(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102148821 A
(43)申请公布日 2011.08.10

(21)申请号 201110024380.9

(22)申请日 2011.01.18

(30)优先权数据
2010-013672 2010.01.25 JP

(71)申请人 索尼公司
地址 日本东京都

(72)发明人 松田诚一 坚木雅宣 吉田亚左实
浅野智之 盛合志帆 浮田昌一
川元洋平 田中雄

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 杜诚 李春晖

(51)Int.Cl.
H04L 29/06(2006.01)

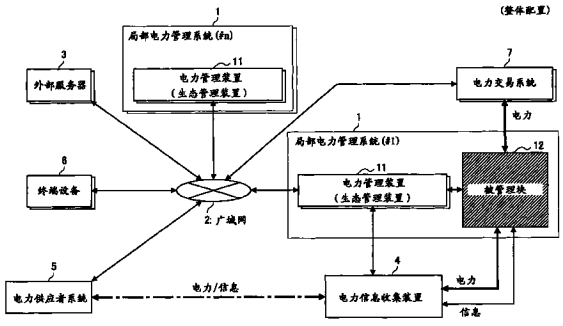
权利要求书 2 页 说明书 85 页 附图 80 页

(54)发明名称

电力管理装置、电子设备以及注册电子设备的方法

(57)摘要

公开了一种电力管理装置、电子设备以及注册电子设备的方法。电力管理装置包括：被管理设备注册单元，其对连接到电力网络的电子设备执行认证，并且将认证成功的电子设备注册为被管理设备；以及控制单元，其控制被管理设备的操作以及对被管理设备的电力供给。在把已经注册在另一个电力管理装置中的电子设备连接到电力网络时，从该电子设备获得数字签名和对于该另一个电力管理装置唯一的标识信息，该数字签名被该另一个电力管理装置分配给对于该电子设备唯一的标识信息，在由该另一个电力管理装置分配的数字签名的验证成功时，临时注册在该另一个电力管理装置中注册的该电子设备。



CN 102148821 A

1. 一种电力管理装置，包括：

被管理设备注册单元，其对连接到电力网络的电子设备执行认证，并且将认证成功的电子设备注册为被管理设备；以及

控制单元，其控制所述被管理设备的操作以及对所述被管理设备的电力供给，

其中，所述被管理设备注册单元

能够进行操作以在把已经注册在另一个电力管理装置中的电子设备连接到所述电力网络时，从所述电子设备获取数字签名和对于所述另一个电力管理装置唯一的标识信息，所述数字签名被所述另一个电力管理装置分配给对于所述电子设备唯一的标识信息，并且

能够进行操作以在由所述另一个电力管理装置分配的所述数字签名的验证成功时，临时注册在所述另一个电力管理装置中注册的所述电子设备。

2. 如权利要求 1 所述的电力管理装置，还包括：

电力使用证书管理单元，其管理由在所述另一个电力管理装置中注册的所述电子设备生成的、并且证实已经接收到从临时注册所述电子设备的所述电力管理装置提供的电力的电力使用证书，

其中所述电力使用证书管理单元

能够进行操作以在所述控制单元已经向所述临时注册的电子设备提供电力时，从所述临时注册的电子设备获取所述电力使用证书，并且

向所获取的电力使用证书分配数字签名，然后将分配了所述数字签名的所述电力使用证书发送给为电力使用计费的外部服务器。

3. 如权利要求 2 所述的电力管理装置，

其中，所述电力使用证书管理单元能够进行操作以在所述电力管理装置已经接收到从所述电子设备提供的电力时，针对接收到的所提供的电力所来自于的所述电子设备生成电力使用证书，所述电力使用证书证实所提供的电力接收自所述电子设备。

4. 一种电子设备，包括：

存储单元，其存储对于所述电子设备唯一的标识信息和已经被指定的证书机构认证的数字签名；以及

认证处理单元，其使用所述存储单元中存储的所述数字签名，与管理对所述电子设备的电力提供的电力管理装置执行认证处理，并且在所述电力管理装置中注册所述电子设备，

其中，所述认证处理单元能够进行操作以在所述电子设备已经被注册在所述电力管理装置中时，从已经注册了所述电子设备的所述电力管理装置获取对于所述电力管理装置唯一的标识信息以及所述电力管理装置已经分配给对于所述电子设备唯一的标识信息的数字签名。

5. 如权利要求 4 所述的电子设备，

其中，所述认证处理单元能够进行操作以在向除已经注册了所述电子设备的所述电力管理装置之外的电力管理装置请求临时注册时，把从已经注册了所述电子设备的所述电力管理装置获取的所述数字签名发送给已被请求临时注册的所述电力管理装置。

6. 如权利要求 5 所述的电子设备，还包括：

控制单元，其能够进行操作以在从临时注册所述电子设备的所述电力管理装置接收到

所提供的电力时生成电力使用证书，所述电力使用证书证实所提供的电力接收自临时注册所述电子设备的所述电力管理装置。

7. 一种注册电子设备的方法，包括：

对连接到电力网络的电子设备执行认证，并将所述认证已成功的电子设备注册为被管理设备的步骤，

其中，执行认证的步骤使用由所述电子设备存储并且已经被指定的证书机构认证的数字签名，

能够进行操作以在所述电子设备已经被注册在所述电力管理装置中时，从所述电力管理装置向所述电子设备发送对于所述电力管理装置唯一的标识信息以及所述电力管理装置已经分配给对于所述电子设备唯一的标识信息的数字签名，

能够进行操作以在将已经被注册在另一个电力管理装置中的电子设备连接到所述电力网络时，从所述电子设备获取已经由所述另一个电力管理装置分配给对于所述电子设备唯一的标识信息的数字签名，和对于所述另一个电力管理装置唯一的标识信息，并且

能够进行操作以在由所述另一个电力管理装置分配的所述数字签名的验证成功时，临时注册在所述另一个电力管理装置中注册的所述电子设备。

电力管理装置、电子设备以及注册电子设备的方法

技术领域

[0001] 本发明涉及电力管理装置、电子设备和注册电子设备的方法。

背景技术

[0002] 近年来，被称为智能电网的技术一直受到关注。智能电网是通过与传输网一起构建具有通信信道的新传输网并且使用该智能传输网来实现高效的电力使用的技术框架。智能电网的背景思想是实现电力使用量的有效管理，当意外事件发生时迅速处理这种意外事件，远程控制电力使用量，使用电力公司控制之外的发电设施的分布式发电，或者电动交通工具的充电管理。特别地，由普通家庭或除电力公司之外的操作者使用可再生能源对室内发电站的高效利用以及通常包括电动汽车的多种电动交通工具的充电管理已经引起高度关注。顺便提及，可再生能源是在不使用矿物燃料的情况下生成的能源。

[0003] 由普通家庭或除电力公司之外的操作者生成的电力由发电操作者使用。发电操作者使用之后剩余的电力目前由电力公司购买。然而，购买由电力公司控制之外的发电设施提供的电力对于电力公司来说是很重的负担。例如，由光电发电设施提供的电力量取决于天气。而且，由普通家庭的室内发电站提供的电力量取决于逐日较大地改变的普通家庭的电力使用。从而，对于电力公司来说，难以从电力公司控制之外的发电设施接收稳定电力供应。由于以上原因，电力公司在未来购买电力可能变得困难。

[0004] 从而，在将由电力公司控制之外的发电设施生成电力临时存储在蓄电池中之后使用该电力的家庭蓄电池计划 (home battery initiative) 近来已经引起关注。例如，考虑通过将由光电发电设施生成的电力存储在蓄电池中并且补偿在夜晚或者当天气不好时的缺乏来使用这种电力的方法。而且，考虑根据电池存储量限制从电力公司接收的电力量，或者通过将电力公司在电费较低的夜晚提供的电力存储在蓄电池中而在电费较高的白天使用存储在蓄电池中的电力的方法。而且，蓄电池能够将电力存储为 DC，这使得在传输期间无需 DC/AC 转换或 AC/DC 转换，从而可以减少转换过程中的损失。

[0005] 从而，关于电力管理的多种期望相互混合在智能电网计划中。为了实现这种电力管理，智能电网计划的前提是除传输网之外还要具有通信信道。也就是说，假设通过使用该智能传输网来交换关于电力管理的信息 (例如，参见 JP-A-2002-354560)。然而，在已经建造了通信基础设施的区域中，可以不使用传输网作为通信信道，而是通过使用由所部署的通信基础设施构建的网络来交换关于电力管理的信息。也就是说，在智能电网计划中，重要的是如何有效地管理未被统一管理的发电设施和存储设施。

发明内容

[0006] 然而，在实际生活中存在各种情况，例如当用户把电子设备带出家以在家外的某个位置使用时，某个电子设备由于用户的移动而移动到不同位置。相应地，对于例如前面描述的智能网格概念，可能存在这样的情况 ：期望把已经由某个装置进行电力管理的电子设备临时连接到管理电力的不同装置。

[0007] 然而，尚未提出用于把已经由某个装置进行电力管理的电子设备临时注册到另一装置中的方案。

[0008] 本发明是考虑到上述问题而构思的，并且目标是提供一种电力管理装置、电子设备和注册电子设备的方法，其能够把已经由某个装置进行电力管理的电子设备临时注册在另一装置中。

[0009] 根据本发明一个实施例，提供一种电力管理装置，包括：被管理设备注册单元，其对连接到电力网络的电子设备执行认证，并且将认证成功的电子设备注册为被管理设备，以及控制单元，其控制被管理设备的操作以及对被管理设备的电力供给。被管理设备注册单元能够进行操作以在把已经注册在另一个电力管理装置中的电子设备连接到电力网络时，从该电子设备获取数字签名和对于另一个电力管理装置唯一的标识信息，该数字签名被该另一个电力管理装置分配给对于该电子设备唯一的标识信息，并且被管理设备注册单元能够进行操作以在由该另一个电力管理装置分配的数字签名的验证成功时，临时注册在该另一个电力管理装置中注册的该电子设备。

[0010] 电力管理装置还可以包括：电力使用证书管理单元，其管理由注册在该另一个电力管理装置中的该电子设备生成的、并且证实已经接收到从该电子设备临时注册的该电力管理装置提供的电力的电力使用证书。电力使用证书管理单元可以能够进行操作以在控制单元已经向该临时注册的电子设备提供电力时，从该临时注册的电子设备获取电力使用证书，并且可以向所获取的电力使用证书分配数字签名，然后把分配了该数字签名的电力使用证书发送给为电力使用计费的外部服务器。

[0011] 电力使用证书管理单元可以能够进行操作以在该电力管理装置已经接收到从该电子设备提供的电力时，针对所接收到的提供的电力来自于的电子设备生成电力使用证书，该电力使用证书证实从该电子设备接收所提供的电力。

[0012] 根据本发明另一个实施例，提供一种电子设备，包括：存储单元，其存储对于该电子设备唯一的标识信息和已经由指定证书机构认证的数字签名；以及认证处理单元，其使用存储单元中存储的数字签名与管理对电子设备的电力提供的电力管理装置执行认证处理，并且在该电力管理装置中注册该电子设备。认证处理单元能够进行操作以在该电子设备已经被注册在该电力管理装置中时，从已经注册了该电子设备的该电力管理装置获取对于该电力管理装置唯一的标识信息和该电力管理装置已经分配给对于该电子设备唯一的标识信息的数字签名。

[0013] 认证处理单元可以能够进行操作以在向除已经注册了该电子设备的该电力管理装置之外的电力管理装置请求临时注册时，把从已注册了该电子设备的该电力管理装置获取的数字签名发送给已被请求临时注册的电力管理装置。

[0014] 电子设备还可以包括控制单元，其能够进行操作以在从已临时注册了该电子设备的电力管理装置接收所提供的电力时，生成电力使用证书，其证实从临时注册了该电子设备的该电力管理装置接收所提供的电力。

[0015] 根据本发明另一个实施例，提供一种注册电子设备的方法，包括步骤：对连接到电力网络的电子设备执行认证，以及将认证成功的电子设备注册为被管理设备。执行认证的步骤使用由电子设备存储并且已经由指定证书机构认证的数字签名，能够进行操作以在电子设备已经被注册在电力管理装置中时，从该电力管理装置向该电子设备发送对于该电力

管理装置唯一的标识信息和该电力管理装置已经分配给对于该电子设备唯一的标识信息的数字签名，能够进行操作以在把已经被注册在另一个电力管理装置中的电子设备连接到电力网络时，从该电子设备获取该另一个电力管理装置已经分配给对于该电子设备唯一的标识信息的数字签名和对于该另一个电力管理装置唯一的标识信息，并且能够进行操作以在由该另一个电力管理装置分配的数字签名的验证成功时，临时注册在该另一个电力管理装置中注册的该电子设备。

[0016] 根据前面描述的本发明实施例，可以把已经由某个电力管理装置进行电力管理的电子设备临时注册在另一电力管理装置中。

附图说明

[0017] 图 1 是用于说明根据本发明的实施例的电力管理系统的概况的图；

[0018] 图 2 是用于说明被管理块的整体配置的图；

[0019] 图 3 是用于说明局部电力管理系统中的通信网络的图；

[0020] 图 4 是用于说明以电力管理装置为中心的系统配置的图；

[0021] 图 5 是用于说明外部服务器的具体示例的图；

[0022] 图 6 是用于说明系统管理服务器的一个功能的图；

[0023] 图 7 是用于说明根据本发明的实施例的电力管理装置的功能配置的图；

[0024] 图 8 是用于说明信息管理单元的详细功能配置的图；

[0025] 图 9 是用于说明信息管理单元的详细功能配置的表格；

[0026] 图 10 是用于说明显示在显示单元上的内容的图；

[0027] 图 11 是用于说明显示在显示单元上的内容的图；

[0028] 图 12 是用于说明显示在显示单元上的内容的图；

[0029] 图 13 是用于说明显示在显示单元上的内容的图；

[0030] 图 14 是用于说明电力消费的时间序列模式的图表；

[0031] 图 15 是用于说明电力消费的时间序列模式的图表；

[0032] 图 16 是用于说明隐藏电力消费模式的方法的图；

[0033] 图 17 是用于说明隐藏电力消费模式的方法的图；

[0034] 图 18 是用于说明隐藏电力消费模式的方法的图；

[0035] 图 19 是用于说明由电力管理装置执行的多种控制的图；

[0036] 图 20 是用于说明由电力管理装置管理的多种信息的图；

[0037] 图 21 是示出根据插座的类型和所连接设备的类型的通信装置、认证装置以及对供电的控制的组合的表格；

[0038] 图 22 是示出设备管理单元的配置的框图；

[0039] 图 23 是示出被管理设备注册单元的配置的框图；

[0040] 图 24 是示出信息篡改检测单元的配置的框图；

[0041] 图 25 是示出信息分析单元的配置的框图；

[0042] 图 26 是示出可控制设备的配置的框图；

[0043] 图 27 是示出可控制设备的控制单元的配置的框图；

[0044] 图 28 是示出可控制设备的控制单元的配置的框图；

[0045] 图 29 是示出篡改检测信息生成单元的配置的框图；

[0046] 图 30 是示出电力存储装置的配置的框图；

[0047] 图 31 是示出电力存储装置的控制单元的配置的框图；

[0048] 图 32 是示出电力存储装置的控制单元的配置的框图；

[0049] 图 33 是示出篡改检测信息生成单元的配置的框图；

[0050] 图 34 是用于说明注册电力管理装置的方法的流程图；

[0051] 图 35 是用于说明注册电力管理装置的方法的具体示例的流程图；

[0052] 图 36 是用于说明注册可控制设备的方法的流程图；

[0053] 图 37 是用于说明注册可控制设备的方法的具体示例的流程图；

[0054] 图 38 是用于说明注册可控制设备的方法的具体示例的流程图；

[0055] 图 39 是用于说明注册可控制插座的方法的流程图；

[0056] 图 40 是用于说明已经被临时注册的可控制设备的记账处理的图；

[0057] 图 41 是用于说明已经被临时注册的可控制设备的记账处理的流程图；

[0058] 图 42 是用于说明对注册可控制设备的方法的修改的图；

[0059] 图 43 是用于说明对注册可控制设备的方法的修改的图；

[0060] 图 44 是用于说明对注册可控制设备的方法的修改的图；

[0061] 图 45 是用于说明对注册可控制设备的方法的修改的图；

[0062] 图 46 是用于说明对注册可控制设备的方法的修改的图；

[0063] 图 47 是用于说明对注册可控制设备的方法的修改的图；

[0064] 图 48 是用于说明对注册可控制设备的方法的修改的图；

[0065] 图 49 是用于说明电力管理装置对于发生了异常的被管理设备的操作的流程图；

[0066] 图 50 是用于说明电力管理装置对于发生了异常的被管理设备的操作的流程图；

[0067] 图 51 是用于说明电力管理装置对于发生了异常的被管理设备的操作的流程图；

[0068] 图 52 是用于说明电力管理装置对于发生了异常的被管理设备的操作的流程图；

[0069] 图 53 是用于说明当在电力状态中发生异常时，电力管理装置的操作的流程图；

[0070] 图 54 是用于说明当在电力状态中发生异常时，电力管理装置的操作的流程图；

[0071] 图 55 是用于说明嵌入电子水印信息的方法的流程图；

[0072] 图 56 是用于说明验证电子水印信息的方法的流程图；

[0073] 图 57 是用于说明嵌入电子水印信息的方法的流程图；

[0074] 图 58 是用于说明验证电子水印信息的方法的流程图；

[0075] 图 59 是用于说明分析服务器的配置的框图；

[0076] 图 60 是示出分析服务器的信息篡改检测单元的配置的框图；

[0077] 图 61 是示出分析服务器的第一验证单元的配置的框图；

[0078] 图 62 是示出分析服务器的第二验证单元的配置的框图；

[0079] 图 63 是用于说明待排除蓄电池的图；

[0080] 图 64 是用于说明保护电力管理装置免受非法攻击的方法的流程图；

[0081] 图 65 是用于说明排除蓄电池的方法的流程图；

[0082] 图 66A 是用于说明通过分析服务器的获取数据验证单元进行验证的方法的流程图；

[0083] 图 66B 是用于说明通过分析服务器的获取数据验证单元进行验证的方法的流程图；

[0084] 图 67 是用于说明第一验证单元的验证处理的流程图；

[0085] 图 68 是用于说明由数据库管理单元进行的测试处理的流程图；

[0086] 图 69 是用于说明由数据库管理单元更新数据库并且生成判断词典的图；

[0087] 图 70 是用于说明由病毒定义文件管理单元管理病毒定义文件的方法的流程图；

[0088] 图 71A 是用于说明由获取数据验证单元执行以指定待排除蓄电池的方法的流程图；

[0089] 图 71B 是用于说明由获取数据验证单元执行以指定待排除蓄电池的方法的流程图；

[0090] 图 71C 是用于说明由获取数据验证单元执行以指定待排除蓄电池的方法的流程图；

[0091] 图 72 是用于说明由获取数据验证单元执行以指定待排除蓄电池的方法的流程图；

[0092] 图 73 是用于说明多个电力管理装置的操作流程的图；

[0093] 图 74 是用于说明多个电力管理装置的操作流程的图；

[0094] 图 75 是用于说明多个电力管理装置的操作流程的图；

[0095] 图 76 是用于说明电力管理装置的服务提供单元的配置的框图；

[0096] 图 77 是用于说明电力管理装置的服务提供单元的配置的框图；

[0097] 图 78 是用于说明到电力管理装置中的数据库的链接的图；

[0098] 图 79 是用于说明关于链接系统的娱乐的安全性的图；

[0099] 图 80 是用于说明链接系统的娱乐的流程的流程图；

[0100] 图 81A 是用于说明链接系统的娱乐的流程的流程图；

[0101] 图 81B 是用于说明链接系统的娱乐的流程的流程图；以及

[0102] 图 82 是用于说明根据本发明的实施例的电力管理装置的硬件配置的框图。

具体实施方式

[0103] 此后，将参考附图详细地描述本发明的优选实施例。注意，在本说明书和所附附图中，用相同附图标记表示具有基本相同功能和结构的结构元件，并且省略这些结构元件的重复说明。

[0104] 按以下指出的顺序给出以下描述。

[0105] (1) 第一实施例

[0106] (1-1) 电力管理装置的概述

[0107] (1-2) 电力管理装置的配置

[0108] (1-3) 由显示单元显示的内容

[0109] (1-4) 隐藏电力消费模式

[0110] (1-5) 由电力管理装置进行的多种控制

[0111] (1-6) 设备管理单元的配置

[0112] (1-7) 信息分析单元的配置

[0113] (1-8) 可控制设备的配置

[0114] (1-9) 电力存储装置的配置

[0115] (1-10) 电子水印信息的嵌入方法和验证方法的具体示例

[0116] (1-11) 注册电力管理装置的方法

[0117] (1-12) 注册可控制设备的方法

[0118] (1-13) 注册可控制插座的方法

[0119] (1-14) 针对临时注册的可控制设备的记账处理

[0120] (1-15) 对注册可控制设备的方法的修改

[0121] (1-16) 在发生异常的情况下电力管理装置对被管理设备的操作

[0122] (1-17) 当在电力状态中发生异常时电力管理装置的操作

[0123] (1-18) 电子水印信息的嵌入方法和验证方法的流程

[0124] (1-19) 分析服务器的作用

[0125] (1-20) 分析服务器的配置

[0126] (1-21) 指定待排除的蓄电池的处理

[0127] (1-22) 保护电力管理装置免受非法攻击的方法

[0128] (1-23) 排除蓄电池的方法

[0129] (1-24) 由获取数据验证单元执行的验证处理

[0130] (1-25) 由第一验证单元进行的验证处理的流程

[0131] (1-26) 由数据库管理单元进行的测试处理

[0132] (1-27) 数据库的更新和判断词典的生成

[0133] (1-28) 管理病毒定义文件的方法

[0134] (1-29) 指定待排除蓄电池的方法的流程

[0135] (1-30) 当存在多个电力管理装置时的处理

[0136] (2) 第二实施例

[0137] (2-1) 第二实施例的概况

[0138] (2-2) 服务提供单元的配置

[0139] (2-3) 到数据库的链接

[0140] (2-4) 对于链接系统的娱乐的安全性

[0141] (2-5) 链接系统的娱乐的流程

[0142] (3) 根据本发明的实施例的电力管理装置的硬件配置

[0143] 第一实施例

[0144] (1-1) 电力管理装置的概述

[0145] 首先，描述根据本发明的第一实施例的电力管理装置的概况。

[0146] 图 1 示出根据本实施例的电力管理系统的总体图。

[0147] 如图 1 所示，根据本实施例的电力管理系统包括：局部电力管理系统 1、广域网 2、外部服务器 3、电力信息收集装置 4、电力供应者系统 5、终端设备 6、以及电力交易系统 7。而且，局部电力管理系统 1、外部服务器 3、电力信息收集装置 4、电力供应者系统 5、终端设备 6、以及电力交易系统 7 连接至广域网 2，从而相互之间能够交换信息。

[0148] 另外，在本说明书中，使用措辞“局部”和“广域”。“局部”表示由在不使用广域网

2 的情况下能够通信的多个元件形成的小组。换句话说，“广域”表示包括经由广域网 2 通信的多个元件的大组。而且，由设置在局部电力管理系统 1 内的多个元件构成的小组可以由措辞“局部”来特别地表达。换句话说，图 1 中所示的整个电力管理系统可以由措辞“广域”来表达。

[0149] 现在，上述电力管理系统试图（如同通过上述智能电网计划）提高电力使用效率，以及适当地管理对电力进行操作的多种设备、存储电力的电力存储装置、生成电力的发电装置、从电源提供电力的供电装置等。该电力管理系统中的电力管理的目标是设置在局部电力管理系统 1 中的设备、电力存储装置、发电装置、供电装置等。另外，被称为 HEMS（家用能量管理系统）或 BEMS（建筑物能量管理系统）的智能电网计划中的系统是局部电力管理系统 1 的示例。

