0232] 此外,图6所示的功能框图仅为示例,不特别限定。即,只要系统具有能够作为整体执行上述一系列处理的功能即可,为了实现此功能而使用什么样的功能块,并不特别限定于图6的例子。

[0233] 此外,功能块的储存位置也不限定于图6,可以为任意位置。

[0234] 此外,一个功能块既可以由单个硬件结构,也可以由单个软件构成,还可以由软件和硬件的组合构成。

[0235] 在通过软件执行各功能块的处理的情况下,构成该软件的程序从网络、存储介质安装到计算机等。

[0236] 计算机可以是组装在专用的硬件的计算机。此外,计算机是通过安装各种程序从而能够执行各种功能的计算机,例如是服务器以外的通用的智能手机、个人电脑。

[0237] 含有这种程序的存储介质不仅由为了向用户提供程序而与装置主体分开配置的未图示的可移动介质构成,也可以由以预先组装在装置主体的状态提供给用户的存储介质等构成。可移动介质由例如磁盘(包括软盘)、光盘或磁光盘等构成。光盘由例如CD-ROM(Compact Disk-Read Only Memory,光盘只读存储器)、DVD(Digital Versatile Disk,数字多用光盘)等构成。磁光盘由MD(Mini-Disk,小型磁盘)等构成。此外,以预先组装在装置主体的状态提供给用户的存储介质由例如记录有程序的未图示的ROM、在图6的存储部22等中包含的硬盘等构成。

[0238] 另外,在本说明书中,描述记录在存储介质中的程序的步骤不仅包括按照其顺序时序地进行的处理,还包括即使不一定时序地处理而是并行或单独执行的处理。

[0239] 此外,在本说明书中,术语“系统”的意思是由多个装置、多个单元等构成的整体装置。

[0240] 综上所述,应用本发明的电子设备采用如下的结构即可,能够采用各种各样的实

施方式。

[0241] 即,应用本发明的电子设备(例如图1等区块链芯片C)具有:

[0242] 生成单元(例如图6的数据块生成部32g),其基于规定的信息(传感器信息等),按每个规定的单位生成数据;

[0243] 第一处理单元(例如图6的第一处理部33g),其将由所述生成单元生成的处理对象的所述单位的数据作为第一单位数据(例如图5的数据块BD2),将在此之前由所述生成单元生成的所述单位的数据作为第二单位数据(例如图5的数据块BD1),生成至少包含根据该第二单位数据得到的哈希值的信息作为第一关联信息(例如图5的第一关联信息HD2),将该第一关联信息附加在处理对象的所述第一单位数据(例如图5的数据块BD2)中;

[0244] 第二处理单元(例如图6的第二处理部34g),其生成至少包含根据所述第一单位数据(例如图5的数据块BD2)得到的哈希值的信息作为第二关联信息(例如图5的第二关联信息FT2),将该第二关联信息附加在处理对象的所述第一单位数据(例如图5的数据块BD2)中;以及

[0245] 存储控制单元(例如图6的存储控制部36g),其执行如下控制,即,利用区块链技术将附加了所述第一关联信息(例如图5的第一关联信息HD2)和所述第二关联信息(例如图5的第二关联信息FT2)的处理对象的所述第一单位数据(例如图5的数据块BD2)与包含所述第二单位数据(例如图5的数据块BD1)的一个以上的其他所述单位的数据(例如图5的数据块BD3)进行关联,并存储在规定的存储介质(例如图6的存储部12g)中。

[0246] 由此,能够在系统的各部分布地检测记录数据的损坏或数据乱码,因此能够提供一种能够进一步降低传输数据时的数据损坏风险的技术。

[0247] 即,能够在引入了区块链技术的复合芯片中,在具有控制CPU的中央复合芯片等与一个以上的传感器侧复合芯片之间在整体上分布共享数据,成为能够迅速地检测由于静电的放电现象等引起的数据损坏或数据乱码的有力的防御手段,并且能够大幅度降低控制CPU的负荷。

[0248] 此外,能够具有:发送控制单元(例如图3的发送控制部37g),其执行将附加了所述第一关联信息(例如图2的第一关联信息HD2)和所述第二关联信息(例如图2的第二关联信息FT2)的所述第一单位数据(例如图2的数据块BD2)发送至其他的电子设备的控制。