[0150] 如图 1 所示，局部电力管理系统 1 包括电力管理装置 11 以及被管理块 12。电力管理装置 11 充当管理设置在局部电力管理系统 1 中的设备、电力存储装置、发电装置、供电装置等的角色。例如，电力管理装置 11 允许或禁止给每个设备供电。而且，电力管理装置 11 执行对每个设备的认证，以识别设备或确认设备的合法性。然后，电力管理装置 11 从每个设备收集关于电力消费等的信息。

[0151] 而且，电力管理装置 11 从电力存储装置获取关于所存储电力量等信息。然后，电力管理装置 11 对电力存储装置执行充电 / 放电控制。而且，电力管理装置 11 从发电装置获取关于发电量等信息。而且，电力管理装置 11 从供电装置获取关于从外部提供的电力量的信息。以这种方式，电力管理装置 11 从设置在局部电力管理系统 1 中的设备、电力存储装置、发电装置、以及供电装置获取信息，并且控制电力的输入 / 输出。当然，电力管理装置 11 在适当的时候对除设备、电力存储装置、发电装置、以及供电装置之外的结构元件执行类似管理。而且，电力管理装置 11 不仅能够对电力执行管理，而且还对其中的减少量可以被量化的一般生态（诸如，CO_2、水资源等）进行管理。即，电力管理装置 11 还能够起到生态管理装置的作用。顺便提及，以下，通过将电力作为其减少量可以被量化的资源的示例来进行说明。

[0152] 在图 1 中所示的局部电力管理系统 1 中，作为电力管理的目标的结构元件（诸如，设备、电力存储装置、发电装置、以及供电装置）被包括在被管理块 12 中。包括在被管理块 12 中的结构元件和电力管理装置 11 能够直接或间接地交换信息。而且，电力管理装置 11 可以被配置为能够与电力信息收集装置 4 交换信息。电力信息收集装置 4 管理从与电力供应者所管理的电力供应者系统 5 提供的电力相关的信息。另外，在智能电网计划中被称为智能仪表的设备是电力信息收集装置 4 的示例。

[0153] 电力供应者系统 5 给每个局部电力管理系统 1 供电。然后，从电力供应者系统 5 提供的电力经由电力信息收集装置 4 被提供给局部电力管理系统 1 中的被管理块 12。这里，电力信息收集装置 4 获取例如关于提供给被管理块 12 的电力量的信息。然后，电力信息收集装置 4 将所获取的关于电力量等的信息发送至电力供应者系统 5。通过使用这种机制，电力供应者系统 5 收集与每个局部电力管理系统 1 中的被管理块 12 的电力消费等相关的信息。

[0154] 而且，电力供应者系统 5 参考所收集的关于电力消费等的信息，控制电力信息收集装置 4，并且控制电力供应量，使得实现被管理块 12 或整个电力管理系统的有效电力使

用。在此，电力信息收集装置 4 限制从电力供应者系统 5 提供至被管理块 12 的电力量，或者根据被管理块 12 的电力消费提高对电力量的限制。另外，电力供应者例如可以是电力公司、拥有发电站的法人或非法人发电管理者、拥有电力存储设施的法人或非法人电力存储管理者等。

[0155] 然而，在当前情况下，电力公司很可能是电力供应者，并且在本说明书中，将假设电力公司是电力供应者的情况作出说明。而且，目前大多数从外部提供的电力都是从电力公司（其为电力供应者）购买的。然而，未来，电力市场可能变得活跃并且在电力市场中购买的电力可能覆盖大多数从外部提供的电力。在这种情况下，假设将从电力交易系统 7 提供电力给局部电力管理系统 1，如图 1 所示。

[0156] 电力交易系统 7 执行关于电力交易的处理，诸如，电力市场中的买卖订单的安排 (placement)、订单执行后的价格计算、结算处理、供电订单的安排等。而且，在图 1 的示例中，在电力市场中已经执行订单的电力接收也由电力交易系统 7 实现。从而，在图 1 的示例中，根据所执行订单的类型，将电力从电力交易系统 7 提供给局部电力管理系统 1，或者将电力从局部电力管理系统 1 提供给电力交易系统 7。而且，通过使用电力管理装置 11 自动地或手动地执行对电力交易系统 7 的订单的安排。

[0157] 而且，图 1 中所示的电力管理系统包括多个局部电力管理系统 1。如上所述，每个局部电力管理系统 1 均包括电力管理装置 11。多个电力管理装置 11 可以经由广域网 2 或安全通信路径（未示出）相互交换信息。还提供了一种将电力从一个局部电力管理系统 1 提供给另一局部电力管理系统 1 的机制。在这种情况下，两个系统的电力管理装置 11 都执行关于电力接收的信息交换，并且执行控制以发送由信息交换适当确定的电力量。

[0158] 对于该部分，电力管理装置 11 可以被配置为可由经由广域网 2 连接的外部终端设备 6 操作。例如，用户可能想要通过使用终端设备 6 检查用户管理的局部电力管理系统 1 的电力状态。在这种情况下，如果电力管理装置 11 被配置为可由终端设备 6 操作，则用户能够获得由终端设备 6 显示的用户管理的局部电力管理系统 1 的电力状态，并且检查电力状态。用户还能够通过使用终端设备 6 通过电力管理装置 11 进行电力交易。

[0159] 另外，终端设备 6 可以设置在局部电力管理系统 1 内。在这种情况下，终端设备 6 通过使用设置在局部电力管理系统 1 中的通信路径连接至电力管理装置 11，而不使用广域网 2。使用终端设备 6 的一个优点在于，用户不必去往电力管理装置 11 的安装位置。也就是说，如果终端设备 6 可以使用，则可以从任意位置对电力管理装置 11 进行操作。另外，作为终端设备 6 的具体形式，可以假设为例如移动电话、移动信息终端、笔记本电脑、便携式游戏机、信息家电、传真机、有线电话、音频 / 视频设备、汽车导航系统、或电动交通工具。

[0160] 以上，已经参考每个结构元件的操作或功能简要地描述了图 1 中所示的电力管理系统中的电力管理。然而，除了与电力管理相关的功能之外，上述电力管理装置 11 还具有通过使用从被管理块 12 等收集的多条信息将多种服务提供给用户的功能。

[0161] 由电力管理装置 11 收集的信息例如可以是每个设备的型号或设备 ID（以下称为设备信息）、关于用户的简档的信息（以下称为用户信息）、关于用户的账户或信用卡的信息（以下称为记账信息）、关于将要使用的服务的注册信息（以下称为服务信息）等。上述设备信息被预先设置在每个设备中或者由用户手动输入。而且，在很多情况下，上述用户信息、记账信息、以及服务信息可以由用户手动输入至电力管理装置 11。另外，信息的输入方

法不限于这些示例，并且可以改变为任意输入方法。而且，在以下说明中，设备信息、用户信息、记账信息、以及服务信息将被称为“初始信息”。

[0162] 除了初始信息之外，电力管理装置 11 能够收集的信息可以为与连接至每个设备的蓄电池的规格相关的信息（以下称为设备蓄电池信息）、与每个设备等（包括电力存储装置、发电装置、供电装置等）的状态相关的信息（以下称为设备状态信息）、能够从连接至广域网 2 的外部系统或服务器获取的信息（以下称为外部信息）等。上述设备状态信息例如可以是电力存储装置在信息收集时间点的放电电压或所存储的电力量、发电装置的发电电压或发电量、每个设备的电力消费等。而且，上述外部信息可以是从电力交易系统 7 获取的电力的单位市场价格、从外部服务器 3 获取的可用服务的列表等。另外，在以下说明中，设备蓄电池信息、设备状态信息，以及外部信息将被称为“初级信息”。

[0163] 而且，电力管理装置 11 能够由其本身或者使用外部服务器 3 的功能，通过使用初始信息和初级信息来计算次级信息。例如，电力管理装置 11 分析上述初级信息，并且计算表示从电力供应者系统 5 提供的电力、由发电装置生成的电力、由电力存储装置充电 / 放电的电力、以及由被管理块 12 消费的电力之间的平衡的索引值（以下称为平衡索引）。而且，电力管理装置 11 基于电力消费，计算记账情况和 CO_2 减少量情况。而且，电力管理装置 11 基于初始信息计算每个设备的消耗程度（使用持续时间与寿命的比例等），或者基于所消费电力随着时间的改变分析用户的生活模式。

[0164] 而且，电力管理装置 11 通过使用次级信息进行计算或者通过执行与连接至广域网 2 的系统或服务器或另一电力管理装置 11 的信息交换，来获得多条信息（以下称为三级信息）。例如，电力管理装置 11 获取与买 / 卖订单的情况或电力市场中的价格相关的信息（以下称为市场数据）、与相邻区域中的剩余电力或不足电力的量相关的信息（以下称为区域电力信息）、与从提高有效电源使用角度看适于用户的生活模式的设备相关的信息（以下称为设备推荐信息）、与计算机病毒等相关的安全信息、或者与设备中的故障等相关的设备危险信息。

[0165] 通过适当地使用上述初始信息、初级信息、次级信息以及三级信息，电力管理装置 11 能够给用户提供多种服务。同时，电力管理装置 11 将拥有与用户的隐私或局部电力管理系统 1 的安全相关的重要信息。而且，电力管理装置 11 用来允许或禁止给被管理块 12 供电。从而，希望从电力管理装置 11 得到高安全等级，使得能够防止来自局部电力管理系统 1 外部的攻击或者在局部电力管理系统 1 内执行的非法行为。

[0166] 作为电力管理装置 11 从局部电力管理系统 1 外部接收的攻击，可以认为是 DoS 攻击（拒绝服务攻击）、计算机病毒等。当然，防火墙被设置在局部电力管理系统 1 和广域网 2 之间，但是为了上述原因，想要更严格的安全措施。而且，作为在局部电力管理系统 1 内执行的非法行为，可以是对设备、电力存储装置等的非法修改、信息的伪造、未授权设备的连接等。而且，从提高安全等级的观点来看，防止由恶意第三方使用与反映用户的生活模式的被消费电力相关的信息、或者检测 / 恢复每个设备或电力管理装置 11 的损坏（在一些情况下为起火等）的措施可能变为必要的。

[0167] 如随后所述，电力管理装置 11 具有实现上述这种高安全等级的功能。电力管理装置 11 实现对被管理块 12 的电力管理、基于从被管理块 12 等收集的初始信息、初级信息、次级信息以及三级信息的服务提供，同时保持安全等级。另外，由电力管理装置 11 保持高安

全等级可以不仅由电力管理装置 11 实现。从而，可以尝试用被管理块 12 中设置的设备、电力存储装置、发电装置、供电装置等与电力管理装置 11 结合来保持安全等级。此外，随后将详细描述被管理块 12 的这种结构元件。

[0168] 被管理块的配置

[0169] 将参考图 2 至图 4 详细地描述被管理块 12 的配置。图 2 示出被管理块 12 的配置。而且，图 3 示出被管理块 12 内的通信网络的配置。而且，图 4 示出用于与电力管理装置 11 交换信息的主要结构元件的具体配置。

[0170] 首先，参考图 2。如图 2 所示，被管理块 12 包括 :配电装置 121、AC/DC 转换器 122、可控制插座 123、电动交通工具 124、可控制设备 125、不可控制设备 126、插座扩展装置 127、电力存储装置 128、第一发电装置 129、第二发电装置 130、以及环境传感器 131。

[0171] 另外，可控制插座 123、电动交通工具 124、可控制设备 125、以及插座扩展装置 127 是上述设备的示例。而且，电力存储装置 128 是上述电力存储装置的示例。而且，第一发电装置 129 和第二发电装置 130 是上述发电装置的示例。可控制插座 123 和插座扩展装置 127 还是上述供电装置的示例。而且，不可控制设备 126 不直接受到电力管理装置 11 的电力管理，从而其本身不是上述设备的示例。然而，如随后所述，通过与插座扩展装置 127 结合，不可控制设备 126 能够被电力管理装置 11 所管理，并且是上述设备的示例。

[0172] 电力流

[0173] 从电力供应者系统 5、电力交易系统 7、或另一局部电力管理系统 1 提供的电力（以下称为外部电力）被输入配电装置 121。假设外部 AC 电力被输入图 2 的示例中的配电装置 121，但是也可以输入外部 DC 电力。然而，为了说明，以下假设外部 AC 电力被输入配电装置 121。输入至配电装置 121 的外部电力由 AC/DC 转换器 122 从 AC 转换为 DC，并且被输入可控制插座 123 或电力存储装置 128。

[0174] 而且，从电力存储装置 128 放电的电力（以下称为放电电力）也被输入配电装置 121。从电力存储装置 128 输出的放电电力由 AC/DC 转换器 122 从 DC 转换为 AC，并且被输入至配电装置 121。输入至配电装置 121 的放电 AC 电力由 AC/DC 转换器 122 从 AC 转换为 DC，并且被输入至可控制插座 123。然而，为了避免放电电力在 AC/DC 转换器 122 处的损失，还可以将放电电力在不经过 AC/DC 转换器 122 的情况下从电力存储装置 128 提供至可控制插座 123。

[0175] 除了经由配电装置 121 输入的外部电力之外，由第一发电装置 129 和第二发电装置 130 生成的电力（以下称为生成电力）被输入至电力存储装置 128。另外，在图 2 的示例中，由第一发电装置 129 和第二发电装置 130 生成的生成电力被临时存储在电力存储装置 128 中。然而，由第一发电装置 129 和第二发电装置 130 生成的生成电力还可以在不经过电力存储装置 128 的情况下被输入 AC/DC 转换器 122 或可控制插座 123。然而，在很多情况下，由于气候或环境原因，从第一发电装置 129 输出的生成电力的提供是不稳定的。从而，在使用从第一发电装置 129 输出的生成电力的情况下，优选在被临时存储在电力存储装置 128 中之后使用生成电力。

[0176] 另外，第一发电装置 129 是用于使用可再生能源生成电力的发电装置。例如，第一发电装置 129 是光电装置、风力发电装置、地热发电装置、水力发电装置等。另一方面，第二发电装置 130 是用于使用不可再生能源生成电力的发电装置（与通过使汽油、煤等燃烧并

且使用燃烧生成电力的热力发电相比是环保的）。例如，第二发电装置 130 是燃料电池、天然气发电装置、生物质发电装置等。顺便提及，在使用从可再生能源得到的电力来生成氢（其为用于燃料电池发电的燃料）的情况下，燃料电池是在不使用不可再生能源的情况下生成电力的发电装置。

[0177] 由第一发电装置 129 和第二发电装置 130 生成的生成电力、以及存储在电力存储装置 128 中的电力，一方面经由配电装置 121 或 AC/DC 转换器 122 输入可控制插座 123，另一方面，可以由电力供应者系统 5、电力交易系统 7 等购买。在这种情况下，由第一发电装置 129 和第二发电装置 130 生成的生成电力以及从电力存储装置 128 输出的放电电力被 AC/DC 转换器 122 从 DC 转换为 AC，并且经由配电装置 121 发送至电力供应者系统 5、电力交易系统 7 等。

[0178] 以上，粗略地描述了被管理块 12 中的电力流。特别地，在此描述了流经配电装置 121 的电力的分配路径。如上所述，配电装置 121 充当对被管理块 12 内的电力的分配路径进行划分的角色。从而，如果配电装置 121 停止，则被管理块 12 内的电力的分配中断。从而，配电装置 121 设置有不间断电源 (UPS)。另外，在图 2 的示例中，独立于电力管理装置 11 地提供配电装置 121，但是配电装置 121 和电力管理装置 11 可以安装在同一外壳内。

[0179] 供电时的认证

[0180] 在被管理块 12 中，经由配电装置 121 流至可控制插座 123 或电力存储装置 128 的电力由电力管理装置 11 管理。例如，电力管理装置 11 控制配电装置 121 并且对可控制插座 123 供电或者停止对可控制插座 123 供电。

[0181] 电力管理装置 11 还执行对可控制插座 123 的认证。然后，电力管理装置 11 对认证成功的可控制插座 123 供电，并且停止对认证失败的可控制插座 123 供电。这样，通过电力管理装置 11 作出的认证成功或失败来确定在被管理块 12 中供电或不供电。电力管理装置 11 进行的认证不仅对可控制插座 123 执行，还对电动交通工具 124、可控制设备 125、以及插座扩展装置 127 执行。顺便提及，由电力管理装置 11 进行的认证不对不可控制设备 126 执行，不可控制设备 126 不拥有与电力管理装置 11 通信的功能，也不拥有认证所需要的计算功能。

[0182] 从而，基于电力管理装置 11 的控制，可以给已被认证的可控制插座 123、电动交通工具 124、可控制设备 125、或插座扩展装置 127 供电。然而，其本身没有被经过认证的不可控制设备 126 将不基于电力管理装置 11 的控制被供电。从而，与电力管理装置 11 的控制无关地将电力连续提供给不可控制设备 126，或者根本不对其提供电力。然而，通过使插座扩展装置 127 执行认证作为代替，可能基于电力管理装置 11 的控制给不可控制设备 126 供电。

[0183] 设备功能的概述

[0184] 在此简短地概述可控制插座 123、电动交通工具 124、可控制设备 125、不可控制设备 126、以及插座扩展设备 127 的功能。

[0185] 可控制插座 123

[0186] 首先，将概述可控制插座 123 的功能。可控制插座 123 具有与电动交通工具 124、可控制设备 125、不可控制设备 126、以及插座扩展装置 127 的电源插头连接的端子。而且，可控制插座 123 具有经由配电装置 121 对连接到该端子的电动交通工具 124、可控制设备

125、不可控制设备 126、以及插座扩展装置 127 供电的功能。即，可控制插座 123 具有供电插座的功能。

[0187] 可控制插座 123 还具有电力管理装置 11 进行认证所需要的多种功能。例如，可控制插座 123 具有与电力管理装置 11 交换信息的通信功能。通过电力线或信号线的线缆通信或者通过给可控制插座 123 提供用于无线通信的通信模块来实现该通信功能。可控制插座 123 还具有用于执行在认证时需要的计算的计算功能。而且，可控制插座 123 保存识别信息诸如认证所需要的设备 ID 以及密钥信息。通过使用这些功能和信息，可控制插座 123 能够被电力管理装置 11 认证。另外，认证的类型可以是使用随机数的相互认证，或者是使用私密密钥和公开密钥对的公开密钥认证。

[0188] 而且，可控制插座 123 还可以具有状态显示装置，用于显示向电力管理装置 11 的认证的成功 / 失败以及在认证过程中的状态（以下称为认证状态）。在这种情况下，设置在可控制插座 123 中的状态显示装置可以显示连接至可控制插座 123 的电动交通工具 124、可控制设备 125、以及插座扩展装置 127 的认证状态。而且，该状态显示装置还可以显示连接至可控制插座 123 的设备是否是不可控制设备 126。另外，该状态显示装置由诸如 LED 或小灯泡的指示灯、或者诸如 LCD 或 ELD 的显示设备配置。

[0189] 如上所述，在电力管理装置 11 的控制下经由配电装置 121 对由电力管理装置 11 认证成功的可控制插座 123 供电。换句话说，在电力管理装置 11 的控制下，停止对认证失败的可控制插座 123 供电。这样，根据认证的成功 / 失败控制供电，可以防止未授权供电插座连接至配电装置 121。还可以容易地检测欺诈性地连接至配电装置 121 的供电插座。而且，在状态显示装置设置在可控制插座 123 中的情况下，可以容易地掌握可控制插座 123 的认证状态，并且可以容易地区分可控制插座 123 的认证失败和损坏。

[0190] 现在，可控制插座 123 的形式不限于用于连接电源插头的插座的形式。例如，还可以实现具有通过使用电磁感应来供电的内置线圈（如用于非接触 IC 卡的读取器 / 写入器）的可控制插座 123，以及具有不同于插座的形式的表面形式的可控制插座 123。在这种情况下，如同非接触 IC 卡那样，将用于从可控制插座 123 生成的电磁场生成感应电动势的线圈设置在电动交通工具 124、可控制设备 125、以及插座扩展装置 127 中。根据这种配置，可以在不使用电源插头的情况下提供或接收电力。另外，在使用电磁感应的情况下，可以在可控制插座 123 和电动交通工具 124、可控制设备 125、或插座扩展装置 127 之间使用磁场的调节进行信息交换。

[0191] 而且，可控制插座 123 具有测量提供给连接至该端子的电动交通工具 124、可控制设备 125、或插座扩展装置 127 的电力量的功能。而且，可控制插座 123 具有将所测量的电力量通知给电力管理装置 11 的功能。而且，可控制插座 123 可以具有从连接至该端子的电动交通工具 124、可控制设备 125、或插座扩展装置 127 获取初级信息并且将所获取的初级信息发送至电力管理装置 11 的功能。这样，通过将可控制插座 123 测量或获取的信息发送至电力管理装置 11，可以使电力管理装置 11 掌握电力状态或者执行对每个独立可控制插座 123 的供电控制。

[0192] 电动交通工具 124

[0193] 接下来将概述电动交通工具 124 的功能。电动交通工具 124 包括用于存储电力的蓄电池。电动交通工具 124 还包括使用从蓄电池放电的电力来驱动的驱动机构。在电动交

通工具 124 是电动车或插电式混合电动车的情况下，该驱动机构包括例如马达、传动装置、轴、车轮、轮胎等。其他电动交通工具 124 的驱动机构至少包括马达。而且，电动交通工具 124 包括在给蓄电池充电时使用的电源插头。可以通过将该电源插头连接至可控制插座 123 来接收电力。顺便提及，在可控制插座 123 通过使用电磁感应供电的方法的情况下，在电动交通工具 124 中设置放在磁场中时生成感应电动势的线圈。

[0194] 电动交通工具 124 还具有用于电力管理装置 11 进行认证所需要的多种功能。例如，电动交通工具 124 具有用于与电力管理装置 11 交换信息的通信功能。通过电力线或信号线的线缆通信或者通过给电动交通工具 124 提供用于无线通信的通信模块来实现该通信功能。电动交通工具 124 还具有用于执行认证时所需要的计算的计算功能。而且，电动交通工具 124 保存识别信息诸如认证所需要的设备 ID 以及密钥信息。通过使用这些功能和信息，电动交通工具 124 能够被电力管理装置 11 认证。另外，认证的类型可以是使用随机数的相互认证，也可以是使用私密密钥和公开密钥对的公开密钥认证。

[0195] 而且，电动交通工具 124 还具有向电力管理装置 11 发送与所装配的蓄电池相关的设备蓄电池信息（诸如剩余蓄电池电平、充电量、以及放电量）的功能。还将与拥有电动交通工具 124 的用户相关的用户信息、与电动交通工具 124 的燃料效率、性能等相关的设备信息发送至电力管理装置 11。通过从电动交通工具 124 发送到电力管理装置 11 的这些条信息，电力管理装置 11 可以执行诸如使用用户信息进行记账以及基于用户信息和设备信息进行征税等处理。例如，可以通过电力管理装置 11 执行征收基于 CO_2 释放量计算的环境税的处理、基于剩余蓄电池电平显示里程的处理等。

[0196] 另外，还可以想到使用电动交通工具 124 的蓄电池代替电力存储装置 128。例如，当临时不可能使用电力存储装置 128 时，诸如当电力存储装置 128 故障或者被更换的时候，可以使用电动交通工具 124 的蓄电池来代替电力存储装置 128。而且，由于电动交通工具 124 本身是可移动的，所以可以携带作为材料的外部电力。即，其可以用作可移动电力存储装置 128。由于这种优点，在天灾或紧急情况下，使电动交通工具 124 作为备用电源也是有用的。当然，这种使用可以在根据本实施例的局部电力管理系统 1 的框架内实现。

[0197] 可控制设备 125

[0198] 接下来，将概述可控制设备 125 的功能。可控制设备 125 具有由电力管理装置 11 进行认证所需要的多种功能。例如，可控制设备 125 具有用于与电力管理装置 11 交换信息的通信功能。通过电力线或信号线的线缆通信或者通过给可控制设备 125 提供用于无线通信的通信模块来实现该通信功能。可控制设备 125 还具有用于执行认证时所需要的计算的计算功能。而且，可控制设备 125 保存识别信息诸如认证所需要的设备 ID 和密钥信息。通过使用这些功能和信息，可控制设备 125 能够被电力管理装置 11 认证。另外，认证的类型可以是使用随机数的相互认证，也可以是使用私密密钥和公开密钥对的公开密钥认证。