[0249] 由此,能够进行电子设备间的数据共享。

[0250] 此外,还能够具有:获取单元(例如图1的通信部14),其从外部获取使所述第一处理单元、所述第二处理单元、以及所述存储控制单元发挥功能的程序(例如区块链主体);以及

[0251] 存储单元(例如图1的非易失性存储器(高速缓冲存储器)121),其存储从外部获取的所述程序(例如区块链主体)。

[0252] 由此,能够总是加载最新版的区块链主体。

[0253] 此外,还能够具有电力获取单元(例如图1的电力获取部17),其获取使本机驱动的电力。

[0254] 由此,能够使电子设备单独驱动。

[0255] 此外,应用本发明的信息处理系统构成为包含多个上述电子设备。

[0256] 由此,能够将由多个电子设备构成的信息处理系统应用于各种场景。

[0257] 此外,多个所述电子设备分别能够向其他的所述电子设备发送与车辆的操作相关的数据。

[0258] 由此,能够将由多个电子设备构成的信息处理系统应用于例如汽车的操作的控制。

[0259] 此外,多个所述电子设备分别能够向其他的所述电子设备发送所拍摄的图像的数据。

[0260] 由此,能够将由多个电子设备构成的信息处理系统应用于例如多个监控摄像机的控制。

[0261] 附图标记说明

[0262] C:区块链芯片

[0263] C1:中央复合芯片

[0264] C2-1至C2-n:传感器侧复合芯片

[0265] N:网络

[0266] M:汽车

[0267] U1至Un:复合传感器单元

[0268] 11:CPU

[0269] 12:存储部

[0270] 13:复位按钮

[0271] 14:通信部

[0272] 15:指示器

[0273] 16:标识器

[0274] 17:电力获取部

[0275] 21:CPU

[0276] 22:存储部

[0277] 31:传感器监控部

[0278] 32:数据块生成部

[0279] 33:第一处理部

[0280] 34:第二处理部

[0281] 35:确认部

[0282] 36:存储控制部

[0283] 37:发送控制部

[0284] 38:接收控制部

[0285] 61:接收控制部

[0286] 62:数据监控部

[0287] 63:存储控制部

[0288] 64:发送控制部

[0289] 71:HUB

[0290] 121:非易失性存储器(高速缓冲存储器)

[0291] 100:有线LAN

- [0292] 122:易失性存储器 (RAM)
- [0293] 141:LAN端子
- [0294] 142:输入输出 (I/O) 端口
- [0295] 143:蓝牙 (注册商标) 天线
- [0296] 200:无线LAN
- [0297] 300:云服务器

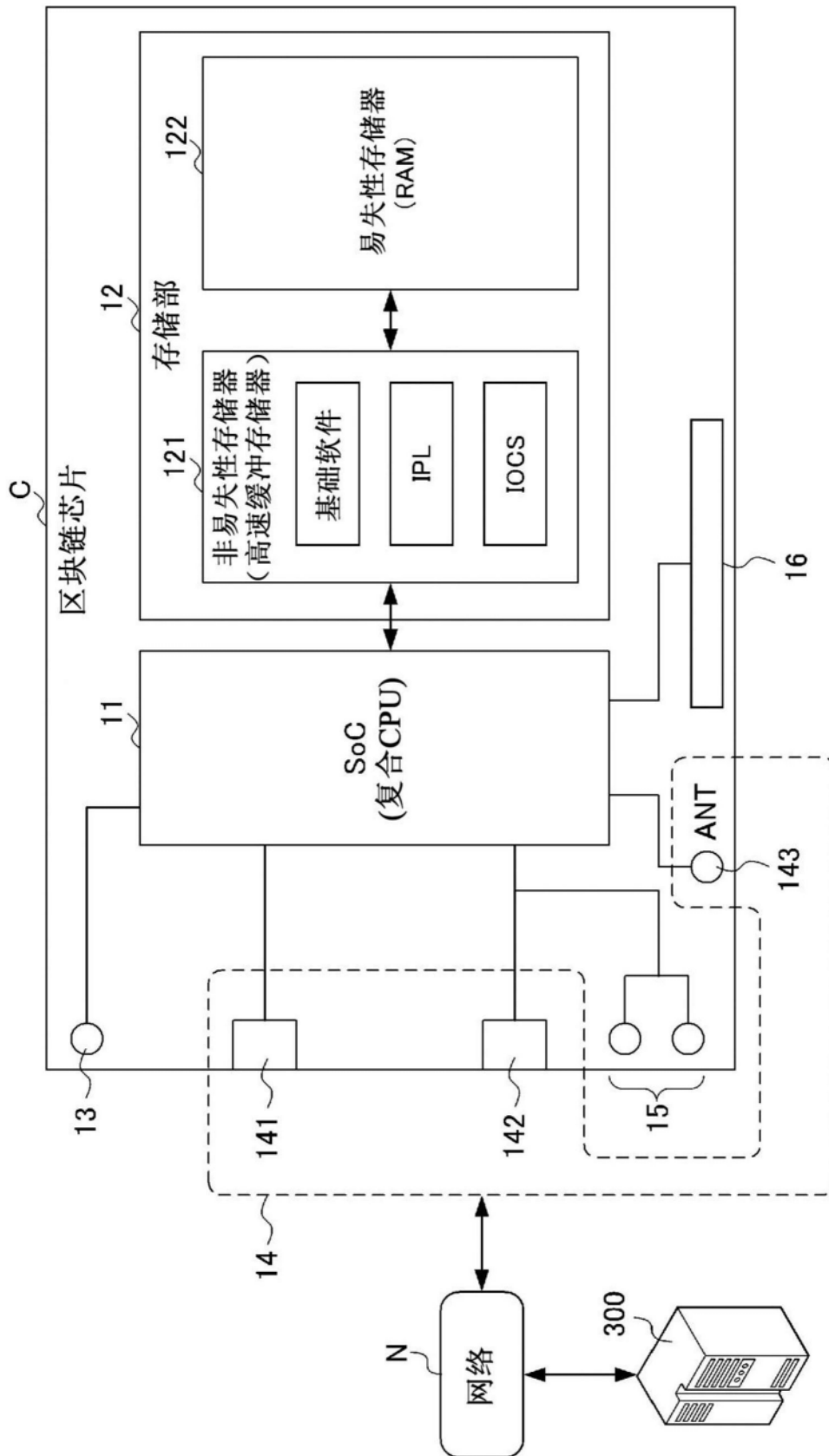


图1

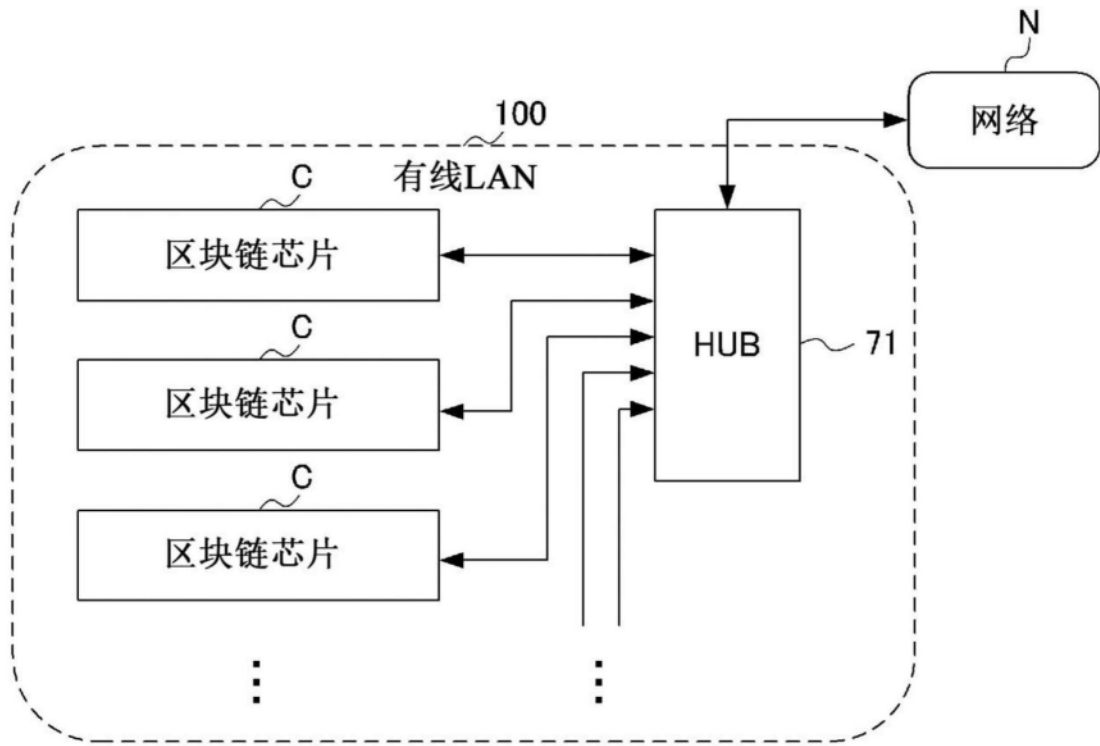