[0199] 而且，可控制设备 125 还具有向电力管理装置 11 发送与所装配的蓄电池相关的设备蓄电池信息，诸如剩余蓄电池电平、充电量、以及放电量。还将与拥有可控制设备 125 的用户相关的用户信息、与可控制设备 125 的类型、性能等相关的设备信息发送至电力管理装置 11。通过从可控制设备 125 发送到电力管理装置 11 的这些条信息，电力管理装置 11 可以执行诸如使用用户信息进行记账以及基于用户信息和设备信息进行征税等处理。例如，可以通过电力管理装置 11 执行征收基于 CO_2 释放量计算的环境税的处理、推荐具有更高环

境性能的设备的显示处理等。

[0200] 不可控制设备 126、插座扩展装置 127

[0201] 接下来，将概述不可控制设备 126 和插座扩展装置 127 的功能。与上述可控制插座 123、电动交通工具 124、以及可控制设备 125 不同，不可控制设备 126 不拥有由电力管理装置 11 认证所需要的功能。即，不可控制设备 126 是现有家用电器、现有视频设备等。未通过认证的不可控制设备 126 不能经受电力管理装置 11 的电力管理，并且在一些情况下，不能接收电力。从而，为了能够在局部电力管理系统 1 中使用不可控制设备 126，用于执行认证的委托装置是必要的。

[0202] 插座扩展装置 127 充当两个角色。一个角色是用于执行委托认证以使得不可控制设备 126 能够在局部电力管理系统 1 中使用的功能。另一个角色是增加连接至可控制插座 123 的设备数量的功能。与电动交通工具 124、可控制设备 125、或不可控制设备 126 的电源插头连接的一个或多个端子被提供给插座扩展装置 127。当使用提供有多个端子的插座扩展装置 127 时，能够增加可以连接至可控制插座 123 的电动交通工具 124、可控制设备 125、或不可控制设备 126 的数量。即，插座扩展装置 127 用作具有高级功能的电源板。

[0203] 以上，简单地概述了可控制插座 123、电动交通工具 124、可控制设备 125、不可控制设备 126、以及插座扩展装置 127 的功能。顺便提及，上述功能不是可控制插座 123、电动交通工具 124、可控制设备 125、不可控制设备 126、以及插座扩展装置 127 仅有的功能。将这些功能作为基础，还可以进一步补充以下描述的用于电力管理装置 11 进行电力管理的操作所需要的功能。

[0204] 通信功能

[0205] 在此，参考图 3 描述局部电力管理系统 1 内的电力管理装置 11、可控制插座 123、电动交通工具 124、可控制设备 125、插座扩展装置 127 等的通信功能。如图 3 所示，在局部电力管理系统 1 中，例如，使用短程无线通信、无线 LAN、电力线通信等。例如，ZigBee 是短程无线通信的一个示例。而且，PLC 是电力线通信的一个示例。

[0206] 如图 2 所示，在局部电力管理系统 1 中，可控制插座 123 和连接至可控制插座 123 的设备通过电力线连接至配电装置 121。这样，能够通过使用这些电力线容易地构建基于电力线通信的通信网络。另一方面，在使用短程无线通信的情况下，可以通过自组方式连接每个设备来构建通信网络，如图 3 所示。而且，在使用无线 LAN 的情况下，每个设备都能够直接连接至电力管理装置 11。从而，能够通过使用任何通信方法，在局部电力管理系统 1 内构建必要的通信网络。

[0207] 然而，如图 3 所示，不可控制设备 126 有时不能通过使用通信网络连接至电力管理装置 11。从而，在使用不可控制设备 126 的情况下，不可控制设备 126 需要连接至插座扩展装置 127。另外，即使在使用不具有通信功能也不具有认证功能的不可控制插座的情况下，如果电动交通工具 124、可控制设备 125、或插座扩展装置 127 连接至不可控制插座，也可以通过使用电动交通工具 124、可控制设备 125、或插座扩展装置 127 的功能来进行经由通信网络到电力管理装置 11 的连接。当然，在不可控制设备 126 连接至不可控制插座的情况下，不能进行到通信网络的连接，从而不能进行由电力管理装置 11 的控制。

[0208] 顺便提及，电力信息收集装置 4 可以作为连接目的地被包括在局部电力管理系统 1 内构建的通信网络中，如图 3 所示。而且，可以通过使用该通信网络在电动交通工具 124

或可控制设备 125 和电力信息收集装置 4 之间交换信息。当然，电力管理装置 11 和电力信息收集装置 4 可以通过使用该通信网络来交换信息。这样，可以根据实施例的模式适当地设置局部电力管理系统 1 内构建的通信网络的结构。另外，该通信网络由充分安全的通信信道构建。而且，应提供允许保证流经通信信道的信息的安全的机制。

[0209] 设备和多种装置的具体示例

[0210] 在此，将参考图 4 介绍局部电力管理系统 1 中的一些结构元件的具体示例。如图 4 所示，可以与电力管理装置 11 交换信息的结构元件包括：例如，电动交通工具 124、可控制设备 125（智能设备）、不可控制设备 126（传统设备）、电力存储装置 128、第一发电装置 129、第二发电装置 130 等。

[0211] 例如，电动车和插电式混合电动车可以被给定为电动交通工具 124 的具体示例。而且，例如家用电器、个人计算机、移动电话、以及视频设备可以被给定为可控制设备 125 和不可控制设备 126 的具体示例。例如，锂离子充电电池、NAS 充电电池、以及电容器可以被给定为电力存储装置 128 的具体示例。而且，例如，光电装置、风力发电装置、以及地热发电装置可以被给定为第一发电装置 129 的具体示例。而且，燃料电池、天然气发电装置、以及生物质发电装置可以被给定为第二发电装置 130 的具体示例。如上所述，多种装置和设备都可以被用作局部电力管理系统 1 的结构元件。

[0212] 以上，已经描述了被管理块 12 的配置。然而，包括在被管理块 12 中的每个结构元件的功能不限于以上所述。在由电力管理装置 11 进行的电力管理需要时，补充每个结构元件的功能。另外，将在随后描述的电力管理装置 11 和其他结构元件的配置的说明中详细描述每个结构元件的补充功能。

[0213] 外部服务器的配置

[0214] 接下来，将参考图 5 描述外部服务器 3 的配置。如图 5 所示，例如，服务提供服务器 31、记账服务器 32、系统管理服务器 33、分析服务器 34、证书机构服务器 35、制造商服务器 36、以及地图 DB 服务器 37 用作外部服务器 3。

[0215] 服务提供服务器 31 具有提供使用电力管理装置 11 等的功能的服务的功能。记账服务器 32 具有根据局部电力管理系统 1 内消费的电力给电力管理装置 11 提供记账信息，并基于关于由电力管理装置 11 管理的电力量的信息请求用户支付使用费的功能。而且，记账服务器 32 与服务提供服务器 31 合作，执行对用户使用的服务的记账处理。另外，记账处理可以针对拥有消费电力的电动交通工具 124、可控制设备 125 等的用户执行，或者可以针对管理关于被消费电力的信息的电力管理装置 11 的用户执行。

[0216] 系统管理服务器 33 具有管理图 1 所示的整个电力管理系统或者基于区域地管理电力管理系统的功能。例如，如图 6 所示，系统管理服务器 33 掌握在用户 #1 的局部电力管理系统 1 中的使用情况、在用户 #2 的局部电力管理系统 1 中的使用情况、在用户 #3 的局部电力管理系统 1 中的使用情况，并且给记账服务器 32 等提供必要信息。

[0217] 在图 6 的示例中，假设用户 #1 使用用户 #1 他 / 她自己、用户 #2、以及用户 #3 的局部电力管理系统 1 中的电力的情况。在这种情况下，由系统管理服务器 33 收集消费电力的用户 #1 的设备 ID 和使用信息（电力消费等），并且将用户 #1 的用户信息和使用信息从系统管理服务器 33 发送至记账服务器 32。而且，系统管理服务器 33 基于所收集的使用信息计算记账信息（记账数目等），并且将其提供给用户 #1。对于该部分，记账服务器 32 以对

应于记账信息的金额对用户 #1 计费。

[0218] 如上所述，通过系统管理服务器 33 对多个局部电力管理系统 1 进行总体控制，即使用户使用另一用户的局部电力管理系统 1 中的电力，也可以实现给使用了电力的用户记账的机制。特别地，在多数情况下，在由其本身管理的局部电力管理系统 1 的外部，执行对电动交通工具 124 的充电。在这种情况下，如果使用系统管理服务器 33 的上述功能，则能够可靠地对电动交通工具 124 的用户计费。

[0219] 分析服务器 34 具有分析由电力管理装置 11 收集的信息、或者连接至广域网 2 的另一服务器所拥有的信息的功能。例如，在优化基于区域的供电控制的情况下，从局部电力管理系统 1 收集的信息量将会很大，并且为了通过分析信息计算用于每个局部电力管理系统 1 的最优控制方法，需要执行大量计算。这种计算对于电力管理装置 11 来说是繁重的，因此通过使用分析服务器 34 来执行。另外，分析服务器 34 还可以用于其他多种计算处理。而且，证书机构服务器 35 用于对公开密钥进行认证，并且用于颁发公开密钥证书。

[0220] 制造商服务器 36 由设备的制造商管理。例如，电动交通工具 124 的制造商服务器 36 保存关于电动交通工具 124 的设计的信息。类似地，可控制设备 125 的制造商服务器 36 保存关于可控制设备 125 的设计的信息。而且，制造商服务器 36 保存用于识别每个所制造设备（诸如，每个电动交通工具 124 和每个可控制设备 125）的信息。制造商服务器 36 具有通过使用这些条信息并且与电力管理装置 11 合作来识别位于每个局部电力管理系统 1 内的电动交通工具 124 或可控制设备 125 的功能。通过使用该功能，电力管理装置 11 能够执行对电动交通工具 124 或可控制设备 125 的认证，或者检测未授权设备的连接。

[0221] 地图 DB 服务器 37 保存地图数据库。从而，连接至广域网 2 的服务器或电力管理装置 11 能够访问地图 DB 服务器 37 并且使用地图数据库。例如，在用户使用他 / 她的局部电力管理系统 1 外部的电力的情况下，系统管理服务器 33 能够从地图数据库搜索使用位置，并且将关于使用位置的信息以及记账信息提供给用户。如上所述，存在多种类型的外部服务器 3，并且除了在此所示的服务器配置之外，在适当的时候，还可以增加不同类型的外部服务器 3。

[0222] (1-2) 电力管理装置的配置

[0223] 以上，描述了根据本实施例的电力管理系统的整体图。以下，将参考图 7 至图 9 描述主要负责电力管理系统中的电力管理的电力管理装置 11 的配置。

[0224] 功能综述

[0225] 首先，将参考图 7 描述电力管理装置 11 的总体功能配置。如图 7 所示，电力管理装置 11 包括局部通信单元 111、信息管理单元 112、存储单元 113、广域通信单元 114、控制单元 115、显示单元 116、输入单元 117、以及服务提供单元 118。

[0226] 局部通信单元 111 是用于经由在局部电力管理系统 1 内构建的通信网络进行通信的通信装置。信息管理单元 112 是用于管理包括在局部电力管理系统 1 内的每个结构元件的设备信息以及与电力相关的信息的装置。而且，由信息管理单元 112 执行对可控制插座 123、电动交通工具 124、可控制设备 125、插座扩展装置 127 等的认证处理。存储单元 113 是用于保存用于认证的信息和用于电力管理的信息的存储装置。存储单元 113 存储与电力管理装置 11 所保存的私密密钥和公开密钥构成的密钥对、公共密钥等相关的密钥信息，多种数字签名或证书，多种数据库，或历史信息。广域通信单元 114 是用于经由广域网 2 与外

部系统和服务器交换信息的通信装置。

[0227] 控制单元 115 是用于控制包括在局部电力管理系统 1 内的每个结构元件的操作的控制装置。显示单元 116 是用于显示与在局部电力管理系统 1 中消费的电力相关的信息、用户信息、记账信息、与电力管理相关的其他类型信息、与局部电力管理系统 1 外部的电力管理相关的信息、与电力交易相关的信息等的显示装置。另外，例如，LCD、ELD 等可以用作显示装置。输入单元 117 是用于用户输入信息的输入装置。另外，例如，键盘、按钮等可以用作输入单元 117。而且，还可以通过结合显示单元 116 和输入单元 117 来构建触摸面板。服务提供单元 118 是用于在电力管理装置 11 处实现多种服务和功能并且将其提供给用户，同时与外部系统、服务器等合作操作的装置。

[0228] 如上所述，电力管理装置 11 包括用于与局部电力管理系统 1 内部或外部的设备、装置、系统、服务器等交换信息的通信装置（局部通信单元 111、广域通信单元 114）。而且，电力管理装置 11 包括用于控制局部电力管理系统 1 内的设备或装置的控制装置（控制单元 115）。而且，电力管理装置 11 包括从局部电力管理系统 1 内部或外部的设备、装置、系统、服务器等收集信息，并且通过使用该信息给局部电力管理系统 1 内的设备或装置提供服务或认证的信息管理装置（信息管理单元 112）。而且，电力管理装置 11 包括用于显示与局部电力管理系统 1 内部或外部的电力相关的信息的显示装置（显示单元 116）。

[0229] 为了安全和有效地管理局部电力管理系统 1 内的电力，首先，需要正确地识别局部电力管理系统 1 内的设备、装置等。而且，为了安全和有效地管理局部电力管理系统 1 内的电力，还需要分析与局部电力管理系统 1 内部和外部的电力相关的信息并且执行适当的电力控制。信息管理单元 112 的功能用于为满足上述要求而执行的信息管理。从而，将更详细地描述信息管理单元 112 的功能。另外，控制单元 115 的功能用于控制具体设备、装置等。

[0230] 功能详情

[0231] 以下，将参考图 8 和图 9 详细地描述信息管理单元 112 的功能配置。图 8 示出信息管理单元 112 的具体功能配置。图 9 示出信息管理单元 112 的每个结构元件的主要功能。

[0232] 如图 8 所示，信息管理单元 112 包括：设备管理单元 1121、电力交易单元 1122、信息分析单元 1123、显示信息生成单元 1124、以及系统管理单元 1125。

[0233] 设备管理单元 1121

[0234] 如图 9 所示，设备管理单元 1121 是用于管理局部电力管理系统 1 内的设备、装置等的装置。例如，设备管理单元 1121 针对可控制插座 123、电动交通工具 124、可控制设备 125、插座扩展装置 127 等执行设备 ID 的注册、认证、管理，操作设置和服务设置的管理，操作状态和使用状态的掌握，环境信息的收集等。另外，通过使用安装在被管理块 12 中的环境传感器 131 来执行环境信息的收集。而且，环境信息是与温度、湿度、天气、风向、风速、地形、区域、天气预报等相关的信息，以及通过对其进行分析获得的信息。

[0235] 电力交易单元 1122

[0236] 如图 9 所示，电力交易单元 1122 执行电力市场中的市场交易数据或个体交易数据的获取、交易执行的定时控制、交易的执行、交易日志的管理等。另外，市场交易数据是与电力市场中的市场价格和交易条件相关的信息。而且，个体交易数据是与在电力供应者和相邻电力消费者之间进行个体交易时确定的交易价格和交易条件等相关的信息。交易执行的

定时控制是，例如，在电力购买价格下降到预定值以下的定时发出预定量的购买订单，或者在电力卖出价格上升到预定值以上的定时发出预定量的出售订单的自动控制。

[0237] 信息分析单元 1123

[0238] 如图 9 所示，信息分析单元 1123 执行发电数据的分析、电力存储数据的分析、生活模式的学习、以及电力消费数据的分析。而且，信息分析单元 1123 基于以上分析，执行电力消费模式的估计、电力存储模式的估计、电力放电模式的估计、以及发电模式的估计。另外，例如，通过使用局部电力管理系统 1 内的第一发电装置 129 或第二发电装置 130 的发电量的时间序列数据、电力存储装置 128 的充电 / 放电量或电力存储量的时间序列数据、或由电力提供者系统 5 提供的电力量的时间序列数据，来执行信息分析单元 1123 的分析和学习。

[0239] 而且，通过将时间序列数据或通过分析时间序列数据获得的分析结果用作用于学习的数据，并且通过使用基于预定机器学习算法获得的估计公式，来执行信息分析单元 1123 的估计。例如，通过使用遗传学习算法（例如，参见 JP-A-2009-48266），可以自动构建估计公式。而且，通过将过去的时间序列数据或分析结果输入估计公式，可以获得估计结果。而且，通过顺序地将所计算的估计结果输入估计公式，可以估计时间序列数据。

[0240] 而且，信息分析单元 1123 执行现在或未来的 CO_2 排放量的计算、用于减少电力消费的供电模式（电力节省模式）的计算、用于减少 CO_2 排放量的供电模式（低 CO_2 排放模式）的计算、以及能够减少局部电力管理系统 1 内的电力消费和 CO_2 排放量的设备配置、设备布置等的计算或建议。基于总电力消费或对于每种发电方法有所区别的电力消费来计算 CO_2 排放量。

[0241] 在使用总电力消费的情况下，计算近似平均 CO_2 排放量。换句话说，在使用对于每种发电方法有所区别的电力消费的情况下，计算较为精确的 CO_2 排放量。另外，通过至少区分从外部提供的电力、由第一发电装置 129 生成的电力与第二发电装置 130 所生成的电力，可以计算出比使用总电力消费时更精确的 CO_2 排放量。在很多情况下，根据 CO_2 排放量来确定税金（诸如，碳税）和记账。从而，认为能够准确计算 CO_2 排放量增加了用户间的公平感，并且有助于广泛使用基于可再生能源的发电装置。

[0242] 显示信息生成单元 1124

[0243] 如图 9 中所示，显示信息生成单元 1124 通过调节与局部电力管理系统 1 内的设备、装置等相关的信息、与电力相关的信息、与环境相关的信息、与电力交易相关的信息、与信息分析单元 1123 的分析结果或估计结果相关的信息等的格式，来生成要显示在显示单元 116 上的显示信息。例如，显示信息生成单元 1124 生成用于以图表格式显示表示电力量的信息的显示信息，或者生成用于以表格形式显示市场数据的显示信息。而且，显示信息生成单元 1124 生成用于显示多种类型信息或输入信息的图形用户界面 (GUI)。由显示信息生成单元 1124 生成的多段显示信息被显示在显示单元 116 上。

[0244] 系统管理单元 1125

[0245] 如图 9 所示，例如，系统管理单元 1125 执行固件（其为用于控制电力管理装置 11 的基本操作的程序）版本的管理 / 更新，限制对其的访问，并且采取防病毒措施。而且，在多个电力管理装置 11 安装在局部电力管理系统 1 中的情况下，系统管理单元 1125 与另一电力管理装置 11 交换信息并且执行控制，使得多个电力管理装置 11 相互协同操作。例如，系统管理单元 1125 管理每个电力管理装置 11 的属性（例如，对设备、装置等的控制处理的

优先级排序）。而且，系统管理单元 1125 执行与参与协同操作或从协同操作退出相关的每个电力管理装置 11 的状态控制。

[0246] 以上，描述了电力管理装置 11 的功能配置。另外，在此描述的电力管理装置 11 的功能配置仅为一个示例，在需要时，可以增加除以上之外的功能。

[0247] (1-3) 显示在显示单元上的内容

[0248] 接下来，将参考图 10 至图 13 更加具体地描述显示在显示单元上的内容。图 10 至图 13 是用于说明显示在显示单元上的内容的图。

[0249] 如先前所述，多种信息被显示在电力管理装置 11 的显示单元 116 上。例如，如图 10 所示，已经注册在电力管理装置 11 中的设备列表与每个设备的电力消费一起显示在电力管理装置 11 的显示单元上。在此，电力消费可以被显示为数值，或者如图 10 所示，例如显示为柱状图的形式。对于装置，诸如插座扩展装置（可以通过选择显示器上的“插座扩展装置”将多个设备连接到插座扩展装置），可以掌握连接至插座扩展装置的各个设备的电力消费。

[0250] 如图 11 所示，显示单元 116 还可以显示连接至电力管理装置 11 的设备的认证状态。通过显示这种信息，电力管理装置 11 的用户可以容易地区分哪个设备已经被认证，其能够增加用户维护的效率。

[0251] 另外，如图 12 所示，用于每个使用位置的电力消费和记账金额的列表可以被显示在显示单元 116 上。通过显示这种信息，例如，用户可以容易地掌握备用电力是否被不必要地消费了。

[0252] 如图 13 所示，在显示单元 116 上显示电力消费时，还可以区分已经使用的电力的类型（即，电力是在系统外部使用的电力还是在系统内使用的电力）。

[0253] (1-4) 隐藏电力消费模式

[0254] 在此，将参考图 14 至图 18 描述隐藏电力消费模式的方法。

[0255] 被管理块 12 的电力消费模式反映用户的生活风格模式。作为一个示例，在图 14 中所示的电力消费模式中，峰值在整天都出现。从该电力消费模式可以明白，用户整天都在家。而且，由于消费峰值大多数在约 0:00（午夜）消失，可以明白，用户在午夜左右上床睡觉。而在图 15 中所示的电力消费模式中，虽然大峰值出现在约 7:00 和在 21:00，但只有很少峰值出现在一天的其他时间。该电力消费模式暗示，用户约 7:00 离开家，并且直到接近 21:00 都不在。

[0256] 这样，电力消费模式反映用户的生活模式。如果这种电力消费模式被恶意第三方知悉，则这样的第三方可以滥用电力消费模式。作为示例，第三方可以尝试在用户不在时进入用户的家里，当用户在家时进行高压销售访问，或者当用户睡觉时进行抢劫。

[0257] 为此原因，需要严格管理关于电力消费的信息，或者提供隐藏电力消费模式的配置。如先前所述，通过由电力供应者管理的电力信息收集装置 4 收集与电力供应者系统 5 提供的电力量相关的信息。这意味着，关于被管理块 12 的电力消费的时间序列模式将暴露给至少一个电力供应者。

[0258] 为此原因，除了以上措施之外，优选提供用于隐藏电力消费模式的配置，以防止用户的生活风格模式被第三方发现。隐藏电力消费模式的一种方式是，在由电力供应者系统 5 提供的电力量的时间序列模式与用户的生活风格模式之间创建差异。例如，电力供应者系

统 5 可以在用户不在家时供电，或者局部系统可以在用户在家时停止接收来自电力供应者系统 5 的电力。

[0259] 使用电力存储装置 128 实现这种措施。例如，可以将用户不在家时从电力供应者系统 5 接收的所提供电力存储在电力存储装置 128 中，并且当用户在家时，使用存储在电力存储装置 128 中的电力，以抑制从电力供应者系统 5 提供的电力量。为了进一步增加安全性，优选执行对电力存储装置 128 的充电 / 放电控制，以使电力消费模式变为指定模式，从而尽量根除由于用户的生活风格模式导致的出现在电力消费模式中的特征。

[0260] 平均化

[0261] 如图 16 所示，一个可能示例是执行电力存储装置 128 的充电 / 放电控制以使电力消费恒定的方法。为了使电力消费为恒定值，可以在电力消费低于恒定值时增加存储在电力存储装置 128 中的电力，并且可以在电力消费高于恒定值时增加电力存储装置 128 的放电。这种控制由电力管理装置 11 执行。除了电力存储装置 128 的充电 / 放电控制之外，可以在电力消费者之间交易电力，和 / 或使用电动交通工具 124 等的蓄电池执行充电 / 放电控制。这样，通过使电力消费恒定，可以根除由于用户的生活风格模式导致的出现在电力消费模式中的特征。结果，可以根除由于电力消费模式的滥用导致的用户遭受犯罪行为的危险。