图2A

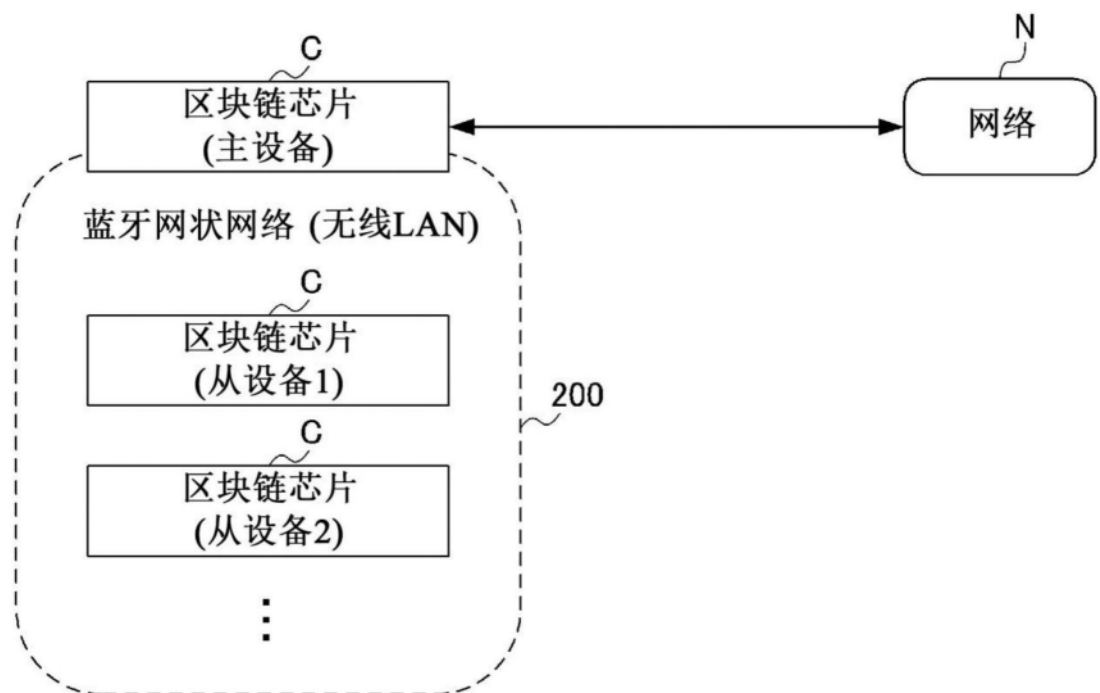


图2B

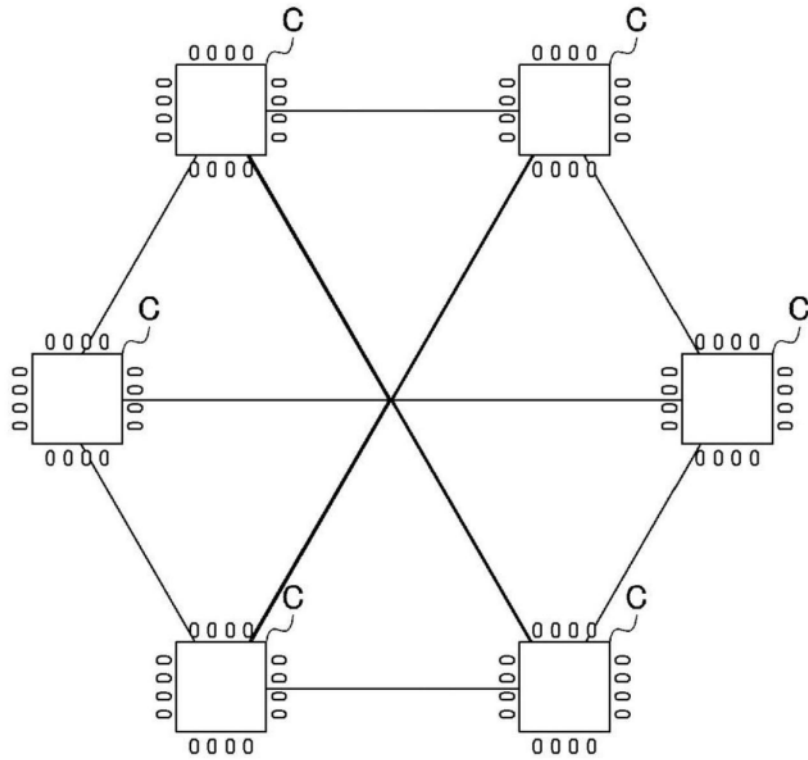


图3

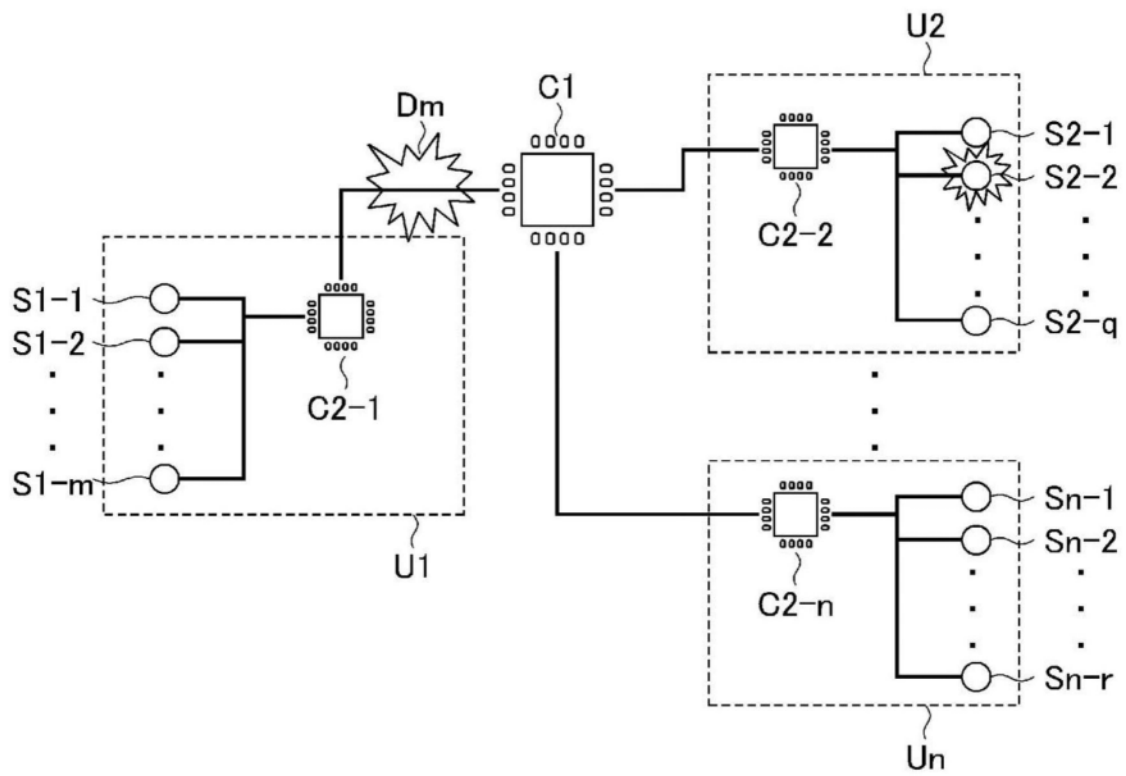


图4