[0262] 复杂化

[0263] 注意，只要电力消费模式和生活风格模式之间存在差异，就不必将电力消费设定为恒定值。为了使电力消费为恒定值，需要具有足够容量以吸收电力消费中的峰值的电力存储装置 128。然而，具有这种大容量的电力存储装置 128 很贵，并且仅仅为了隐藏电力消费模式而在普通家庭中提供这种装置不太现实。为此原因，优选使用小容量的电力存储装置 128 在电力消费模式和生活风格模式之间创建差异的方法。如图 17 所示，这种方法的一个可能示例使电力消费模式变复杂（即，增加电力消费模式的复杂性）。

[0264] 以下描述使电力消费模式变复杂以在模式各处生成相对小的峰值和波谷的一种可能方法。虽然大容量电力存储装置 128 会是将大峰值抑制为接近平均值所需要的，但是可以使用容量小很多的存储装置生成和移动相对小的峰值。虽然可以使以一天为单位的电力消费模式变复杂，还可以有效地使电力消费模式变复杂，以生成每天的不同电力消费模式和 / 或根除基于星期几或日期的循环。使事件的定时（诸如，尤其容易被滥用的外出、回家、就寝、起床）变复杂的设置也能够在不使电力存储装置 128 的充电 / 放电控制过度复杂的情况下充分抑制不正当行为。

[0265] 模式化

[0266] 而且，如图 18 所示，还可以想到控制电力消费模式以基本匹配邻居的平均模式的方法。基于其他人的生活风格模式获得邻居的平均模式。这意味着，需要进行少量电力控制，以使特定用户的电力消费模式与邻近的平均模式匹配。与当电力消费被控制变为恒定值时相比，应该可以使用低容量的电力存储装置 128 隐藏具体用户的生活风格模式。当这样控制电力消费时，在邻居的电力管理装置 11 之间交换电力信息。使用信息分析单元 1123 的功能或分析服务器 34 的功能计算邻居的平均模式。基于所计算出的平均模式，对电力存储装置 128 执行充电 / 放电控制。

[0267] (1-5) 由电力管理装置进行的多种控制

[0268] 现在将参考图 19 简要描述上述局部电力管理系统 1 的电力管理装置 11 执行的多种控制操作。图 19 是用于说明由电力管理装置进行的多种控制的概要的图。

[0269] 如图 19 所示，电力管理装置 11 执行对将被管理的配电装置 121、可控制插座 123、电动交通工具 124、可控制设备 125、插座扩展装置 127 等的控制。即，电力管理装置 11 对将被管理的设备执行多种控制操作，诸如，电力存储控制、平均化控制、交易控制、供电切换控制、异常切换控制、恢复控制、认证 / 注册控制、信息收集 / 信息处理控制、外部访问控制、以及服务链接控制。除了这种控制之外，充电控制是关于电力使用和存储的控制，诸如，在白天使用被管理块内的多种类型的发电装置生成的电力，而在夜晚使用外部电力。

[0270] 如图 19 所示，电力管理装置 11 通过参考与电力资源相关的信息、与优先级排序相关的信息、与控制条件（参数）相关的信息等，执行这种控制。

[0271] 如图 19 所示，例如，与电力资源相关的信息是与电力管理装置 11 所属的局部电力管理系统 1 能够使用的电力资源相关的信息。如图 19 所示，这种电力资源可以粗略地被分类为外部电力和家庭电力（或“系统内部电力”）。外部电力是从局部电力管理系统 1 外部提供的电力，并且一个示例可以为从供电公司等提供的标准电力。系统内部电力是在局部电力管理系统 1 内管理的电力，示例可以是存储在电力存储装置中的电力，由发电装置生成的电力，存储在电动交通工具中的电力，以及存储在蓄电池模块中的电力。注意，此处的表达“存储在电力存储装置中的电力”不仅指存储在所谓的专用电力存储装置中的电力，还包括在能够由电力管理装置 11（诸如，计算机、家用电器、或移动电话）控制的装置中设置的蓄电池等中存储的电力。电力管理装置 11 还能够使用这种信息来存储表示哪个电力资源提供了被存储在电力存储装置中的电力的信息。

[0272] 如图 19 所示，例如，与优先级排序相关的信息是设定供电的优先级排序的信息。如果停止对用于为食物和饮料保鲜的冰箱或者维护系统安全的安全相关设备供电，或者如果用于照明或控制设备的电力停止，则变得难以实现这种功能，其可能不利地影响用户。从而，电力管理装置 11 能够对这种设备提供不受限制的电力，以保证维持这种功能。电力管理装置 11 还能够通过适当地对优先级排序被设置为“电力节省模式 (POWERSAVING MODE)”的设备（诸如，电视或空调）的供电进行控制来抑制电力使用。电力管理装置 11 还能够设定“关机 (POWER OFF)”优先级排序，一个示例是能够实现控制以使得充电器的电力正常关断。注意，图 19 中所示的优先级排序仅是示例，电力管理装置 11 中设置的优先级排序不限于图 19 中所示的示例。

[0273] 如图 19 所示，例如，与控制条件相关的信息是设定电力管理装置 11 的控制条件的信息。作为一个示例，这种控制条件可以被粗略地分为，例如，与电力的使用环境相关的条件、与电力的使用时段相关的条件、与电力使用模式相关的条件、以及与异常相关的条件。如图 19 所示，可以为各个条件设置更详细的条件项。注意，图 19 中所示的控制条件仅是示例，并且电力管理装置 11 中设置的控制条件不限于图 19 中所示的示例。

[0274] 基于这种信息，电力管理装置 11 实现对系统 1 中的各个设备的控制，如图 19 所示。通过这样做，电力管理装置 11 能够执行对被管理的各个设备的充电控制，控制设备的操作，以及更新设备的固件。例如，电力管理装置 11 能够执行诸如“在 XX 点钟启动饭煲的功能”的控制。还可以将这种控制链接至电力估计功能（其是设置在电力管理装置 11 中的另一功能），以及在电力便宜的时段内启动多个功能。电力管理装置 11 还能够与设置在系

统 1 外部的服务器协同操作，以给用户提供多种服务。例如，外部设置的服务器能够使用由电力管理装置 11 输出的输出信息来提供服务等，使得可以容易地检查分开住的家庭成员是否具有正常电力使用状态（即，这种家庭成员正常生活，没有健康问题）。

[0275] 这种控制不仅能够由电力管理装置 11 实现，还能够由例如设置在电力管理系统 1 中的可控制插座 123、插座扩展装置 127 等实现。

[0276] 为了实现这种控制，电力管理装置 11 存储信息，诸如图 20 中所示的信息，并且还将这种信息注册在系统 1 外部设置的系统管理服务器 33 中。图 20 是用于说明由电力管理装置 11 管理的多种信息的图。

[0277] 如图 20 所示，电力管理装置 11 存储诸如分配给装置的标识号（ID）的信息，与制造商、型号等相关的信息，在系统中的注册日期、以及情况。另外，电力管理装置 11 存储诸如用户名、地址、电话号码、记账信息（与账户等相关的信息）、以及拥有电力管理装置 11 的用户的紧急联系方式等信息。电力管理装置 11 还存储与被分配给系统 1 中存在的配电装置 121 的 ID、制造商名称、型号、注册日期、状态等相关的信息。另外，电力管理装置 11 存储与被分配给系统 1 中存在的多种类型可控制设备 125 的 ID、制造商名称、型号、注册日期、状态等相关的信息。

[0278] 通过存储这种信息，电力管理装置 11 可以发送获取多种信息的请求和 / 或向设置在系统 1 外部的服务器提供多种服务的请求。例如，电力管理装置 11 能够参考用于特定可控制设备 125 的制造商信息，访问由该制造商管理的服务器，以及从被访问服务器获取与可控制设备 125 相关的多种信息。

[0279] 注意，除了能够由电力管理装置 11 控制的可控制设备 125（即，配电装置 121、可控制插座 123、电动交通工具 124、插座扩展装置 127、电力存储装置 128、以及发电装置 129、130）之外，还存在不可控制设备和 / 或不可控制插座（为不能被控制的装置）存在于局部电力管理系统 1 中的情形。为此原因，电力管理装置 11 根据什么类型的装置（可控制设备或不可控制设备）连接至什么类型的插座（可控制插座或不可控制插座）来选择用于交换信息的装置、控制供电的方法等。注意，如下所述，除非特别说明，措辞“可控制设备 125”还包括可以被控制的设备类型，诸如可控制插座 123、电动交通工具 124、插座扩展装置 127、电力存储装置 128 等。

[0280] 图 21 是用于说明通信装置、认证装置、以及根据插座的类型和被连接设备的类型设置的供电控制的组合的图。从图 21 可以清楚地看出，一种类型的插座以及连接至这种插座的一种类型的被连接设备的组合可以粗略地被划分为四种模式。

[0281] 当可控制设备 125 连接至可控制插座 123 时，电力管理装置 11 能够与可控制插座 123 和可控制设备 125 通信并对其进行控制。从而，当被连接设备将电力信息发送至电力管理装置 11 时，例如，被连接设备（即，可控制设备 125）可以使用 ZigBee 将电力信息发送至电力管理装置 11。可控制插座 123 可以使用例如 ZigBee 或 PLC 来将电力信息发送至电力管理装置 11。此外，在对被连接设备进行认证期间，被连接设备（可控制设备 125）能够使用例如 ZigBee 来执行与电力管理装置 11 的认证。关于对被连接设备的供电的控制，电力管理装置 11 可以将控制命令发送至配电装置 121。在一些情况下，可控制插座 123 还可以执行对被连接设备的供电的有限控制。

[0282] 当不可控制设备 126 连接至可控制插座 123 时，被连接设备可能不能与电力管理

装置 11 执行认证处理。这意味着，在这种情况下，被连接设备和电力管理装置 11 无法执行设备认证。在这种情况下的电力信息传输可以经由例如 ZigBee 或 PLC，由不可控制设备 126 连接至的可控制插座 123 来执行。关于对被连接设备的供电的控制，电力管理装置 11 可以将控制命令发送至配电装置 121。而且，在一些情况下，可控制插座 123 可以对被连接设备的供电执行有限控制。

[0283] 当可控制设备 125 连接至不可控制插座时，被连接设备可以使用例如 ZigBee 来与电力管理装置 11 执行设备认证处理，并且将电力信息发送至电力管理装置 11。而且，关于对被连接设备的供电的控制，电力管理装置 11 可以将控制命令发送至配电装置 121。

[0284] 当不可控制设备 126 连接至不可控制插座时，被连接设备不能与电力管理装置 11 执行设备认证处理或者将电力信息发送至电力管理装置 11。而且，由于不能控制对被连接设备的供电，电力管理装置 11 不断地对被连接设备供电。

[0285] (1-6) 设备管理单元的配置

[0286] 对上述设备的控制基于由设置在电力管理装置 11 中的信息管理单元 112 获得的多种信息来执行。现在将参考图 22 详细地描述设置在电力管理装置 11 的信息管理单元 112 中的设备管理单元 1121 的具体配置。图 22 是示出根据本实施例的设备管理单元 1121 的配置的框图。

[0287] 设备管理单元 1121 主要包括 :密钥生成单元 1501、系统注册单元 1503、被管理设备注册单元 1505、被管理设备信息获取单元 1507、被管理设备信息输出单元 1509、被排除设备指定单元 1511、信息篡改检测单元 1513、以及电力使用证书管理单元 1515。

[0288] 作为一个示例，密钥生成单元 1501 可以通过 CPU（中央处理单元）、ROM（只读存储器）、RAM（随机存取存储器）等实现。密钥生成单元 1501 生成在局部电力管理系统 1 中使用的多种类型密钥，诸如，公开密钥、私密密钥、或公共密钥，以及用于在局部电力管理系统 1 和设置在系统 1 外部的装置之间进行通信的多种类型的密钥，诸如，公开密钥、私密密钥、或公共密钥。密钥生成单元 1501 使用已由例如系统管理服务器 33 或证书机构服务器 35 披露的公开参数，来生成当生成这种密钥时使用的多种参数或生成密钥本身。密钥生成单元 1501 将所生成的参数或密钥安全地存储在存储单元 113 等中。

[0289] 根据来自系统注册单元 1503 或被管理设备注册单元 1505 的请求，实现由密钥生成单元 1501 执行的密钥生成处理，随后描述。一旦密钥生成处理结束，密钥生成单元 1501 就可以将所生成的密钥等输出至作出请求的处理单元（系统注册单元 1503 或被管理设备注册单元 1505）。密钥生成单元 1501 可以向作出请求的处理单元（系统注册单元 1503 或被管理设备注册单元 1505）通知密钥生成处理结束，使得处理单元然后可以从特定位置（例如，存储单元 113）获取所生成的密钥等。

[0290] 密钥生成单元 1501 执行密钥生成处理时的协议不限于指定协议，并且例如可以使用在局部电力管理系统 1 内设置的或者由与服务器达成的协议所确定的协议。

[0291] 系统注册单元 1503 由例如 CPU、ROM、RAM 等实现。系统注册单元 1503 是执行经由广域通信单元 114 将电力管理装置 11 本身注册在管理局部电力管理系统 1 的系统管理服务器 33 中的处理的处理单元。

[0292] 系统注册单元 1503 首先经由广域通信单元 114 连接至系统管理服务器 33，并且实现与系统管理服务器 33 的具体认证处理。接下来，系统注册单元 1503 将指定的注册信息

发送至系统管理服务器 33，以将电力管理装置 11 本身注册在系统管理服务器 33 中。

[0293] 系统注册单元 1503 发送至系统管理服务器 33 的注册信息的一个示例是图 20 中所示的信息。

[0294] 随后将详细地描述由系统注册单元 1503 实现的注册处理的具体示例。

[0295] 被管理设备注册单元 1505 由例如 CPU、ROM、RAM 等实现。被管理设备注册单元 1505 与能够经由局部通信单元 111 进行通信的可控制插座 123、电动交通工具 124、可控制设备 125、插座扩展装置 127、电力存储装置 128、发电装置 129、130 等执行通信，并且将建立了通信的设备注册为被管理设备。当这种可控制装置连接至电源插座（可控制插座 123、插座扩展装置 127、不可控制插座）和 / 或被接通时，被管理设备注册单元 1505 与这种装置执行指定认证处理，并且在认证之后执行指定注册处理。

[0296] 被管理设备注册单元 1505 从可控制装置获取该装置特有的标识号（设备 ID）、制造商名称、型号、电力使用、被连接插座的 ID 等作为注册信息。被管理设备注册单元 1505 将所获取的注册信息注册在存储单元 113 等中所存储的数据库中。被管理设备注册单元 1505 还经由广域通信单元 114 将所获取的注册信息发送至系统管理服务器 33，以将该信息注册在系统管理服务器 33 中。

[0297] 随后将更详细地描述被管理设备注册单元 1505 的详细配置。随后还将详细地描述由被管理设备注册单元 1505 执行的注册处理的具体示例。

[0298] 被管理设备信息获取单元 1507 由例如 CPU、ROM、RAM 等实现。被管理设备信息获取单元 1507 经由局部通信单元 111 从注册在电力管理装置 11 中的被管理设备获取多种信息。如图 8 所示，例如，示出设备的操作状态的信息、示出设备的使用状态的信息、环境信息、电力信息等都可以被给定为从被管理设备获取的信息的示例。被管理设备信息获取单元 1507 还能够从被管理设备获取除了上述信息之外的多种信息。

[0299] 被管理设备信息获取单元 1507 还能够将从被管理设备获取的多种信息传递至被管理设备信息输出单元 1509 和被排除设备指定单元 1511，将在随后描述。如果设备管理单元 1121 包括信息篡改检测单元 1513，则被管理设备信息获取单元 1507 可以将从被管理设备获取的多种信息传递至信息篡改检测单元 1513。

[0300] 被管理设备信息输出单元 1509 由例如 CPU、ROM、RAM 等实现。被管理设备信息输出单元 1509 将被管理设备信息获取单元 1507 从被管理设备获取的多种信息输出至电力管理装置 11 的指定处理单元，和 / 或经由广域通信单元 114 将该信息输出至设置在电力管理装置 11 外部的装置。而且，如随后所描述的，如果被管理设备将用于检测信息是否已经被篡改的数据嵌入到该信息中，则当嵌入有该数据的这种信息被传递至分析服务器 34 时，被管理设备信息输出单元 1509 起到中介者的作用。

[0301] 被排除设备指定单元 1511 由例如 CPU、ROM、RAM 等实现。被排除设备指定单元 1511 基于由被管理设备信息获取单元 1507 从被管理设备获取的多种信息，指定要从局部电力管理系统 1 排除的被管理设备。可以基于已经获取的多种信息来确定被排除设备，或者可以基于不能获取正常情况下可用的信息来确定。指定被排除设备的方法不限于具体方法，可以使用任意方法。

[0302] 信息篡改检测单元 1513 由例如 CPU、ROM、RAM 等实现。如果用于检测信息是否已经被篡改的数据被嵌入到由被管理设备信息获取单元 1507 从被管理设备获取的信息中，

则信息篡改检测单元 1513 验证这种数据并且检测该信息是否已经被篡改。电子水印可以被给定为信息中所嵌入的这种数据的一个示例。

[0303] 在检测到该信息已经被篡改时，信息篡改检测单元 1513 可以向被排除设备指定单元 1511 通知这种结果。通过这样做，被排除设备指定单元 1511 变得能够从系统 1 中排除信息已被篡改的设备。

[0304] 随后将描述由信息篡改检测单元 1513 执行的篡改检测处理。

[0305] 电力使用证书管理单元 1515 由例如 CPU、ROM、RAM 等实现。在包括电力管理装置 11 的局部电力管理系统 1 中，在一些情况下，电力可以被提供给不属于系统 1 的可控制设备 125 等。为了这样做，如下所述，可控制设备 125 等从接收供电的系统 1 外部，将电力使用证书颁发至对接收供电的系统进行管理的电力管理装置 11。电力使用证书是具有特定格式的证书，表示是否已经接收到供电。电力使用证书管理单元 1515 管理所颁发的电力使用证书，并且验证所颁发的电力使用证书是否为官方证书。当所颁发的电力使用证书为官方证书时，电力使用证书管理单元 1515 能够使用电力使用证书对与所提供电力相关的记账执行控制。

[0306] 随后将详细地描述由电力使用证书管理单元 1515 执行的处理。

[0307] 被管理设备注册单元的配置

[0308] 接下来，将参考图 23 详细地描述被管理设备注册单元 1505 的配置。图 23 是用于说明被管理设备注册单元 1505 的配置的框图。

[0309] 如图 23 所示，被管理设备注册单元 1505 包括被管理设备认证单元 1551、签名生成单元 1553、以及签名验证单元 1555。

[0310] 被管理设备认证单元 1551 由例如 CPU、ROM、RAM 等实现。如果未被注册在由电力管理装置 11 管理的局部电力管理系统 1 中的可控制设备 125 等被连接，则被管理设备认证单元 1551 使用由密钥生成单元 1501 生成的密钥等来认证未被注册的可控制设备 125 等。该认证处理可以是使用公开密钥的公开密钥认证处理，或者可以是使用公共密钥的公共密钥认证处理。通过与随后描述的签名生成单元 1553 和签名验证单元 1555 协作，被管理设备认证单元 1551 执行对被管理设备的认证处理和注册处理。

[0311] 签名生成单元 1553 由例如 CPU、ROM、RAM 等实现。签名生成单元 1553 使用由密钥生成单元 1501 生成的密钥等来生成具体签名（数字签名）和 / 或用于执行认证处理的可控制设备 125 等的证书。签名生成单元 1553 将与所生成的签名相关的信息和 / 或证书注册在存储单元 113 等中存储的数据库中，并且经由局部通信单元 111 将所生成的签名和 / 或证书发送至执行认证处理的可控制设备 125 等。

[0312] 签名验证单元 1555 由例如 CPU、ROM、RAM 等实现。签名验证单元 1555 使用由密钥生成单元 1501 生成的密钥等来验证由执行验证处理的可控制设备 125 等发送至电力管理装置 11 的签名（数字签名）和 / 或证书。如果签名和 / 或证书的验证成功，则签名验证单元 1555 将与验证成功的签名和 / 或证书相关的信息注册在存储单元 113 等中存储的数据库中。如果签名和 / 或证书的验证失败，则签名验证单元 1555 可以取消认证处理。

[0313] 随后将描述由被管理设备注册单元 1505、被管理设备认证单元 1551、签名生成单元 1553、以及签名验证单元 1555 协同对被管理设备执行认证处理和注册处理的具体示例。

[0314] 信息篡改检测单元的配置

[0315] 接下来，将参考图 24 详细地描述信息篡改检测单元 1513 的配置。图 24 是用于说明信息篡改检测单元 1513 的配置的框图。

[0316] 如图 24 所示，信息篡改检测单元 1513 还包括嵌入位置指定单元 1561、电子水印提取单元 1563、以及电子水印验证单元 1565。

[0317] 通过根据本实施例的局部电力管理系统 1，可以将适于这些信息的电子水印数据嵌入到诸如电流、电压、温度、以及湿度的物理数据中，或者嵌入到使用这种物理数据计算出的多种信息中。通过验证电子水印数据，局部电力管理系统 1 中的装置和能够与局部电力管理系统 1 双向通信的多种类型服务器能够检测物理数据（在下文中物理数据包括使用物理数据计算出的多种信息）是否已被篡改。

[0318] 嵌入位置指定单元 1561 由例如 CPU、ROM、RAM 等实现。通过对已经使用预定信号处理电路嵌入有电子水印的物理数据进行分析，嵌入位置指定单元 1561 根据与数据对应的信号的特征，指定电子水印信息的嵌入位置。当指定电子水印信息的嵌入位置时，嵌入位置指定单元 1561 向电子水印提取单元 1563 通知与指定的嵌入位置相关的信息。注意，如果电子水印的嵌入位置在可控制设备 125 等与电力管理装置 11 之间预先确定，则可以不必执行对嵌入位置的指定处理。

[0319] 电子水印提取单元 1563 由例如 CPU、ROM、RAM 等实现。电子水印提取单元 1563 基于与嵌入位置指定单元 1561 所提供的嵌入位置相关的信息，从物理数据提取电子水印信息。电子水印提取单元 1563 将从物理数据提取的电子水印传递至电子水印验证单元 1565，随后描述。

[0320] 电子水印验证单元 1565 由例如 CPU、ROM、RAM 等实现。电子水印验证单元 1565 首先基于与可控制设备 125 等共享的共享信息以及由电子水印提取单元 1563 提取的物理数据生成电子水印信息。为了生成电子水印信息，使用散列函数、伪随机数发生器、公开密钥加密、公共密钥加密、另一加密原语（例如，消息认证码 (MAC)）等。此后，电子水印验证单元 1565 将所生成的电子水印信息与电子水印提取单元 1563 所提取的电子水印信息进行比较。

[0321] 如果所生成的电子水印信息与所提取的电子水印信息相同，则电子水印验证单元 1565 判断由可控制设备 125 生成的物理数据等未被篡改。而如果所生成的电子水印信息与所提取的电子水印信息不同，则电子水印验证单元 1565 判断物理数据已经被篡改。

[0322] 如果物理数据被篡改，则电子水印验证单元 1565 通知被排除设备指定单元 1511。通过这样做，被排除设备指定单元 1511 能够从局部电力管理系统 1 中排除其操作可能已经被修改的可控制设备 125 等。

[0323] 以上完成了设备管理单元 1121 的配置的详细描述。

[0324] (1-7) 信息分析单元的配置

[0325] 接下来，将详细地描述信息分析单元 1123 的配置。图 25 是用于说明信息分析单元的配置的框图。

[0326] 信息分析单元 1123 是生成次级信息的处理单元，诸如图 8 所示的信息分析单元，次级信息是多种数据的分析结果并且基于由设备管理单元 1121 获取或生成的信息。如图 25 所示，例如，信息分析单元 1123 包括设备状态判断单元 1601 和电力状态判断单元 1603。