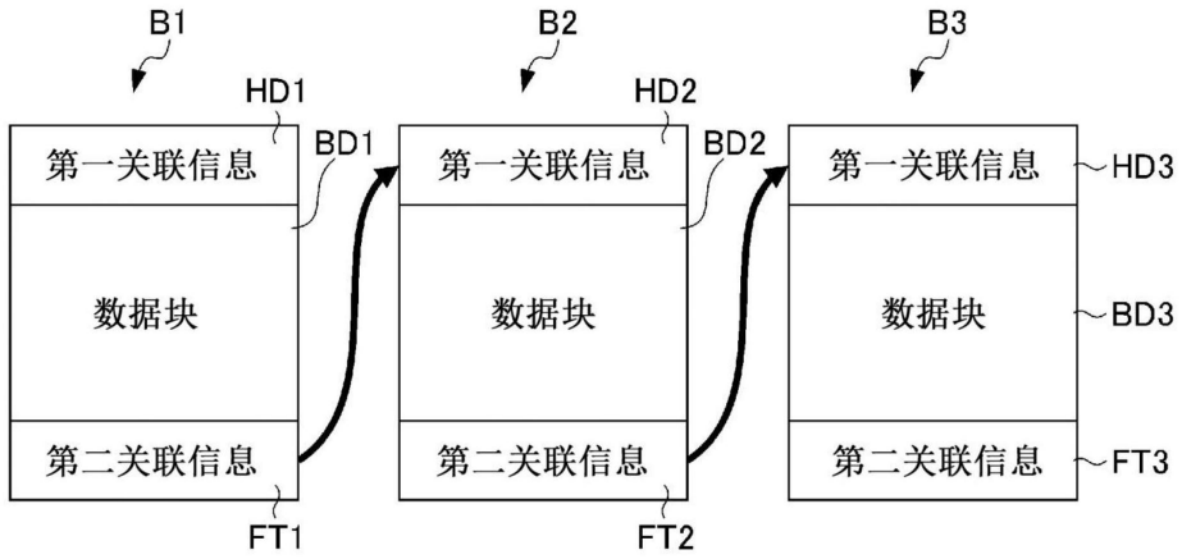


图5

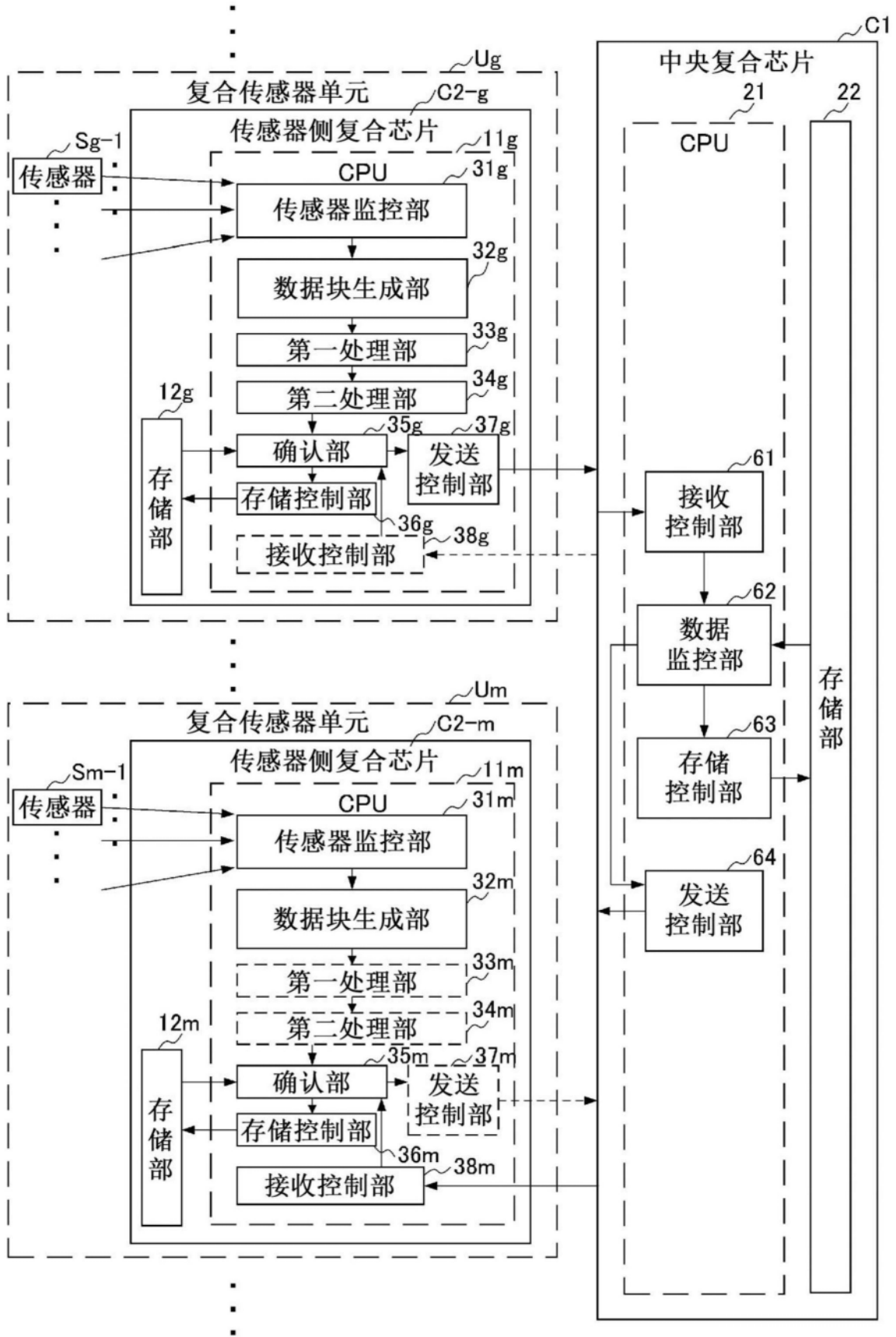


图6