[0327] 设备状态判断单元 1601 由例如 CPU、ROM、RAM 等实现。基于由设备管理单元 1121

获取的多种被管理设备信息，设备状态判断单元 1601 判断各个被管理设备的设备状态。当作为判断的结果，被管理设备的状态被判断为异常时，设备状态判断单元 1601 经由显示单元 116 向用户通知异常，并且还请求控制单元 115 控制被判断为处于异常状态的被管理设备。

[0328] 电力状态判断单元 1603 由例如 CPU、ROM、RAM 等实现。电力状态判断单元 1603 基于由设备管理单元 1121 从多个装置获取的电力信息，来判断电力状态由电力管理装置 11 管理的局部电力管理系统 1 中的电力状态。当作为判断结果，被管理设备的状态被判断为异常时，电力状态判断单元 1603 经由显示单元 116 向用户通知异常，并且还请求控制单元 115 控制被判断为处于异常状态的被管理设备。

[0329] 以上完成了根据本实施例的电力管理装置 11 的功能的一个示例的描述。上述多种组成元件可以使用通用部件和电路来配置，或者可以使用专用于各个组成元件的功能的硬件来配置。可替选地，各个组成元件的功能均可以由 CPU 等来执行。从而，可以根据当实现本实施例时的主流技术水平适当地改变所使用的配置。

[0330] 注意，用于实现根据以上实施例的电力管理装置的功能的计算机程序可以被创建并安装在个人计算机等中。还可以提供其上存储有计算机程序的计算机可读记录介质。作为示例，记录介质可以为磁盘、光盘、磁光盘、或闪存。上述计算机程序还可以例如经由网络分配，而不使用记录介质。

[0331] (1-8) 可控制设备的配置

[0332] 接下来，将参考图 26 详细地描述根据本实施例的可控制设备的配置。图 26 是用于说明根据本实施例的可控制设备的配置的框图。

[0333] 如图 26 所示，可控制设备 125 主要包括控制单元 2001、传感器 2003、蓄电池 2005、功能提供单元 2007、局部通信单元 2009、输入单元 2011、显示单元 2013、存储单元 2015 等。

[0334] 控制单元 2001 由例如 CPU、ROM、RAM 等实现。控制单元 2001 是执行对设置在可控制设备 125 中的处理单元的执行控制的处理单元。如先前所述，控制单元 2001 还将与可控制设备 125 相关的初级信息等发送至电力管理装置 11。另外，当已经从临时注册了可控制设备 125 的电力管理装置接收到供电时，控制单元 2001 生成电力使用证书，如随后所述。注意，随后将描述控制单元 2001 的配置。

[0335] 传感器 2003 由监控蓄电池状态的电流传感器或电压传感器或者监控可控制设备 125 的安装位置处的周围环境的能够获取多种物理数据的传感器（诸如温度传感器、湿度传感器、气压计等）构成。基于控制单元 2001 的控制，传感器 2003 以指定时间间隔或在任意定时测量多种物理数据，并且将所获得的物理数据作为传感器信息输出至控制单元 2001。

[0336] 蓄电池 2005 是设置在可控制设备 125 中的电力存储装置，由一个或多个电池 (cell) 构成，并且提供可控制设备 125 操作所需要的电力。电力由外部电力或存在于系统 1 中的发电装置 129、130 提供给蓄电池 2005，并且被存储在蓄电池 2005 中。蓄电池 2005 由控制单元 2001 控制，并且以指定时间间隔或任意定时将多种物理数据作为蓄电池信息输出至控制单元 2001。

[0337] 注意，虽然图 26 示出了可控制设备 125 装配有蓄电池 2005 的示例，但是根据可控制设备 125 的类型，可以使用不设置蓄电池 2005 并且直接给可控制设备 125 提供电力的配

置。

[0338] 功能提供单元 2007 由例如 CPU、ROM、RAM、以及多种设备等实现。功能提供单元 2007 是实现由可控制设备 125 提供给用户的指定功能（例如，做饭功能、制冷功能、或记录和执行多种内容的功能）的处理单元。功能提供单元 2007 基于控制单元 2001 的控制向用户提供这种功能。

[0339] 局部通信单元 2009 由例如 CPU、ROM、RAM、以及通信装置等实现。局部通信单元 2009 是用于经由局部电力管理系统 1 内构建的通信网络进行通信的通信装置。局部通信单元 2009 能够经由局部电力管理系统 1 内构建的通信网络与根据本实施例的电力管理装置 11 通信。

[0340] 输入单元 2011 由例如 CPU、ROM、RAM、以及输入设备等实现。输入单元 2011 是使用户能够输入信息的输入设备。注意，作为示例，键盘、按钮等被用作输入单元 2011。还可以结合随后描述的显示单元 2013 和输入单元 2011，以构建触摸面板。

[0341] 显示单元 2013 由例如 CPU、ROM、RAM、以及输出装置等实现。显示单元 2013 是用于显示关于可控制设备 125 的电力消费的信息、用户信息、记账信息、与电力管理相关的其他信息、与局部电力管理系统 1 外部的电力管理相关的信息、与电力交易相关的信息等的显示设备。注意，作为示例，LCD、ELD 等被用作显示设备。

[0342] 存储单元 2015 是设置在可控制设备 125 内的存储装置的一个示例。存储单元 2015 存储可控制设备 125 特有的识别信息、与可控制设备 125 所保存的多种密钥相关的信息、由可控制设备 125 保存的多种数字签名和 / 证书等。多种历史信息也可以记录在存储单元 2015 中。另外，当根据本实施例的可控制设备 125 执行处理时应该被存储的处理的多种参数和中间过程或多种数据库等，被适当地记录在存储单元 2015 中。可控制设备 125 的多种处理单元还能够自由地对存储单元 2015 进行读取和写入。

[0343] 控制单元的配置 - 第 1 部分

[0344] 以上完成了根据本实施例的可控制设备 125 的总体配置的描述。现在将参考图 27 详细地描述可控制设备 125 的控制单元 2001 的配置。

[0345] 如图 27 所示，可控制设备 125 的控制单元 2001 包括 ：认证处理单元 2021、传感器控制单元 2023、传感器信息输出单元 2025、蓄电池控制单元 2027、以及蓄电池信息输出单元 2029。

[0346] 认证处理单元 2021 由例如 CPU、ROM、RAM 等实现。认证处理单元 2021 与电力管理装置 11 一起基于指定协议执行认证处理，并且还执行将可控制设备 125 注册在电力管理装置 11 中的处理。当与电力管理装置 11 执行处理时，认证处理单元 2021 能够使用存储在存储单元 2015 等中的多种密钥、当制造可控制设备 125 时由制造商提供的数字签名或证书、以及多种参数等。由认证处理单元 2021 执行的认证处理不限于任何指定处理，并且可以根据系统 1 的内容和配置使用任意处理。

[0347] 传感器控制单元 2023 由例如 CPU、ROM、RAM 等实现。传感器控制单元 2023 是对设置在可控制设备 125 中的传感器 2003 进行控制的处理单元。传感器控制单元 2023 根据指定方法执行对传感器 2003 的控制，以指定时间间隔或在任意定时获取由传感器 2003 测量的物理数据，并且将物理数据输出至传感器信息输出单元 2025，随后描述。

[0348] 传感器信息输出单元 2025 由例如 CPU、ROM、RAM 等实现。传感器信息输出单元

2025 经由局部通信单元 2009 将从传感器控制单元 2023 输出的传感器信息输出至电力管理装置 11。当输出传感器信息时，传感器信息输出单元 2025 还可以实现预处理，诸如降噪处理和数字化处理。传感器信息输出单元 2025 可以使用从传感器控制单元 2023 获取的信息来生成多种类型的次级信息，并将这种信息作为传感器信息输出。

[0349] 蓄电池控制单元 2027 由例如 CPU、ROM、RAM 等实现。蓄电池控制单元 2027 是对设置在可控制设备 125 中的蓄电池 2005 进行控制的处理单元。蓄电池控制单元 2027 使用存储在蓄电池 2005 中的电力以使可控制设备 125 起作用，并且根据状态将存储在蓄电池 2005 中的电力提供至可控制设备 125 的外部。蓄电池控制单元 2027 根据指定方法执行对蓄电池 2005 的控制，以指定时间间隔或在任意定时获取由蓄电池 2005 测量的物理数据，并将物理数据输出至蓄电池信息输出单元 2029，如随后描述。

[0350] 蓄电池信息输出单元 2029 由例如 CPU、ROM、RAM 等实现。蓄电池信息输出单元 2029 经由局部通信单元 2009 将从蓄电池控制单元 2027 输出的蓄电池信息输出至电力管理装置 11。当输出蓄电池信息时，蓄电池信息输出单元 2029 还可以实现预处理，诸如降噪处理和数字化处理。蓄电池信息输出单元 2029 还可以使用从蓄电池控制单元 2027 获取的信息来生成多种次级信息，并且将次级信息作为蓄电池信息输出。

[0351] 控制单元的配置 - 第 2 部分

[0352] 可控制设备 125 的控制单元 2001 可以具有以下描述的配置以代替图 27 中所示的配置。现在将参考图 28 详细地描述设置在可控制设备 125 中的控制单元 2001 的另一种配置。

[0353] 如图 28 所示，可控制设备 125 的控制单元 2001 可以包括 ：认证处理单元 2021、传感器控制单元 2023、蓄电池控制单元 2027、以及篡改检测信息生成单元 2031。

[0354] 由于图 28 中所示的认证处理单元 2021 具有与图 27 中所示的认证处理单元 2021 相同的配置并且实现相同的效果，所以省略其详细描述。类似地，除了将传感器控制信息和蓄电池信息输出至篡改检测信息生成单元 2031 之外，图 28 中所示的传感器控制单元 2023 和蓄电池控制单元 2027 具有与图 27 中所示的相应处理单元相同的配置并且实现相同的效果。从而，省略其详细描述。

[0355] 篡改检测信息生成单元 2031 由例如 CPU、ROM、RAM 等实现。篡改检测信息生成单元 2031 基于从传感器控制单元 2023 输出的传感器信息和从蓄电池控制单元 2027 输出的蓄电池信息，生成用于检测信息是否已被篡改的篡改检测信息。篡改检测信息生成单元 2031 经由局部通信单元 2009 将所生成的篡改检测信息发送至电力管理装置 11。电力管理装置 11 还可以将篡改检测信息生成单元 2031 生成的篡改检测信息传递至设置在局部电力管理系统 1 外部的多个服务器，诸如，分析服务器 34。

[0356] 篡改检测信息生成单元的配置

[0357] 现在将参考图 29 描述篡改检测信息生成单元 2031 的详细配置。图 29 是用于说明篡改检测信息生成单元的配置的框图。

[0358] 如图 29 所示，篡改检测信息生成单元 2031 还包括 ：设备表征信息生成单元 2033、电子水印生成单元 2035、嵌入位置确定单元 2037、以及电子水印嵌入单元 2039。

[0359] 设备表征信息生成单元 2033 由例如 CPU、ROM、RAM 等实现。设备表征信息生成单元 2033 基于从传感器控制单元 2023 和蓄电池控制单元 2027 输出的传感器信息和蓄电池

信息来生成设备表征信息，设备表征信息是表征可控制设备 125 的表征量信息。设备表征信息生成单元 2033 可以使用传感器信息和蓄电池信息本身作为设备表征信息，或者可以将使用传感器信息和蓄电池信息新生成的信息用作设备表征信息。设备表征信息生成单元 2033 将所生成的设备表征信息输出至嵌入位置确定单元 2037 和电子水印嵌入单元 2039，随后描述。

[0360] 注意，设备表征信息生成单元 2033 可以在生成设备表征信息之前验证输入的传感器信息和蓄电池信息。在这种情况下，设备表征信息生成单元 2033 可以参考存储在存储单元 2015 等中的数据库等来获取物理数据（诸如，传感器信息和蓄电池信息）的取值范围，并且判断所获得的物理数据是否存在于该范围内。而且，设备表征信息生成单元 2033 可以分析所获取的物理数据，并且确认可控制设备 125 没有呈现异常行为。如果设备表征信息生成单元 2033 通过执行这样的验证检测出异常行为或者物理数据的合法性被确认，则设备表征信息生成单元 2033 可以经由显示单元 2013 向用户通知这种状态。

[0361] 电子水印生成单元 2035 由例如 CPU、ROM、RAM 等实现。电子水印生成单元 2035 使用在可控制设备 125 与电力管理装置 11 或外部服务器（诸如分析服务器 34）之间被共享的共享信息（诸如与密钥信息和标识号相关的信息），以生成要被用作篡改检测信息的电子水印信息。

[0362] 作为示例，由电子水印生成单元 2035 生成的电子水印信息可以使用共享信息本身、基于共享信息生成的伪随机串、使用可控制设备 125 特有的唯一值（诸如 ID 信息）生成的信息等来生成。如果生成和嵌入电子水印信息的方法或者嵌入电子水印信息本身不被第三方所知，则可以通过使用利用这种信息生成的电子水印信息来检测对信息的篡改。

[0363] 还可以经由电力管理装置 11 将嵌入了由以下方法生成的电子水印信息的物理数据传递至诸如分析服务器 34 的外部服务器。同时，还存在用作中间装置的电力管理装置 11 被恶意第三方等接管的危险。在这种情况下，接管电力管理装置 11 的该第三方可能从事非法行为，诸如重新使用接管之前的篡改检测信息以防止外部服务器的真正用户、管理者等注意到该接管。为此，除了以上描述的信息之外还通过使用时间信息定期地生成电子水印信息，电子水印生成单元 2035 能够检测诸如电力管理装置 11 以上述方式被接管的现象。

[0364] 为了生成电子水印信息，电子水印生成单元 2035 能够使用多种技术，诸如散列函数、公开密钥加密、随机数发生器、公共密钥加密、另一加密原语 (MAC) 等。在这种情况下，被输出的电子水印信息的数据大小被设置为 m 个比特。

[0365] 这样，根据本实施例的电子水印生成单元 2035 使用物理数据生成电子水印信息，而不使用物理数据本身作为电子水印信息。

[0366] 电子水印生成单元 2035 将所生成的电子水印信息输出至电子水印嵌入单元 2039，随后描述。

[0367] 嵌入位置确定单元 2037 由例如 CPU、ROM、RAM 等实现。嵌入位置确定单元 2037 分析从设备表征信息生成单元 2033 传递的设备表征信息，并且确定篡改检测信息在设备表征信息中的嵌入位置。更具体地，嵌入位置确定单元 2037 确定将在设备表征信息中具有等于或大于指定阈值的大值的区域、具有高离差的区域、与噪声区域对应的区域、当频域上的数据被处理时的高频域等作为嵌入位置。如果电子水印信息被嵌入到数据的某个区域，诸如具有高噪声的区域和具有高 SN 比的区域中，则对设备表征信息的总体倾向（例如，统计

特性）基本没有影响。这意味着，通过使用这种区域作为电子水印信息的嵌入位置，不必独立于设备表征信息发送电子水印信息，并且甚至仅具有用于接收设备表征信息的功能的电力管理装置 11 都可以检测篡改。

[0368] 嵌入位置确定单元 2037 将与所确定的嵌入位置相关的位置信息输出至电子水印嵌入单元 2039，随后描述。注意，当电子水印信息的嵌入位置被预先确定时，不需要执行该处理。

[0369] 电子水印嵌入单元 2039 由例如 CPU、ROM、RAM 等实现。电子水印嵌入单元 2039 基于从嵌入位置确定单元 2037 接收的与嵌入位置相关的位置信息，将由电子水印生成单元 2035 生成的电子水印信息嵌入到设备表征信息生成单元 2033 所生成的设备表征信息中。通过这样做，生成嵌入有电子水印信息的设备表征信息。

[0370] 电子水印嵌入单元 2039 可以再次对嵌入有电子水印信息的设备表征信息进行验证。通过执行这样的验证，在该信息包括超过设备表征信息的取值范围的值时，或者在异常行为被清楚地指示时，篡改检测信息生成单元 2031 可以重复嵌入电子水印信息的处理。而且，当嵌入尝试的次数等于或在预定阈值以上时，电子水印嵌入单元 2039 可以经由显示单元 2013 通知用户。

[0371] 注意，当时间信息被用于不仅验证信息是否被篡改，还验证电力管理装置 11 是否被接管时，这种时间信息可以被结合作为上述电子水印信息的一部分，或者这种时间信息可以独立于电子水印信息而被嵌入到设备表征信息中。

[0372] 以上完成了根据本实施例的可控制设备 125 的功能的一个示例的描述。上述多种组成元件可以使用通用部件和电路来配置，或者可以使用专用于各个组成元件的功能的硬件来配置。可替选地，各个组成元件的功能均可以由 CPU 等来执行。从而，可以根据当实现本实施例时的主流技术水平，适当地改变所使用的配置。

[0373] 例如，在图 26 中，示出蓄电池 2005 与可控制设备 125 整体地形成的情况，但是蓄电池还可以独立于可控制设备 125 形成。

[0374] 而且，除了图 26 中所示的处理单元之外，可控制设备 125 还可以包括诸如广域通信单元的通信功能。

[0375] 注意，用于实现根据以上实施例的电力管理装置的功能的计算机程序可以被创建并安装在个人计算机等中。还可以提供其上存储有计算机程序的计算机可读记录介质。作为示例，记录介质可以为磁盘、光盘、磁光盘、或闪存。上述计算机程序还可以例如经由网络分配，而不使用记录介质。

[0376] (1-9) 电力存储装置的配置

[0377] 接下来，将参考图 30 详细地描述根据本实施例的电力存储装置 128 的配置。图 30 是用于说明根据本实施例的电力存储装置的配置的框图。

[0378] 如图 30 所示，电力存储装置 128 主要包括：控制单元 2501、传感器 2503、电池 2505、局部通信单元 2507、显示单元 2509、存储单元 2511 等。

[0379] 控制单元 2501 由例如 CPU、ROM、RAM 等实现。控制单元 2501 是执行对设置在可控制设备 125 中的处理单元的执行控制的处理单元。控制单元 2501 还将与可控制设备 125 相关的先前描述的初级信息等发送至电力管理装置 11。而且，如果稍后描述的电池 2505 中出现问题如损坏，则控制单元 2501 执行对电池的重配置（电池配置的重新设置）。注意，随

后将详细描述控制单元 2501 的配置。

[0380] 传感器 2503 由对电池 2505 的状态进行监控的电流传感器或电压传感器或者对电力存储设备 128 的安装位置处的周围环境进行监控的能够获取多种物理数据的传感器（诸如温度传感器、湿度传感器、气压计等）构成。基于控制单元 2501 进行的控制，传感器 2503 以指定时间间隔或在任意定时测量多种物理数据，并且将所获得的物理数据作为传感器信息输出至控制单元 2501。

[0381] 电池 2505 是设置在电力存储装置 128 中的电力存储设备，由一个或多个电池构成，并且对电力存储装置 128 以及设置在电力存储装置 128 外部的装置供电。电力由外部电力或存在于系统 1 中的发电装置 129、130 提供给电池 2505，并且被存储在电池 2505 中。电池 2505 由控制单元 2501 控制，并且以指定时间间隔或任意定时将多种物理数据作为电池信息输出至控制单元 2501。

[0382] 局部通信单元 2507 由例如 CPU、ROM、RAM、以及通信装置等实现。局部通信单元 2507 是用于经由局部电力管理系统 1 内构建的通信网络进行通信的通信装置。局部通信单元 2507 能够经由局部电力管理系统 1 内构建的通信网络与根据本实施例的电力管理装置 11 通信。

[0383] 显示单元 2509 由例如 CPU、ROM、RAM、以及输出装置等实现。显示单元 2509 是用于显示关于电力存储装置 128 的电力消费的信息、用户信息、记账信息、与电力管理相关的其他信息、与局部电力管理系统 1 外部的电力管理相关的信息、与电力交易相关的信息等的显示设备。注意，作为示例，LCD、ELD 等被用作显示设备。

[0384] 存储单元 2511 是设置在电力存储装置 128 内的存储装置的一个示例。存储单元 2511 存储电力存储装置 128 特有的识别信息、与电力存储装置 128 所保存的多种密钥相关的信息、由电力存储装置 128 保存的多种数字签名和 / 证书等。多种历史信息也可以被记录在存储单元 2511 中。另外，当根据本实施例的电力存储装置 128 执行处理时应该被存储的处理的多种参数和中间过程或多种数据库等被适当地记录在存储单元 2511 中。电力存储装置 128 的多种处理单元还能够自由地对存储单元 2511 进行读取和写入。

[0385] 控制单元的配置 - 第 1 部分

[0386] 以上完成了根据本实施例的电力存储装置 128 的总体配置的描述。现在将参考图 31 详细地描述电力存储装置 128 的控制单元 2501 的配置。

[0387] 如图 31 所示，电力存储装置 128 的控制单元 2501 包括 ：认证处理单元 2521、传感器控制单元 2523、传感器信息输出单元 2525、电池控制单元 2527、以及电池信息输出单元 2529。

[0388] 认证处理单元 2521 由例如 CPU、ROM、RAM 等实现。认证处理单元 2521 与电力管理装置 11 一起基于指定协议执行认证处理，并且还执行将电力存储装置 128 注册在电力管理装置 11 中的处理。当与电力管理装置 11 执行处理时，认证处理单元 2521 能够使用存储在存储单元 2511 等中的多种密钥、制造电力存储装置 128 时由制造商提供的数字签名或证书、以及多种参数等。由认证处理单元 2521 执行的认证处理不限于任何指定处理，并且可以根据系统 1 的内容和配置使用任意处理。

[0389] 传感器控制单元 2523 由例如 CPU、ROM、RAM 等实现。传感器控制单元 2523 是控制设置在电力存储装置 128 中的传感器 2503 的处理单元。传感器控制单元 2523 根据指定方

法执行对传感器 2503 的控制，以指定时间间隔或在任意定时获取由传感器 2503 测量到的物理数据，并且将物理数据输出至传感器信息输出单元 2525，随后描述。

[0390] 传感器信息输出单元 2525 由例如 CPU、ROM、RAM 等实现。传感器信息输出单元 2525 经由局部通信单元 2507 将从传感器控制单元 2523 输出的传感器信息输出至电力管理装置 11。当输出传感器信息时，传感器信息输出单元 2525 还可以实现预处理，诸如降噪处理和数字化处理。传感器信息输出单元 2525 可以使用从传感器控制单元 2523 获取的信息，来生成多种类型的次级信息，并将这种信息作为传感器信息输出。

[0391] 电池控制单元 2527 由例如 CPU、ROM、RAM 等实现。电池控制单元 2527 是控制设置在电力存储装置 128 中的电池 2505 的处理单元。电池控制单元 2527 使用存储在电池 2505 中的电力以使电力存储装置 128 起作用，并且根据状态将存储在电池 2505 中的电力提供至电力存储装置 128 的外部。电池控制单元 2527 根据指定方法执行对电池 2505 的控制，以指定时间间隔或在任意定时获取由电池 2505 测量的物理数据，并将物理数据输出至电池信息输出单元 2529，如随后描述。

[0392] 电池信息输出单元 2529 由例如 CPU、ROM、RAM 等实现。电池信息输出单元 2529 经由局部通信单元 2507 将从电池控制单元 2527 输出的电池信息输出至电力管理装置 11。当输出电池信息时，电池信息输出单元 2529 还可以实现预处理，诸如降噪处理和数字化处理。电池信息输出单元 2529 还可以使用从电池控制单元 2527 获取的信息来生成多种类型的次级信息，并且将这种信息作为电池信息输出。

[0393] 控制单元的配置 - 第 2 部分

[0394] 电力存储装置 128 的控制单元 2501 可以具有以下描述的配置以代替图 31 中所示的配置。现在将参考图 32 详细地描述设置在电力存储装置 128 中的控制单元 2501 的另一种配置。

[0395] 如图 32 所示，电力存储装置 128 的控制单元 2501 可以包括 ：认证处理单元 2521、传感器控制单元 2523、电池控制单元 2527、以及篡改检测信息生成单元 2531。

[0396] 由于图 32 中所示的认证处理单元 2521 具有与图 31 中所示的认证处理单元 2521 相同的配置并且实现相同的效果，所以省略其详细描述。类似地，除了将传感器控制信息和电池信息输出至篡改检测信息生成单元 2531 之外，图 32 中所示的传感器控制单元 2523 和电池控制单元 2527 具有与图 31 中所示的相应处理单元相同的配置并且实现相同的效果。从而，省略其详细描述。

[0397] 篡改检测信息生成单元 2531 由例如 CPU、ROM、RAM 等实现。篡改检测信息生成单元 2531 基于从传感器控制单元 2523 输出的传感器信息和从电池控制单元 2527 输出的电池信息，生成用于检测信息是否已被篡改的篡改检测信息。篡改检测信息生成单元 2531 经由局部通信单元 2507 将所生成的篡改检测信息发送至电力管理装置 11。电力管理装置 11 还可以将篡改检测信息生成单元 2531 所生成的篡改检测信息传递至设置在局部电力管理系统 1 外部的多个服务器，诸如分析服务器 34。

[0398] 篡改检测信息生成单元的配置

[0399] 现在将参考图 33 描述篡改检测信息生成单元 2531 的详细配置。图 33 是用于说明篡改检测信息生成单元的配置的框图。

[0400] 如图 33 所示，篡改检测信息生成单元 2531 还包括 ：设备表征信息生成单元 2533、

电子水印生成单元 2535、嵌入位置确定单元 2537、以及电子水印嵌入单元 2539。

[0401] 除了基于从传感器控制单元 2523 输出的传感器信息和从电池控制单元 2527 输出的电池信息生成设备表征信息之外，设备表征信息生成单元 2533 具有与图 29 中所示的设备表征信息生成单元 2033 相同的功能并且实现相同的效果。从而，省略其详细描述。

[0402] 而且，电子水印生成单元 2535、嵌入位置确定单元 2537 以及电子水印嵌入单元 2539 具有与图 29 中所示的相应处理单元相同的功能并且实现相同的效果。从而，省略其详细描述。

[0403] 以上完成了根据本实施例的电力存储装置 128 的功能的一个示例的描述。上述多种组成元件可以使用通用部件和电路来配置，或者可以使用专用于各个组成元件的功能的硬件来配置。可替选地，各个组成元件的功能均可以由 CPU 等来执行。从而，可以根据当实现本实施例时的主导技术水平，适当地改变所使用的配置。

[0404] 例如，除了图 30 中所示的处理单元之外，电力存储装置 128 还可以包括诸如广域通信单元的通信功能。

[0405] 注意，用于实现根据以上实施例的电力存储装置的功能的计算机程序可以被创建并安装在具有电力存储装置的个人计算机等中。还可以提供其上存储有计算机程序的计算机可读记录介质。作为示例，记录介质可以为磁盘、光盘、磁光盘、或闪存。上述计算机程序还可以例如经由网络分配，而不使用记录介质。

[0406] (1-10) 电子水印信息的嵌入方法和验证方法的具体示例

[0407] 现在将详细地描述电子水印信息的嵌入方法和验证方法的具体示例。

[0408] 在智能、网络化、以及数字化的局部电力管理系统 1 中，电力管理装置 11 关于该系统中各个设备的电力使用与各设备和蓄电池进行通信，以优化整个系统中的电力使用。通过这样做，电力管理装置 11 监控来自各个设备 / 蓄电池的传感器信息以及状态 (如日期 / 时间、电价、温度、以及用户是在家还是外出)，并且根据这种状态执行诸如设置操作模式和各个设备的最大电流的控制。还可受益于多种服务，诸如经由电力管理装置 11 从家外进行控制，以制定由安全检验服务器支持的高度安全措施、以及最优化。

[0409] 当这样做时，由于可以从外部对设备和蓄电池进行访问，所以增加了安全威胁，诸如发送至设备或蓄电池的异常操作命令、从另一电力管理装置启动的对家用电力管理装置或设备或蓄电池的攻击、DoS 攻击、以及信息泄露。对这种威胁的可能对策包括 :由电力管理装置 11 进行业务 (traffic) 管理、防病毒措施、以及安装防火墙。为了对付未知攻击，假设用于设备或蓄电池的传感器信息和执行命令信息被发送至诸如分析服务器 34 的安全检验服务器，并且物理仿真或学习理论被用于估计危害程度和 / 或检测非法使用。

[0410] 然而，由于这种对策以电力管理装置正常操作为前提，当电力管理装置 11 的控制功能受到外部攻击者危害时，这种防御将会无效。而且，由于制造和管理成本导致的设备和蓄电池很可能具有相对弱的防御性，在电力管理装置 11 的控制功能受到危害的情况下，实际上可以想象，设备和蓄电池是无防御的。另外，虽然可以想到非法电力管理装置用作合法电力管理装置、篡改物理数据、并且将这种数据发送至安全检验服务器的攻击，但是由于对于服务来说很难区分非法电力管理装置和有效电力管理装置，所以很难检测这种攻击。由于与对计算机的传统攻击相比，对设备或蓄电池的攻击具有导致主要危害的较高风险，所以必须给电力管理装置以及设备和电池都提供特定级别的安全功能。

[0411] 为此，在本实施例中，如先前所描述的，可以将用于防止非法篡改的电子水印插入到从设备和蓄电池的传感器等获取的物理数据中。通过使用这种方法，甚至当物理数据在通信路径上被攻击者篡改时，仍可以检测到攻击。而且，甚至当电力管理装置的控制功能受到危害时，通过将包括时间信息的电子水印信息定期地发送至安全检验服务器，可以通过与服务的协作检测到控制功能已经受到危害。另外，通过使用电子水印信息，不必分别向物理数据发送诸如 MAC 的认证信息，这使得可以使用能够仅接收物理数据的电力管理装置。

[0412] 现在将通过给出示例来更具体地描述电子水印信息的嵌入方法和验证方法。注意，在以下解释中，假设电子水印信息被嵌入在特定时间获得的物理数据（设备表征信息）中。物理数据是由 n 个数据构成的时间序列数据，并且在时间 k（其中，$0 \leqslant k \leqslant n-1$）处的物理数据值被表示为 X_k。在各时间处的物理数据值从传感器等获取之后，经过离散化，并且被设置为 r 比特数据。电子水印信息的数据大小被设置为 m 比特。

[0413] 使用共享信息的电子水印信息的嵌入方法和验证方法

[0414] 现在将通过给出具体示例来详细描述使用共享信息的电子水印信息的嵌入方法和验证方法。

[0415] 具体示例 1

[0416] 首先，将描述由可控制设备 125 等执行的电子水印信息的嵌入方法。

[0417] 首先，篡改检测信息生成单元 2031 的嵌入位置确定单元 2037 使用指定信号处理电路等，从作为物理数据的设备表征信息等中选择具有大值的 p 个数据。此后，电子水印嵌入单元 2039 使用指定嵌入处理电路等，相继地将基于共享信息生成的电子水印信息按照时间序列顺序插入到从所选择的 p 个设备表征信息的最低有效位 (LSB) 开始数起的 q(k) 比特部分中。在此，q(k) 为满足以下给定的条件的值。

[0418] 表达式 1

[0419] $$1 \leq q(k) \leq r-1,\ 0 \leq k \leq p-1,\ \sum_{k=0}^{p-1} q(k) = m$$（条件 a）

[0420] 在一些情况下，在电子水印信息被嵌入之后的所选择的 p 个设备表征信息的值将等于或小于从第 p+1 个数据起的值。在这种情况下，篡改检测信息生成单元 2031 的设备表征信息生成单元 2033 校正除电子水印信息的嵌入位置之外的数据，使得从第 p+1 个值起的值低于嵌入 p 个电子水印信息之后的设备表征信息的最低值。篡改检测信息生成单元 2031 基于校正后的值更新电子水印信息，并且重复嵌入处理，直到满足条件为止。

[0421] 接下来，将描述通过电力管理装置 11 的信息篡改检测单元或者安全检验服务器（诸如分析服务器 34）的信息篡改检测单元执行的验证电子水印信息的方法。

[0422] 信息篡改检测单元的嵌入位置指定单元使用指定信号处理电路等，来从作为物理数据的设备表征信息等中指定具有大值的 p 个数据位置。接下来，电子水印提取单元使用表示指定数据位置的位置信息以及指定嵌入提取电路等，以便按照时间序列连续地提取从所选择的 p 个设备表征信息的 LSB 开始数起的 q(k) 个比特的值。此后，电子水印验证单元基于存储在存储单元等中的共享信息（诸如，密钥信息）生成电子水印信息，并将所生成的信息与由电子水印提取单元提取的电子水印信息进行比较。

[0423] 具体示例 2

[0424] 首先，将描述由可控制设备 125 实现的嵌入电子水印信息的方法。

[0425] 首先，篡改检测信息生成单元 2031 的嵌入位置确定单元 2037 使用指定信号处理电路等来执行由以下公式 101 表达的离散傅立叶变换或者由以下公式 102 表达的离散余弦变换，以将时域中的设备表征信息（物理数据）$(X_0, X_1, \ldots, X_{n-1})$ 变换为频域中的数据串 $(Y_0, Y_1, \ldots, Y_{n-1})$。

[0426] 表达式 2

[0427] $$y_j = \sum_{k=0}^{n-1} x_k e^{-\frac{2\pi i}{n}jk}, \quad j = 0, \cdots, n-1 \ldots \text{（公式 101）}$$

[0428] $$y_j = \begin{cases} \frac{\sqrt{2}}{n}\sum_{k=0}^{n-1} x_k \quad (j=0) \\ \frac{2}{n}\sum_{k=0}^{n-1} x_k \cos\frac{(2k+1)j\pi}{2n} \quad (j \neq 0) \end{cases} \ldots \text{（公式 102）}$$

[0429] 此后，嵌入位置确定单元 2037 按照从高频率开始的顺序选择 p 个高频分量（即，在公式 101 和 102 中 j 很大的分量）。接下来，电子水印嵌入单元 2039 使用指定嵌入处理电路等，将基于共享信息生成的电子水印信息相继地插入从所选择的 p 个频域数据的最低有效位 LSB 开始数起的 q(k) 比特部分中。在此，“q(k)”是满足以上给定条件的值。

[0430] 在此，作为在使用离散傅立叶变换时嵌入的方法，可以使用任意方法，诸如给实数和复数均一地指派，或者给大值指派优先级。

[0431] 接下来，电子水印嵌入单元 2039 使用指定信号处理电路等，以使嵌入电子水印信息之后的频域中的数据进行由公式 103 表达的离散傅立叶逆变换或者由公式 104 表达的离散余弦逆变换，以将该数据恢复为时域中的数据串。

[0432] 表达式 3

[0433] $$x_k = \frac{1}{n}\sum_{j=0}^{n-1} y_j e^{\frac{2\pi i}{n}jk}, \quad k = 0, \cdots, n-1 \ldots \text{（公式 103）}$$

[0434] $$x_k = \frac{1}{\sqrt{2}} y_0 + \sum_{j=1}^{n-1} y_j \cos\frac{(2k+1)j\pi}{2n}, \quad k = 0, \cdots, n-1 \ldots \text{（公式 104）}$$

[0435] 接下来，将描述通过电力管理装置 11 的信息篡改检测单元或安全检验服务器（诸如分析服务器 34）的信息篡改检测单元实现的验证电子水印信息的方法。

[0436] 信息篡改检测单元的嵌入位置指定单元首先使用指定信号处理电路等，执行由以上公式 101 表达的离散傅里叶变换或者由以上公式 102 表达的离散余弦变换，以将时域中的设备表征信息（物理数据）$(X_0, X_1, \ldots, X_{n-1})$ 变换为频域中的数据串 $(Y_0, Y_1, \ldots, Y_{n-1})$。接下来，嵌入位置指定单元按照从高频率开始的顺序选择 p 个高频分量（即，在公式 101 和 102 中 j 很大的分量）。通过这样做，可以指定电子水印信息嵌入的位置。此后，电子水印提取单元使用表示指定数据的位置的位置信息，并且使用预定嵌入提取电路等相继地提取从所选择的 p 个设备表征信息的最低有效位 LSB 开始数起的 q(k) 比特值。然后，电子水印验证单元基于存储在存储单元等中的共享信息（诸如，密钥信息）生成电子水印信息，并且将所生成的电子水印信息与由电子水印提取单元提取的电子水印信息进行比较。

[0437] 具体示例 3

[0438] 首先，将描述由可控制设备 125 等实现的嵌入电子水印信息的方法。

[0439] 首先，篡改检测信息生成单元 2031 的设备表征信息生成单元 2033 基于设备表征信息 X_k 生成差数据 $S_k = X_k - X_{k-1}(1 \leqslant k \leqslant n-1)$。接下来，嵌入位置确定单元 2037 选择 p-1 连续数据串 $S_k(t \leqslant k \leqslant t+p-2, 1 \leqslant t \leqslant n-p+1)$，使得 p-1 个连续差数据的和低于指定阈值 σ，并且所选 p-1 个数据在满足这种条件的连续数据串中具有最高平方和。

[0440] 此后，电子水印嵌入单元 2039 使用指定嵌入处理电路等，将基于共享信息生成的电子水印信息按照时间序列顺序相继地插入从所选择的 p 个设备表征信息 $X_k(t-1 \leqslant k \leqslant t+p-2)$ 的最低有效位 LSB 开始数起的 q(k) 比特部分。在此，“q(k)”是满足以上给定条件的值。

[0441] 关于嵌入电子水印信息之后的 p 个所选择的设备表征信息的连续差数据，可能存在以下情况：和低于阈值 σ 和 / 或平方和是满足这种条件的连续数据串中的最高者不再为真。在这种情况下，篡改检测信息生成单元 2031 的设备表征信息生成单元 2033 校正除了电子水印信息的嵌入位置之外的数据，使得以上给定的条件为真。篡改检测信息生成单元 2031 基于校正后的值更新电子水印信息，并且重复嵌入处理，直到以上条件为真为止。

[0442] 接下来，将描述由电力管理装置 11 和安全检验服务器（诸如，分析服务器 34）的信息篡改检测单元实现的验证电子水印信息的方法。

[0443] 信息篡改检测单元的嵌入位置指定单元首先生成用于设备表征信息 X_k 的差数据 $S_k = X_k - X_{k-1}(1 \leqslant k \leqslant n-1)$。接下来，嵌入位置指定单元选择 p-1 连续数据串 $S_k(t \leqslant k \leqslant t+p-2, 1 \leqslant t \leqslant n-p+1)$，其中，p-1 连续差数据的和低于预定阈值 σ，并且平方和是满足这种条件的连续数据串中的最高者。通过这样做，可以指定嵌入电子水印信息的位置。

[0444] 此后，电子水印提取单元使用表示指定数据的位置的位置信息和指定嵌入提取电路等，按照时间序列顺序相继地提取从所选择的 p 个设备表征信息 $X_k(t-1 \leqslant k \leqslant t+p-2)$ 的 LSB 开始数起的 q(k) 比特部分的值。接下来，电子水印验证单元基于存储在存储单元等中的共享信息（诸如，密钥信息）生成电子水印信息，并且将所生成的电子水印信息与由电子水印提取单元提取的电子水印信息进行比较。

[0445] 使用共享信息和时间信息的电子水印信息的嵌入方法和验证方法

[0446] 以上描述了使用共享信息的电子水印信息的嵌入方法和验证方法。接下来，将通过给出具体示例来描述使用共享信息和时间信息的电子水印信息的嵌入方法和验证方法。

[0447] 注意，由于使用共享信息和时间信息的电子水印信息还可以用于检测电力管理装置 11 是否被接管，这种信息的验证通常由诸如分析服务器 34 的安全检验服务器来执行。

[0448] 注意，当验证使用时间信息的电子水印信息时，诸如分析服务器 34 的安全检验服务器根据时间信息如何被嵌入来改变验证方法。即，如果时间信息与电子水印信息一起被嵌入，则在验证期间嵌入的时间信息被提取并且用于数据生成处理。如果未嵌入时间信息，则使用预先确定的时间信息或者基于用于设备表征信息的估计获取时间所选择的一个或多个时间信息，生成电子水印信息。

[0449] 具体示例 1

[0450] 首先，将描述由可控制设备 125 实现的嵌入电子水印信息的方法。

[0451] 篡改检测信息生成单元 2031 的电子水印生成单元 2035 使用指定电路等，基于从 n

个设备表征信息（物理数据）的最高有效位 (MSB) 开始数起的 r-m(1 ≤ m ≤ r-1) 比特串、诸如密钥信息的共享信息、时间信息、以及在一些情况下的其它信息，生成用于每个设备表征信息的 m 比特电子水印信息。

[0452] 此后，嵌入位置确定单元 2037 使用指定嵌入电路等，以将为每个设备表征信息生成的电子水印信息嵌入从设备表征信息的 LSB 开始的 m 比特部分。在这种情况下，整个电子水印信息的数据大小为 nm 比特。

[0453] 接下来，将描述由安全检验服务器（诸如，分析服务器 34）的信息篡改检测单元实现的验证电子水印信息的方法。

[0454] 首先，信息篡改检测单元的电子水印提取单元使用指定嵌入提取电路，以提取从 n 个设备表征信息中的每个的 LSB 开始数起的 m 比特数据作为电子水印信息。接下来，电子水印验证单元基于从 n 个设备表征信息的 MSB 开始数起的 r-m(1 ≤ m ≤ r-1) 比特串、诸如密钥信息的共享信息、时间信息、以及由嵌入侧使用的数据，生成用于每个设备表征信息的 m 比特电子水印信息。此后，电子水印验证单元基于存储在存储单元等中的共享信息（诸如，密钥信息）生成电子水印信息，并且将所生成的电子水印信息与由电子水印提取单元提取的电子水印信息进行比较。

[0455] 注意，虽然在以上说明中描述了时域中的数据，还可以使用关于频域数据的相同方式，该频域数据是通过经由离散傅立叶变换或离散余弦变换来转换设备表征信息（诸如，物理数据）而生成的。

[0456] 具体示例 2

[0457] 首先，将描述由可控制设备 125 等实现的嵌入电子水印信息的方法。

[0458] 篡改检测信息生成单元 2031 的嵌入位置确定单元 2037 使用指定信号处理电路等，从作为物理数据的设备表征信息等中选择具有大值的 p 个数据。

[0459] 此后，电子水印生成单元 2035 基于除了从所选择的 p 个设备表征信息的 LSB 开始数起的 q(k) 比特之外的每个比特 (nr-m 比特)、共享信息（诸如，密钥信息）、时间信息、以及在一些情况下的其它信息，生成 m 比特电子水印信息。在此，“q(k)”是满足以上给定条件的值。

[0460] 接下来，电子水印嵌入单元 2039 使用指定嵌入处理电路等，按照时间序列顺序将所生成的电子水印信息相继地插入从所选择的 p 个设备表征信息的 LSB 开始数起的 q(k) 比特部分中。

[0461] 在一些情况下，嵌入电子水印信息之后的所选择的 p 个设备表征信息的值等于或小于从第 p+1 个数据起的值。在这种情况下，篡改检测信息生成单元 2031 的设备表征信息生成单元 2033 校正除电子水印信息的嵌入位置之外的数据，使得从第 p+1 个值起的值低于嵌入 p 个电子水印信息之后设务表征信息的最低值。篡改检测信息生成单元 2031 基于校正后的值更新电子水印信息，并且重复嵌入处理，直到满足条件为止。

[0462] 接下来，将描述由安全检测服务器（诸如，分析服务器 34）的信息篡改检测单元实现的验证电子水印信息的方法。

[0463] 信息篡改检测单元的嵌入位置指定单元使用指定信号处理电路等，在作为物理数据的设备表征信息等中指定具有大值的 p 个数据位置。接下来，电子水印提取单元使用表示指定数据位置的位置信息和指定嵌入提取电路等，按照时间序列相继地提取从所选择的

p 个设备表征信息的 LSB 开始数起的 q(k) 比特的值。

[0464] 接下来，电子水印验证单元基于未嵌入电子水印信息的部分中的每比特 (nr-m 比特)、共享信息（诸如，密钥信息）、时间信息、由嵌入侧使用的数据，生成 m 比特电子水印信息。然后，电子水印验证单元将电子水印提取单元所提取的电子水印信息与已经生成的电子水印信息进行比较。

[0465] 具体示例 3

[0466] 首先，将描述由可控制设备 125 等实现的嵌入电子水印信息的方法。

[0467] 首先，篡改检测信息生成单元 2031 的嵌入位置确定单元 2037 使用指定信号处理电路等，来执行由以上公式 101 表达的离散傅立叶变换或者由以上公式 102 表达的离散余弦变换，以将时域中的设备表征信息（物理数据）$(X_0, X_1, \ldots, X_{n-1})$ 转换为频域中的数据串 $(Y_0, Y_1, \ldots, Y_{n-1})$。

[0468] 此后，嵌入位置确定单元 2037 按照从高频率开始的顺序选择 p 个高频分量（即，在公式 101 和 102 中 j 很大的分量）。

[0469] 此后，电子水印生成单元 2035 基于除从所选择的 p 个设备表征信息的 LSB 开始数起的 q(k) 比特之外的每个比特 (nr-m 比特)、共享信息（诸如，密钥信息）、时间信息、以及在一些情况下的其它信息，生成 m 比特电子水印信息。在此，“q(k)”是满足以上给定条件的值。

[0470] 接下来，电子水印嵌入单元 2039 使用指定嵌入处理电路等，将基于共享信息生成的电子水印信息相继地插入从所选择的 p 个频域数据的最低有效位 LSB 开始数起的 q(k) 比特部分中。

[0471] 在此，作为在使用离散傅立叶变换时嵌入的方法，可以使用任意方法，诸如给实数和复数均一地指派，或者给大值指派优先级。

[0472] 接下来，电子水印嵌入单元 2039 使用指定信号处理电路等，使嵌入电子水印信息之后的频域中的数据经受由公式 103 表达的离散傅立叶逆变换或者由公式 104 表达的离散余弦逆变换，以将数据恢复为时域中的数据串。

[0473] 接下来，将描述由安全服务器（诸如，分析服务器 34）的信息篡改检测单元实现的验证电子水印信息的方法。

[0474] 信息篡改检测单元的嵌入位置指定单元首先使用指定信号处理电路等，执行由以上公式 101 表达的离散傅里叶变换或者由以上公式 102 表达的离散余弦变换，以将时域中的设备表征信息（物理数据）$(X_0, X_1, \ldots, X_{n-1})$ 转换为频域中的数据串 $(Y_0, Y_1, \ldots, Y_{n-1})$。接下来，嵌入位置指定单元按照从高频率开始的顺序选择 p 个高频分量（即，在公式 101 和 102 中 j 很大的分量）。通过这样做，可以指定电子水印信息嵌入的位置。此后，电子水印提取单元使用表示指定数据的位置的位置信息，使用预定嵌入提取电路等，相继地提取从所选择的 p 个设备表征信息的最低有效位 LSB 开始数起的 q(k) 比特值。

[0475] 接下来，电子水印验证单元基于电子水印信息未嵌入的部分中的每比特 (nr-m 比特)、共享信息（诸如，密钥信息）、时间信息、由嵌入侧使用的数据，生成 m 比特电子水印信息。然后，电子水印验证单元将由电子水印提取单元提取的电子水印信息与已经生成的电子水印信息进行比较。

[0476] 具体示例 4

[0477] 首先，将描述由可控制设备 125 等实现的嵌入电子水印信息的方法。

[0478] 首先，篡改检测信息生成单元 2031 的设备表征信息生成单元 2033 基于设备表征信息 X_k 生成差数据 $S_k = X_k - X_{k-1}$ ($1 \leqslant k \leqslant n-1$)。接下来，嵌入位置确定单元 2037 选择 p-1 连续数据串 S_k ($t \leqslant k \leqslant t+p-2, 1 \leqslant t \leqslant n-p+1$)，使得 p-1 个连续差数据的和低于指定阈值 σ，并且所选 p-1 个数据在满足这种条件的连续数据串中具有最高平方和。