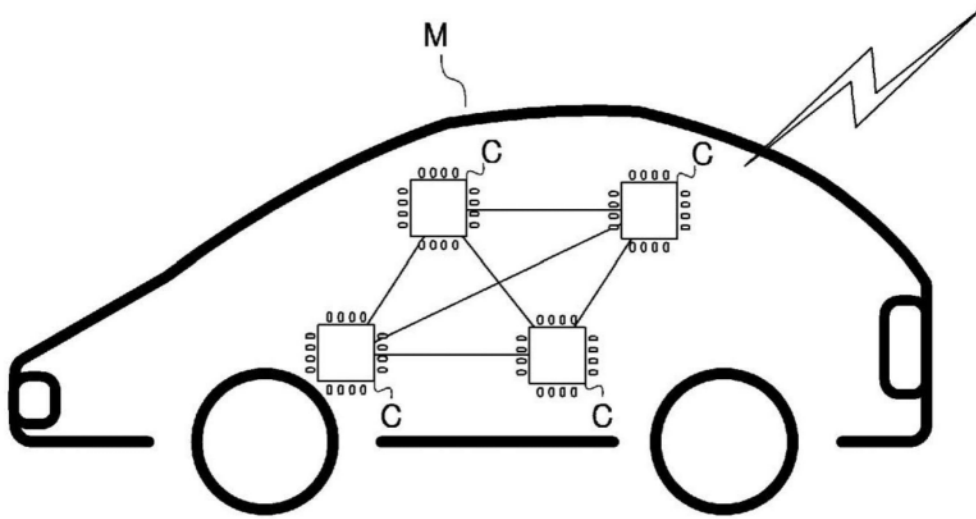


图7A

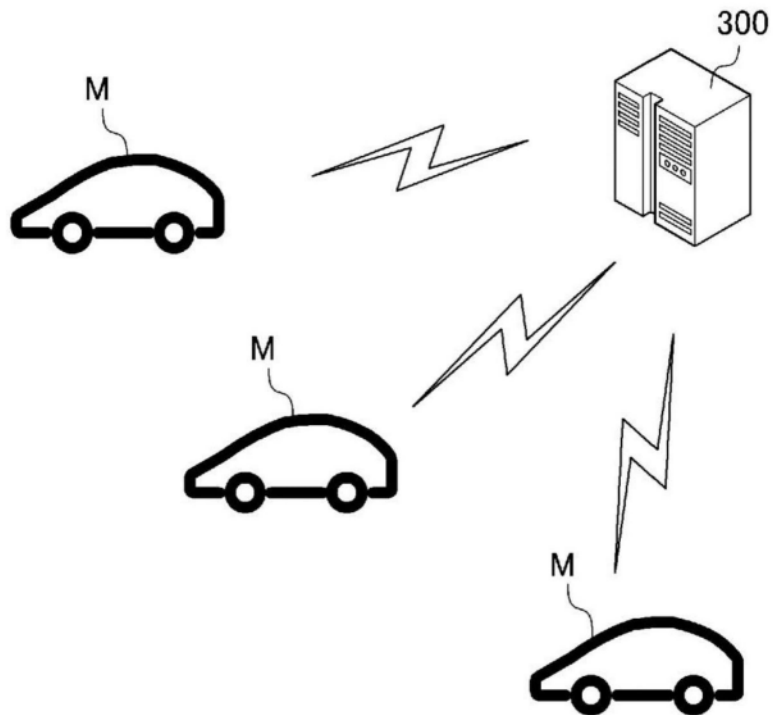


图7B