[0479] 此后，电子水印生成单元 2035 基于除从所选择的 p 个设备表征信息的 LSB 开始数起的 q(k) 比特之外的每个比特 (nr-m 比特)、共享信息 (诸如，密钥信息)、时间信息、以及在一些情况下的其它信息，生成 m 比特电子水印信息。在此，“q(k)”是满足以上给定条件的值。

[0480] 接下来，电子水印嵌入单元 2039 使用指定嵌入处理电路等，将基于共享信息生成的电子水印信息相继地插入从所选择的 p 个频域数据的最低有效位 LSB 开始数起的 q(k) 比特部分中。

[0481] 关于嵌入电子水印信息之后的 p 个所选择的设备表征信息的连续差数据，可存在以下情况 :和低于阈值 σ 和 / 或平方和是满足这种条件的连续数据串中的最高者不再为真。在这种情况下，篡改检测信息生成单元 2031 的设备表征信息生成单元 2033 校正除了电子水印信息的嵌入位置之外的数据，使得以上给定的条件为真。篡改检测信息生成单元 2031 基于校正后的值更新电子水印信息，并且重复嵌入处理，直到以上条件为真为止。

[0482] 接下来，将描述由电力管理装置 11 的信息篡改检测单元和安全检验服务器 (诸如，分析服务器 34) 的信息篡改检测单元实现的验证电子水印信息的方法。

[0483] 信息篡改检测单元的嵌入位置指定单元首先生成用于设备表征信息 X_k 的差数据 $S_k = X_k - X_{k-1}$ ($1 \leqslant k \leqslant n-1$)。接下来，嵌入位置指定单元选择 p-1 连续数据串 S_k ($t \leqslant k \leqslant t+p-2, 1 \leqslant t \leqslant n-p+1$)，其中，p-1 连续差数据的和低于预定阈值 σ，并且平方和是满足这种条件的连续数据串中的最高者。通过这样做，可以指定嵌入电子水印信息的位置。

[0484] 此后，电子水印提取单元使用表示指定数据的位置的位置信息和指定嵌入提取电路等，按照时间序列顺序相继地提取从所选择的 p 个设备表征信息 X_k ($t-1 \leqslant k \leqslant t+p-2$) 的 LSB 开始数起的 q(k) 比特部分的值。

[0485] 接下来，电子水印验证单元基于电子水印信息未嵌入的部分中的每比特 (nr-m 比特)、共享信息 (诸如，密钥信息)、时间信息、以及由嵌入侧使用的数据，生成 m 比特电子水印信息。然后，电子水印验证单元将由电子水印提取单元提取的电子水印信息与已经生成的电子水印信息进行比较。

[0486] 以上已经描述了使用共享信息的电子水印信息的嵌入方法和验证方法，以及使用共享信息和时间信息的电子水印信息的嵌入方法和验证方法，同时给出了具体示例。通过在根据本实施例的局部电力管理系统 1 中使用这种方法，可以检测诸如信息是否已被篡改和电力管理装置是否已被接管的进展。

[0487] 注意，虽然在以上解释中具体描述了将电子水印信息嵌入具有大值的区域中的情况，但是还可以实现当电子水印信息被嵌入具有高离差的区域、噪声区域等中时的相同处理。

[0488] (1-11) 注册电力管理装置的方法

[0489] 接下来，将参考图 34 和图 35 按照处理流程的顺序描述由电力管理装置 11 实现的注册电力管理装置的方法。图 34 是用于解释根据本实施例的注册电力管理装置的方法的流程图。图 35 是用于解释根据本实施例的注册电力管理装置的方法的具体示例的流程图。

[0490] 首先，将参考图 34 描述电力管理装置 11 的注册方法的整体流程。

[0491] 电力管理装置 11 的设备管理单元 1121 首先连接设置在局部电力管理系统 1 中的配电装置 121（步骤 S1001）。更具体地，设备管理单元 1121 从配电装置 121 获取在制造配电装置 121 时存储在配电装置 121 中的数字签名、证书等，并且自动地或经由在线识别来识别配电装置 121。根据用于可控制设备 125 等的识别处理和注册处理的流程，来执行用于配电装置 121 的识别处理和注册处理，随后描述。

[0492] 此后，设备管理单元 1121 将询问用户待注册信息（被注册信息）的内容的消息显示在设置于电力管理装置 11 中的显示单元 116 上。用户对设置在电力管理装置 11 中的输入单元 117（诸如，触摸面板或键盘）进行操作，并且将注册信息的内容（诸如，图 20 中所示的信息）输入至电力管理装置 11 中。通过这样做，设备管理单元 1121 能够获取注册信息（步骤 S1003）。

[0493] 接下来，设备管理单元 1121 经由广域通信单元 114 连接至系统管理服务器 33，并且由系统管理服务器 33 执行认证（步骤 S1005）。虽然可以使用任意技术连接至系统管理服务器 33 并且执行认证处理，但作为一个示例，使用公开密钥加密。

[0494] 在由系统管理服务器 33 执行的认证处理中，系统管理服务器 33 向电力管理装置 11 通知认证结果。设备管理单元 1121 参考所接收的认证结果，并且判断认证是否成功（步骤 S1007）。

[0495] 当由系统管理服务器 33 进行的认证处理失败时，设备管理单元 1121 确定写入认证结果中的错误内容（步骤 S1009）。在注册信息不完整的情况 (a) 下，设备管理单元 1121 返回至步骤 S1003，询问不完整注册信息的内容，并且获取正确内容。在注册信息并非不完整但认证失败的情况 (b) 下，设备管理单元 1121 连接至系统管理服务器 33 并且再次执行认证处理。而且，在认证失败连续反复的指定次数或更多的情况 (c) 下，设备管理单元 1121 取消对电力管理装置 11 的注册。

[0496] 同时，当由系统管理服务器 33 执行的认证处理成功时，设备管理单元 1121 将所获取的注册信息正式地发送至系统管理服务器 33（步骤 S1011），并且将电力管理装置 11 注册在系统管理服务器 33 的数据库中。

[0497] 通过根据上述流程执行处理，电力管理装置 11 的设备管理单元 1121 能够将电力管理装置 11 本身注册在系统管理服务器 33 中。注意，当电力管理装置 11 的注册成功时，电力管理装置 11 定期地与系统管理服务器 33 进行通信并且检验当前状态。

[0498] 注册电力管理装置的方法的具体示例

[0499] 接下来，将参考图 35 描述注册电力管理装置的方法的具体示例。图 35 示出使用公开密钥加密来注册电力管理装置的方法的示例。

[0500] 注意，假设在以下解释开始之前，电力管理装置 11 已经根据任意方法公开地获取了可用系统参数（公开参数）。还假设，例如，电力管理装置特有的识别信息 (ID) 和由系统管理服务器 33 生成的识别信息的数字签名已由制造商存储在该设备中。另外，假设系统管理服务器 33 具有系统管理服务器 33 特有的公开密钥和私密密钥。

[0501] 当电力管理装置 11 的用户已执行开始用于电力管理装置的注册处理的操作时，设备管理单元 1121 的密钥生成单元 1501 使用公开参数来生成由公开密钥和私密密钥构成的密钥对（步骤 S1021）。密钥生成单元 1501 将所生成的密钥对存储在存储单元 113 等中。

[0502] 接下来，系统注册单元 1503 使用系统管理服务器 33 的公开密钥对电力管理装置的识别信息、识别信息的数字签名、以及生成的公开密钥进行加密。此后，系统注册单元 1503 将所生成的密码作为证书颁发请求，经由广域通信单元 114 发送至系统管理服务器 33（步骤 S1023）。

[0503] 当获取从电力管理装置 11 发送的证书颁发请求时，系统管理服务器 33 首先验证附加至数字签名的签名的合法性（步骤 S1025）。更具体地，系统管理服务器 33 使用由服务器隐藏的私密密钥，来验证附加至电力管理装置的识别信息的数字签名是否有效。

[0504] 如果验证失败，则系统管理服务器 33 将表示认证失败的认证结果发送至电力管理装置 11。同时，如果验证成功，则系统管理服务器 33 将电力管理装置 11 的识别信息添加至由系统管理服务器 33 存储的数据库中的被管理列表中（步骤 S1027）。

[0505] 接下来，系统管理服务器 33 颁发用于由电力管理装置 11 生成的公开密钥的公开密钥证书（步骤 S1029），并且将所生成的公开密钥证书发送至电力管理装置 11。

[0506] 当接收到从系统管理服务器 33 发送的公开密钥证书时，电力管理装置 11 的系统注册单元 1503 验证公开密钥证书（步骤 S1031）。如果公开密钥证书的验证成功，则系统注册单元 1503 将注册信息发送至系统管理服务器 33（步骤 S1033）。注意，使用加密通信来执行对注册信息的这种发送。

[0507] 当接收到从电力管理装置 11 发送的注册信息时，系统管理服务器 33 将所接收到的注册信息注册在被管理列表中（步骤 S1035）。通过这样做，由电力管理装置 11 和系统管理服务器 33 执行的用于注册电力管理装置 11 的处理被认为成功（步骤 S1037）。

[0508] 以上已经描述了用于注册电力管理装置 11 的具体示例。注意，上述注册方法的具体示例仅为一个示例，根据本实施例的注册处理不限于以上示例。

[0509] (1-12) 注册可控制设备的方法

[0510] 接下来，将参考图 36 至图 38 描述将可控制设备 125 注册在电力管理装置 11 中的方法。图 36 是用于解释根据本实施例的注册可控制设备的方法的流程图。图 37 和图 38 是用于解释根据本实施例的注册可控制设备的方法的具体示例的流程图。

[0511] 注意，将可控制设备 125 作为由电力管理装置 11 管理的被管理设备的一个示例，描述该注册方法。以下描述的注册方法以与当将电动交通工具 124、电力存储设备 128、第一发电设备 129、以及第二发电设备 130 注册在电力管理装置 11 时的相同方式来执行。

[0512] 首先，将参考图 36 描述注册可控制设备 125 的方法的整体流程。

[0513] 当未被注册的可控制设备 125 连接至由电力管理装置 11 管理的局部电力管理系统 1 时，电力管理装置 11 的设备管理单元 1121 检测到可控制设备 125 连接至系统（步骤 S1041）。更具体地，电力管理装置 11 本身可以检测出可控制设备 125 被连接，或者配电装置 121 或电源插座（可控制插座 123 或插座扩展设备 127）可以检测出可控制设备 125 被连接，并且通知电力管理装置 11。作为该处理的结果，电力管理装置 11 能够掌握与可控制设备 125 所连接的插座相关的信息（位置信息）。

[0514] 接下来，设备管理单元 1121 对新连接的可控制设备 125 进行认证处理。该认证处

理可以使用任意技术来执行，例如，公开密钥加密。通过执行认证处理，设备管理单元 1121 从可控制设备 125 获取诸如图 20 中所示的信息。

[0515] 如果可控制设备 125 的认证失败，则设备管理单元 1121 结束对可控制设备 125 的注册处理。注意，如果设备管理单元 1121 确定尝试对可控制设备 125 进行认证，而不是突然终止注册处理，处理可以返回至步骤 S1043，在步骤 S1043 中重复进行认证处理。

[0516] 同时，当可控制设备 125 的认证成功时，设备管理单元 1121 经由广域通信单元 114 将可控制设备 125 注册在系统管理服务器 33 中（步骤 S1047）。接下来，设备管理单元 1121 向认证成功的可控制设备 125 颁发签名（数字签名）、证书等（步骤 S1049）。此后，设备管理单元 1121 将可控制设备 125 注册在存储单元 113 等中存储的管理数据库中（步骤 S1051）。

[0517] 注册可控制设备的方法的具体示例

[0518] 接下来，将参考图 37 和图 38 描述注册可控制设备的方法的具体示例。图 37 和图 38 是使用公开密钥加密注册可控制设备的方法的示例。

[0519] 注意，假设在以下解释开始之前，电力管理装置 11 已经根据任意方法公开地获取了可用系统参数（公开参数）。还假设例如电力管理装置特有的识别信息 (ID) 和系统管理服务器 33 所生成的识别信息的数字签名已经由制造商存储在该设备中，并且假设由公开密钥和私密密钥构成的密钥对也被存储在该设备中。还假设系统管理服务器 33 存储系统管理服务器 33 特有的公开密钥和私密密钥。最后，假设例如可控制设备 125 特有的识别信息 (ID) 和由系统管理服务器 33 生成的数字签名已经由制造商存储在可控制设备 125 内。

[0520] 首先，将参考图 37 描述最初注册可控制设备的方法的具体示例。

[0521] 当可控制设备 125 连接至系统 1 时（更具体地，当可控制设备 125 连接至可控制插座 123 等时）（步骤 S1061），在随后描述的过程中，电力管理装置 11 的被管理设备注册单元 1505 检测出可控制设备 125 已经被连接（步骤 S1063）。

[0522] 接下来，被管理设备注册单元 1505 获取注册条件，诸如，图 19 中所示的优先级排序（步骤 S1065）。更具体地，被管理设备注册单元 1505 将对用户询问注册条件的消息显示在电力管理装置 11 中所设置的显示单元 116 上。用户对设置在电力管理装置 11 中的输入单元 117（诸如，触摸面板或键盘）进行操作，并且将注册条件（诸如，图 19 中所示的注册条件）输入至电力管理装置 11 中。

[0523] 此后，被管理设备注册单元 1505 经由局部通信单元 111 将注册开始信号发送至可控制设备 125（步骤 S1067）。

[0524] 接收到注册开始信号的可控制设备 125 的认证处理单元 2021，将设备特有的识别信息 (ID) 和系统管理服务器 33 生成的数字签名作为设备注册请求发送至电力管理装置 11（步骤 S1069）。

[0525] 接收到设备注册请求的被管理设备注册单元 1505 使用系统管理服务器 33 的公开密钥，来验证所接收的数字签名的合法性（步骤 S1071）。当验证失败时，被管理设备注册单元 1505 将表示验证失败的验证结果发送至可控制设备 125。同时，当验证成功时，被管理设备注册单元 1505 请求系统管理服务器 33 注册可控制设备 125 的识别信息和 / 或可控制设备 125 的设备信息（包括制造商名称、型号等）（步骤 S1073）。

[0526] 当接收注册请求时，系统管理服务器 33 确认包括在注册请求中的可控制设备 125 是否是合法设备（即，设备是否已经被注册）（步骤 S1075）。当可控制设备 125 是合法设备

时，系统管理服务器 33 将所接收的设备信息添加至存储在系统管理服务器 33 中的数据库中的被管理列表中（步骤 S1077）。

[0527] 此后，系统管理服务器 33 从由系统管理服务器 33 本身存储的各个数据库或者从属于制造商等的服务器，获取与所注册的可控制设备 125 的规格相关的信息（设备规格信息），并且将所获取的信息发送至电力管理装置 11（步骤 S1079）。

[0528] 然后，电力管理装置 11 的被管理设备注册单元 1505 使用由被管理设备注册单元 1505 本身保存的密钥，颁发用于可控制设备的识别信息（ID）的签名（证书）（步骤 S1081）。此后，被管理设备注册单元 1505 将所颁发的签名与电力管理装置 11 的识别信息（ID）一起发送至可控制设备 125（步骤 S1083）。

[0529] 可控制设备 125 的认证处理单元 2021 将所接收的签名和电力管理装置 11 的识别信息（ID）存储到指定位置，诸如存储单元 2015 中（步骤 S1085）。电力管理装置 11 的被管理设备注册单元 1505 将可控制设备 125 的设备信息注册在存储单元 113 等中存储的管理数据库中（步骤 S1087）。通过这样做，最初注册可控制设备 125 的处理被认为成功（步骤 S1089）。

[0530] 图 37 示出可控制设备 125 被正式注册（最初注册）在电力管理装置 11 中的处理。然而，作为一个示例，还可能存在用户想要将已经被注册在用户家的电力管理装置 11 中的可控制设备 125 临时注册在朋友家设置的电力管理装置 11 中的情况。为此，根据本实施例的电力管理装置 11 设置有用于临时注册最初已经注册在另一电力管理装置 11 中的可控制设备 125 的注册处理。现在参考图 38 描述临时注册可控制设备 125 的处理。

[0531] 注意，假设在以下解释开始之前，电力管理装置 11 已经根据任意方法公开地获取了可用系统参数（公开参数）。还假设例如电力管理装置特有的识别信息（ID）和由系统管理服务器 33 生成的识别信息的数字签名已经由制造商存储在该设备中，并且假设由公开密钥和私密密钥构成的密钥对也被存储在该设备中。另外，还假设系统管理服务器 33 具有系统管理服务器 33 特有的公开密钥和私密密钥。最后，假设例如可控制设备 125 特有的识别信息（ID）和由系统管理服务器 33 生成的数字签名已经由制造商存储在可控制设备 125 内，并且假设所注册的电力管理装置的识别信息（ID）和签名已经被存储在可控制设备 125 中。

[0532] 当可控制设备 125 连接至系统 1 时（更具体地，当可控制设备 125 连接至可控制插座 123 等时）（步骤 S1091），在之前描述的过程中，电力管理装置 11 的被管理设备注册单元 1505 检测出可控制设备 125 已经被连接（步骤 S1093）。

[0533] 接下来，被管理设备注册单元 1505 获取注册条件，诸如，图 19 中所示的优先级排序（步骤 S1095）。更具体地，被管理设备注册单元 1505 将询问用户注册条件的消息显示在设置在电力管理装置 11 中的显示单元 116 上。用户对设置在电力管理装置 11 中的输入单元 117（诸如，触摸面板或键盘）进行操作，并且将注册条件（诸如，图 19 中所示的注册条件）输入至电力管理装置 11 中。

[0534] 接下来，被管理设备注册单元 1505 经由局部通信单元 111 将注册开始信号发送至可控制设备 125（步骤 S1097）。

[0535] 接收到注册开始信号的可控制设备 125 的认证处理单元 2021，将所注册的电力管理装置 11 的识别信息（ID）、所提供的数字签名、以及可控制设备 125 特有的识别信息（ID）

作为设备注册请求发送至电力管理装置 11（步骤 S1099）。

[0536] 接收到设备注册请求的被管理设备注册单元 1505 检验可控制设备 125 特有的并且包括在设备注册请求中的识别信息（ID）（步骤 S1101）。此后，基于可控制设备 125 特有的识别信息（ID），被管理设备注册单元 1505 向系统管理服务器 33 请求可控制设备 125 的证书（步骤 S1103）。

[0537] 在确认请求证书的可控制设备 125 不是包括在失效列表中的设备（步骤 S1105）之后，系统管理服务器 33 将所请求的证书发送至电力管理装置 11（步骤 S1107）。

[0538] 电力管理装置 11 的被管理设备注册单元 1505 验证可控制设备 125 所拥有的签名（从所注册的电力管理装置获取的签名）（步骤 S1109）。当签名的验证成功时，被管理设备注册单元 1505 将可控制设备 125 临时注册在电力管理装置 11 中（步骤 S1111）。通过这样做，电力管理装置 11 能够临时注册已经注册在另一电力管理装置 11 中的可控制设备 125。

[0539] (1-13) 注册可控制插座的方法

[0540] 接着，将参考图 39 描述的将可控制插座 123 注册在电力管理装置 11 中的方法。图 39 是用于解释根据本实施例的注册可控制插座的方法的流程图。

[0541] 注意，尽管下面的描述以可控制插座 123 为例，但是可以以同样的方式对插座扩展设备 127 执行这种注册方法。

[0542] 电力管理装置 11 的设备管理单元 1121 首先连接到配电装置 121（步骤 S1121），并从配电装置 121 获取关于系统 1 中存在的插座的信息（步骤 S1123）。“与插座相关的信息”的表述是指如下信息：诸如可控制插座或不可控制插座的指示、可控制插座的识别信息（ID）、制造商名称和型号、诸如电力供应量和电源限制等技术规格、系统内的插座的位置信息等等。

[0543] 接着，设备管理单元 1121 的被管理设备注册单元 1505 与系统中存在的可控制插座建立连接（步骤 S1125）。此后，被管理设备注册单元 1505 将已建立连接的可控制插座注册到存储在存储单元 113 等中的管理数据库中（步骤 S1127）。

[0544] 接着，被管理设备注册单元 1505 确认电力供应控制方法和如图 21 所示的那些设备认证手段，并将这种信息设置在管理数据库中。这样，当可控制设备 125 或不可控制设备 126 连接到可控制插座 123 时，电力管理装置 11 能够进行适当的电力供应控制和设备认证处理。

[0545] 接着，被管理设备注册单元 1505 判断是否已对每个插座（可控制插座）执行了该处理（步骤 S1131）。当存在未进行该处理的可控制插座时，被管理设备注册单元 1505 返回步骤 S1125 并继续该处理。当已经对每个可控制插座进行过该处理时，被管理设备注册单元 1505 正常结束该处理。

[0546] 这完成了对于根据本实施例在局部电力管理系统 1 中注册各种设备的处理的描述。

[0547] (1-14) 针对临时注册的可控制设备的计账处理

[0548] 现在将参考图 40 和 41，描述临时注册的可控制设备的记账处理。图 40 是用于解释临时注册的可控制设备的记账处理的图。图 41 是用于解释临时注册的可控制设备的记账处理的流程图。

[0549] 如上所述，可以设想如下情况：已在某个电力管理装置 11 中注册的可控制设备

125 被临时注册在管理不同的局部电力管理系统 1 的另一电力管理装置 11 中。当这样做时，可能出现如下情况：已临时注册的可控制设备 125 在另一个电力管理装置 11 的控制下，从该不同的局部电力管理系统 1 接收电力供应。

[0550] 图 40 示出了这种情况。如图 40 所示，属于局部电力管理系统 #1 的可控制设备 #1 已被注册在电力管理装置 #1 中。可控制设备 #1 已经从电力管理装置 #1 接收到电力管理装置 #1 的识别信息 (ID_{P1}) 和关于可控制设备 #1 识别信息的电力管理装置的数字签名 ($sig(ID_{P1})$)。这里，设想如下情况：可控制设备 #1 被临时注册在由电力管理装置 #2 管理的局部电力管理系统 #2（例如，公共电力供应站等）中，并且可控制设备 #1 从局部电力管理系统 #2 接收电力供应。这里，假定系统管理服务器 33 已经获得电力管理装置 #1 的识别信息 (ID_{P1}) 和电力管理装置 #2 的识别信息 (ID_{P2})。

[0551] 对于这种电力使用费用而言，优选的是，向注册有可控制设备 #1 的电力管理装置 #1 计费，并且对于电力管理装置 #1 而言，优选的是，采用记账服务器 32 实现指定的记账处理。仅当该设备存储了公开密钥和私密密钥时，这种方案才有可能，并且这当种信息未被存储时，电力管理装置 #2 将结束免费向可控制设备 #1 供应电力。注意，即使存储了由公开密钥和私密密钥组成的密钥对，也可以依据已做的设置许可免费电力供应。

[0552] 这种情况下的潜在问题是，当电力管理装置 #1 是非法装置时，即使由电力管理装置 #2 向可控制设备 #1 供应电力，计费也可能是无效的。为此，在本实施例中，在许可向可控制设备 #1 电力供应之前，电力管理装置 #2 确认电力管理装置 #1 的合法性，并确认可控制设备 #1 已正式注册到电力管理装置 #1 中。甚至当电力管理装置 #2 免费供应电力时，为了安全也应优选进行这种确认操作。也就是说，每当电力供应，电力管理装置 #2 使用电力管理装置 #1 的签名和 / 或证书等来验证电力管理装置 #1 和可控制设备 #1 之间的关系，并且电力管理装置 #2 还查询系统管理服务器 33 以检查电力管理装置 #1 和可控制设备 #1 的合法性。

[0553] 此外，在本实施例中，如以下参考图 41 所描述的，关于计费，通过将电力供应与官方证明电力已被使用的电力使用证书的交换结合，能够实现安全的记账处理。

[0554] 现在将参考图 41 描述已临时注册的可控制设备的记账处理的流程。注意，以下处理主要由可控制设备 125 的控制单元 2001 和电力管理装置 11 的设备管理单元 1121 执行。

[0555] 首先，可控制设备 #1 请求电力管理装置 #2 执行认证处理（步骤 S1141）。当请求认证时，可控制设备 #1 将电力管理装置 #1 的识别信息 (ID_{P1})、可控制设备 #1 的识别信息 (ID_{d1})、以及可控制设备 #1 中存储的 ID_{P1} 和 ID_{d1} 的数字签名发送到电力管理装置 #2。

[0556] 电力管理装置 #2 检查接收到的可控制设备的识别信息 (ID_{d1}) 是否存在于由电力管理装置 #2 自身管理的被管理列表中。电力管理装置 #2 也检查电力管理装置 #1 的识别信息 (ID_{P1}) 是否存在于由电力管理装置 #2 存储的证书列表中。这样，电力管理装置 #2 检查电力管理装置 #1（步骤 S1143）。

[0557] 如果电力管理装置 #1 的识别信息不存在于由电力管理装置 #2 存储的证书列表中，则电力管理装置 #2 向系统管理服务器 33 请求电力管理装置 #1 的证书（步骤 S1145）。根据对证书的请求，电力管理装置 #1 可以向系统管理服务器 33 通知可控制设备 #1 的识别信息。

[0558] 通过检查电力管理装置 #1 是否不在失效列表中，系统管理服务器 33 检查电力管

理装置 #1 的合法性（步骤 S1147）。如果电力管理装置 #1 的识别信息包括在失效列表中，则系统管理服务器 33 向电力管理装置 #2 通知这种情况并且电力管理装置 #2 错误地结束该处理。

[0559] 同时，电力管理装置 #2 向可控制设备 #1 请求由电力管理装置 #1 颁发的证书或者由电力管理装置 #1 生成的数字签名（步骤 S1149）。在接收到这个请求时，可控制设备 #1 向电力管理装置 #2 发送从电力管理装置 #1 提供的数字签名（$sig(ID_{P1})$）（步骤 S1151）。

[0560] 当系统管理服务器 33 确认了电力管理装置 #1 的合法性时，系统管理服务器 33 向电力管理装置 #2 发送存储在系统管理服务器 33 中的电力管理装置 #1 的证书（步骤 S1153）。

[0561] 电力管理装置 #2 验证从可控制设备 #1 发送的数字签名和 / 或证书（步骤 S1155），并且当验证成功时，电力管理装置 #2 允许对可控制设备 #1 的电力供应。此时，电力管理装置 #2 通知可控制设备 #1 电力收费还是免费。如果电力免费，则不进行以下步骤。

[0562] 由于验证成功，因此，电力管理装置 #2 在指定时间内向可控制设备 #1 供应电力（步骤 S1157）。

[0563] 接收了电力供应的可控制设备 #1 生成关于电力使用的消息作为证据，以证明消耗了给定时间的电力，并将该消息附有签名地发送到电力管理装置 #2（步骤 S1159）。附有签名的关于电力使用的消息是电力使用证书。注意，步骤 S1157 和步骤 S1159 的处理应当优选以固定的间隔重复进行，直至电力管理装置 #2 停止电力供应或者可控制设备 #1 从电网（局部电力管理系统）断开为止。

[0564] 电力管理装置 #2 将从电力管理装置 #1 获得的、增加了电力管理装置 #2 的识别信息（ID_{P2}）和设备证书的电力使用证书发送到系统管理服务器 33 中（步骤 S1161）。

[0565] 系统管理服务器 33 验证“可控制设备 #1 是否已经从电力管理装置 #2 购电”。使用该设备的证书，通过验证该电力使用证书来进行验证（步骤 S1163）。

[0566] 当电力使用证书验证成功时，系统管理服务器 33 请求记账服务器 32 执行记账处理（步骤 S1165）。此后，记账服务器 32 根据从系统管理服务器 33 请求的内容进行记账处理（步骤 S1167）。

[0567] 通过进行该处理，能够实现可以扩展到公共电力站的安全记账处理功能。

[0568] 注意，除电力管理装置 11 管理的可控制设备等之外，可以想到：装备有大容量蓄电池的电动交通工具 124 等可能会将蓄电池中存储的电力卖给另一个电网（局部电力管理系统）。这种情况也可采用图 41 所示的过程来处理。在这种情况下，电力管理装置 11 接收来自电动交通工具 124 等的电力，并且电力管理装置 11 向电动交通工具 124 等颁发电力使用证书。这里，优选地，已经购电的电力管理装置 11 主要负责将电力使用证书发送到系统管理服务器 33。

[0569] 还可以想到接受了电力供应的电力管理装置 11 非法地进行这种操作，例如，通过不向系统管理服务器 33 发送电力使用证书。在这种情况下，通过使注册了电动交通工具 124 等的电力管理装置 11 向系统管理服务器 33 发送存储在电动交通工具 124 等中的电力使用证书，可以检测这种非法活动。

[0570] (1-15) 对注册可控制设备的方法的修改

[0571] 这里，将参考图 42 至 48 详细描述注册上述可控制设备的方法的示例变型。图 42

至 47 是用于解释注册可控制设备的方法的修改的图，图 48 是用于解释注册可控制设备的方法的修改的流程图。

[0572] 如上所述，在局部电力管理系统 1 中，以防止向非法设备和非法蓄电池供应电力和防止非法设备及非法蓄电池连接到该系统为目的，对设备和蓄电池进行认证。下述根据本实施例的注册可控制设备的方法的示例变型的目的在于，提供一种注册方法，其能够有效地执行可控制设备或者包含多个蓄电池的蓄电装置的认证。

[0573] 在下面解释中，如图 24 所示，考虑如下情况 :电力管理装置 11 认证和注册表示为“A”到“H”的八个可控制设备 125。

[0574] 在上述方法中，对于可控制设备 125 重复电力管理装置 11 与一个可控制设备 125 之间所进行的一对一认证处理共 8 次。在这种情况下，当认证单个可控制设备 125 时，进行下列处理。也就是说，首先，电力管理装置 11 向可控制设备 125 发送包含随机数的挑战消息。接着，可控制设备 125 通过使用由可控制设备 125 存储的密钥对挑战消息进行操作来生成应答消息，并发送应答消息作为答复。此后，电力管理装置 11 验证接收的应答消息是否正确。

[0575] 这里，认证方法可被大致分类为两类，包括 :(i) 当执行操作以从挑战消息生成应答消息时，采用公开密钥加密中使用的私密密钥作为密钥的方法，使得应答消息是数字签名 ;以及 (ii) 使用利用电力管理装置 11 与可控制设备 125 之间共享的密钥的公共密钥加密的方法。

[0576] 该示例变型关注使用由以上 (i) 指示的数字签名的认证方法。这是因为这种认证方法包含能够使用称为批量验证 (batch verification) 和聚合签名 (aggregate signature) 技术的方法。

[0577] 这里，“批量验证”的表述是指能够在单次操作中对多个数字签名集中进行验证的验证技术，其中只有当全部数字签名正确时，验证算法才输出“验证成功”。通过使用该技术，较之于分别对各个数字签名进行验证的情况，可提高计算效率。

[0578] 批量验证处理的具体示例是 D.Naccache 等在 1994 年德国施普林格的 Eurocrypt 会议记录 94、计算机科学讲稿 Vol.950 中的“Can D.S.A beimproved ? Complexity trade-offs with the digital signature standard,”以及 M.Bellare 等在 1998 年德国施普林格的 Eurocrypt 会议记录 98、计算机科学讲稿 Vol.1403 中的“Fast Batch Verification for Modular Exponentiation and Digital Signatures,”中公开的方法。在本变型中，通过使用批量验证处理，可以改进计算效率。这些技术包括能够响应于各个不同消息集中验证由多个签名者生成的签名的技术。

[0579] “聚合签名”的表述是指如下验证技术 :其能够将多个签名聚合为单个签名，并且当对聚合签名进行验证处理时，只有当全部签名均正确时该验证算法才输出“验证成功”。这里，响应于各个不同的消息，可由多个签名者生成多个签名。

[0580] 聚合签名的具体示例是 D.Boneh 等在 2003 年德国施普林格的 Eurocrypt 会议记录 2003、计算机科学 Vol.2656 中的讲稿的“Aggregate and Verifiably Encrypted Signatures from Bilinear Maps,”以及 D.Boneh 等在 2003 年 CryptoBytes Vol.6，No.2 的“A Survey of Two Signature Aggregation Techniques,”中公开的方法。在这个变型中，通过使用聚合签名，可以改进计算效率。

[0581] 这里，如图 42 所示，考虑到如下情况：电力管理装置 11 认证八个可控制设备 125。在重复一对一认证的常见方法中，共进行八次验证处理，然而如图 42 下半部分所示，通过采用批量验证处理或聚合签名能够改进计算效率。

[0582] 注意，下述认证处理主要由电力管理装置 11 的设备管理单元 1121 和可控制设备 125 的控制单元 2001 执行。

[0583] 首先，电力管理装置 11 向可控制设备 A 到 H 发送挑战消息 C（步骤 S1171）。由于在该发送期间无需向各个可控制设备分别发送各消息，因此若通信网络是允许广播的环境，则可采用广播。

[0584] 可控制设备 A 到 H 分别对挑战消息 C 使用该设备中保存的用于公开密钥加密的私密密钥，以生成挑战消息 C 的应答消息，然后将所生成的应答消息作为答复发送到电力管理装置 11。

[0585] 例如，接收到挑战消息 C 时，可控制设备 A 使用由可控制设备 A 存储的私密密钥生成应答消息 RA 作为挑战消息 C 的答复（步骤 S1173）。此后，可控制设备 A 将生成的应答消息 RA 发送到电力管理装置 11（步骤 S1175）。

[0586] 类似地，接收到挑战消息 C 时，可控制设备 H 使用由可控制设备 H 存储的私密密钥生成应答消息 RH 作为挑战消息 C 的答复（步骤 S1177）。接着，可控制设备 H 将生成的应答消息 RH 发送到电力管理装置 11（步骤 S1179）。

[0587] 更具体地，应答消息 RA 到 RH 是各可控制设备 A 到 H 关于挑战消息 C 的数字签名。

[0588] 在此期间，电力管理装置 11 等待来自正进行验证处理的可控制设备 A 到 H 的应答消息。电力管理装置 11 收集来自八个可控制设备的应答消息，集中认证全部的应答消息 RA 到 RH（步骤 S1181），并验证全部应答消息是否都正确。可通过批量验证处理执行该验证或可通过使用聚合签名技术将八个应答消息聚合为单个数字签名并对所生成的数字签名进行验证来执行该验证。

[0589] 注意，尽管为了简化上述解释假定电力管理装置 11 已经知道每个可控制设备的公开密钥，但是可控制设备 A 到 H 可以将它们各自的公开密钥证书和应答消息一起发送到电力管理装置 11。

[0590] 这里，公开密钥证书是证书机构服务器 35 对于设备的识别信息（ID）和 / 或公开密钥的数字签名。这意味着可采用诸如批量验证或聚合签名之类的方法有效率地进行验证。

[0591] 当已经收集到各个可控制设备响应于来自电力管理装置 11 的挑战消息而发送的应答消息并且集中验证了应答消息时，在多数情况下，全部应答消息将是正确的并且验证结果将为“成功”。在此情况下，因为电力管理装置 11 已经确认全部可控制设备 A 到 H 的合法性，所以该处理可如常进行。

[0592] 然而，在某些情况下，在对 n 个设备进行集中验证处理期间，输出“验证失败”。这意味着这 n 个可控制设备中存在至少一个异常设备。因此，除了对正常设备进行新的集中验证处理之外，电力管理装置 11 指定异常的可控制设备并对这些异常设备进行单独处理是很重要的。

[0593] 通过将经过集中验证的可控制设备组重复划分为更小的组，可以指定异常设备。下面参考图 43 和 44 描述这样做的两种具体方法。

[0594] 第一种策略是指定异常的一个设备的最小值的方法，这样做所需迭代（计算负荷）次数为 O(log2n)。

[0595] 第二种策略是指定全部异常设备的方法，这样做所需迭代次数为 O(n)。

[0596] 现在详细描述基于各策略的方法。

[0597] 策略 1 是如下方法：从集中验证结果为“失败”的组中选择一个组（例如，该组具有最小数目的组成元件），并且重复执行集中验证，直至组中仅包含一个可控制设备。图 43 显示这种方法的示例。在图 43 中，可控制设备 A 到 H 中的三个可控制设备 C、E 和 F 异常。

[0598] 步骤 1 中，电力管理装置 11 向全部八个可控制设备发送挑战消息，并对八个可控制设备进行集中验证。如果验证结果是“失败”，则电力管理装置 11 转到步骤 2，其中由八个可控制设备组成的单个组被划分为两个组。

[0599] 在图 43 所示的示例中，电力管理装置 11 将组划分为由可控制设备 A 到 D 组成的组以及由可控制设备 E 到 H 组成的组，并将挑战消息发送到各个组。此后，电力管理装置 11 对组单元中所获得的应答消息进行集中验证。在图 43 所示的示例中，两个组的集中验证结果都是“验证失败”。

[0600] 接着，在步骤 3 中，电力管理装置 11 选择将被从验证结果为“失败”的当前组（在图 43 中，可控制设备 ABCD 组和可控制设备 EFGH 组）中（即，从两个组中）划分出去的下一个组。在图 43 所示的示例中，电力管理装置 11 选择由可控制设备 ABCD 组成的组，并进一步划分该组。在图 43 所示的示例中，以一组由可控制设备 AB 组成且另一组由可控制设备 CD 组成的形式，将由可控制设备 ABCD 组成的组分为两个具有两个设备的组。

[0601] 电力管理装置 11 然后向具有两个设备的两个组发送挑战消息，并对已接收到的应答消息进行集中验证。在图 43 所示的示例中，因为由可控制设备 AB 组成的组的验证结果为“成功”，所以确认可控制设备 A、B 都正常。同时，因为由可控制设备 CD 组成的组的验证结果是“失败”，理解可控制设备 C、D 中至少一个是异常。

[0602] 接着，在步骤 4 中，电力管理装置 11 将由可控制设备 CD 组成的组划分为具有单个设备的组，并对每个组进行验证处理。这样，电力管理装置 11 可以指定可控制设备 C 异常。

[0603] 在图 43 所示的示例中，可以按照四级步骤，从八个可控制设备中指定一个异常的可控制设备。一般地说，如果可控制设备数目是 n，则可以容易地设想出具有 n 个叶节点的二叉树，但是通过分组使得组成元件的数目大致二等分，可在作为二叉树的高度的 $\log_2(n+1)$ 个步骤中完成该处理。因为一个步骤中对最多两个组执行验证处理，因此验证处理的迭代次数为 $O(\log_2 n)$。

[0604] 接着，将描述策略 2。

[0605] 策略 2 是用于检测全部异常设备的方法。图 44 示出这种方法的示例。在图 44 中，可控制设备 A 到 H 中的三个可控制设备 C、E 和 F 异常。

[0606] 在步骤 1 中，电力管理装置 11 向全部八个可控制设备发送挑战消息，并对八个可控制设备进行集中验证。如果验证结果是“失败”，则电力管理装置 11 转到步骤 2，在步骤 2 中，由八个可控制设备组成的单个组被划分成两个组。

[0607] 在图 44 所示的示例中，电力管理装置 11 将组划分为由可控制设备 A 到 D 组成的组以及由可控制设备 E 到 H 组成的组，并将挑战消息发送到各个组。此后，电力管理装置 11 对组单元中所获得的应答消息进行集中验证。在图 44 所示的示例中，对两个组的集中验证

结果是“验证失败”。

[0608] 在策略 2 中，在步骤 3 中，对在先前步骤中验证为“失败”的全部组重复认证处理。在图 44 所示的示例中，由可控制设备 ABCD 组成的组被分成由可控制设备 AB 组成的组和由可控制设备 CD 组成的组。电力管理装置 11 还将由可控制设备 EFGH 组成的组划分为由可控制设备 EF 组成的组和由可控制设备 GH 组成的组。此后，电力管理装置 11 对生成的四个组分别进行验证处理。

[0609] 在图 44 所示的示例中，由可控制设备 AB 组成的组和由可控制设备 GH 组成的组的验证结果为“成功”，而由可控制设备 CD 组成的组和由可控制设备 EF 组成的组的验证结果为“失败”。

[0610] 接着，在步骤 4 中，电力管理装置 11 将由验证失败的可控制设备 CD 组成的组划分为由可控制设备 C 组成的组和由可控制设备 D 组成的组。以同样的方式，电力管理装置 11 将由验证失败的可控制设备 EF 组成的组划分为由可控制设备 E 组成的组和由可控制设备 F 组成的组。然后电力管理装置 11 单独对新的四个组进行认证处理。

[0611] 结果，如图 44 所示，以可控制设备 D “成功”而其它三个可控制设备“失败”结束认证。这样，电力管理装置 11 能够指定所有异常的可控制设备 C、E 和 F。

[0612] 以与策略 1 相同的方式，策略 2 中的步骤数为 4，但在第 I 步中，对 2I-1 个组进行验证处理。在这种方法中，在某些情况下，诸如当异常设备和正常设备交替对准时，将对每个设备进行验证处理，使得验证迭代次数为 2n。这意味着策略 2 的计算负荷为 O(n)。

[0613] 然而，电力管理装置 11 是掌握连接到局部电力管理系统 1 的可控制设备等的类型的装置。这是因为该信息对于控制向哪个设备供应电力是必需的。也就是说，例如，当用户将设备引入家中的局部电力管理系统 1 时，执行将该设备注册在电力管理装置 11 中的处理。因此，如前所述，电力管理装置 11 管理已注册设备列表。

[0614] 这里，在局部电力管理系统 1 中，假定可控制设备 A 到可控制设备 H 这八个设备已经注册到电力管理装置 11 中，但作为认证结果已知可控制设备 C 异常。

[0615] 在这种情况下，电力管理装置 11 从被管理列表中删除可控制设备 C，或者将可控制设备 C 标记为临时不可用。这样，在下次认证迭代期间，电力管理装置 11 能够从认证中预先排除可控制设备 C，这样能够相应地减少认证处理的负荷。例如，如果除了可控制设备 C 以外的七个可控制设备正常，则可在对七个可控制设备进行的单个认证中确认此情况。

[0616] 此外，如果经由用户指示已经通知电力管理装置 11 ：设备已修复且恢复正常，或者如果通过电力管理装置 11 定期地或不定期地尝试对异常设备进行认证而获得“成功”的结果，则电力管理装置 11 可校正电力管理装置 11 所管理的被管理列表，使得先前从认证排除的设备被认为是正常的。

[0617] 蓄电池的认证

[0618] 多数情况下，在蓄电池壳中提供多个蓄电池组电池。通过组合该多个电池，蓄电池能够产生多种输出。

[0619] 例如，图 45 示出装备有六个 1V 蓄电池组电池单元的电力存储设备 128 的示例。如图 45 所示，能够组合这些电池 A 到 F 以输出多种电压。如果还考虑到一些电池未被使用和 / 或电力存储装置 128 设置有不是一个而是多对输出终端的布置，则可实现更大数量的输出变化。

[0620] 如果蓄电池包括失败的电池和 / 或非法制造的电池，则存在增大的风险 :不仅无法达到期望输出，而且在充电期间发生诸如火灾等的事故。为此，对各个蓄电池组电池进行认证以确认每个电池（以及还有蓄电池自身）正常是很重要的。

[0621] 这里，可以设想电力管理装置 11 或蓄电池的控制单元能够对各个电池进行认证。当这样做时，如图 46 所示，可以设想使用以三个电池为组合的六个电池以获得 3V 的输出。这里，通过正常地重复电力管理装置 11 或蓄电池的控制单元对一个电池的认证，蓄电池的控制单元能够预先掌握全部电池的状态。基于注册在电力管理装置 11 中的型号等，电力管理装置 11 能够从外部的服务器等获得蓄电池的电池配置。

[0622] 在需要 3V 电压的情况下，即使具有低载流容量，也可对电池 A、B 和 C（或 D 和 E 和 F）三个电池进行认证，并将这些电池作为蓄电池。在此情况下，进行三次验证处理。

[0623] 然而，通过采用前述的批量验证或聚合签名的技术进行 ABC（或 DEF）的集中验证，能够经单次验证处理掌握是否能使用这些电池作为 3V 蓄电池，从而改进认证处理的效率。另外，如果给出了由 ABC 组成的组和由 DEF 组成的组中至少一个组验证“成功”，则能够容易地掌握电池可被用作蓄电池。

[0624] 另外，当存在认证结果为“失败”的组时，采用前述方法连续划分该组能够指定异常电池。

[0625] 如图 46 所示，当需要 2V 电压时，可对串联连接的两个电池的组 AB、CD、EF 进行集中认证。

[0626] 以这种方式，通过根据蓄电池组电池的组合将待认证的电池划分为组，能够改进验证处理的效率。

[0627] 这里假定如图 47（中的初始状态）所示，采用六个蓄电池组电池产生 2V 电压。这里，假定全部六个电池在初始状态均正常，但当在给定时间进行认证时，给出“失败”的认证结果。

[0628] 电力管理装置 11 和蓄电池的控制单元能够采用上述策略 2 以指定所有异常的电池。结果，如在图 47 中间所示，假定这里已经指定电池 D 和电池 E 异常。

[0629] 在这种情况下，蓄电池的控制单元或电力管理装置 11 能够切换连接蓄电池组电池的线，以如图 47 右侧所示重新配置电池。通过这样做，可以仅使用正常电池来配置能够用作蓄电池的组合。如果不进行重新配置，则正常的电池 C 和 F 将不可避免地被浪费，而通过重新配置，能使用资源而不会浪费。通过蓄电池的控制单元或电力管理装置 11 准确地掌握各个电池的状态并且根据认证结果重新配置电池之间的连接，可以实现电池的重新配置。

[0630] 在图 48 中示出了上述可控制设备的批量认证的整体流程。

[0631] 首先，电力管理装置 11 的设备管理单元 1121 生成挑战消息并将该挑战消息广播到全部待认证的可控制设备 125（步骤 S1191）。通过这样做，每个可控制设备 125 的控制单元 2001 生成答复挑战消息的应答消息，并将生成的应答消息发回电力管理装置 11。

[0632] 在电力管理装置 11 中，等待从可控制设备 125 发送的应答消息，当从可控制设备 125 发送应答消息时，电力管理装置 11 获得发送来的应答消息（步骤 S1193）。

[0633] 这里，电力管理装置 11 的设备管理单元 1121 判断是否已经获得全部应答消息（步骤 S1195）。如果一些应答消息没有获得，则设备管理单元 1121 回到步骤 S1193，并等待

其它应答消息。

[0634] 同时，如果已经从全部可控制设备 125 获得应答消息，则设备管理单元 1121 执行批量认证处理（步骤 S1197）。如果批量认证处理对全部可控制设备都成功，则设备管理单元 1121 判断出认证成功，并且批量认证处理正常结束。

[0635] 如果批量认证处理未对全部可控制设备 125 成功，则设备管理单元 1121 根据前述策略 1 或策略 2 指定认证失败的可控制设备（步骤 S1201）。此后，设备管理单元 1121 重复排除认证失败的设备的认证处理（步骤 S1203），返回步骤 S1199，并且判断批量认证处理是否成功。

[0636] 通过执行上述流程中的处理，在本示例变型中能够有效率地认证可控制设备。

[0637] 上述解释说明如下方法：使用批量验证或者来自基于公开密钥加密的数字签名技术中的聚合签名技术，通过对可控制设备和电力存储装置分组以有效率地进行认证。然而，尽管公开密钥加密较之于公共密钥加密的优势在于能够使用利用单个私密密钥生成的数字签名等，但是其缺点在于计算负荷通常极大。

[0638] 为了克服这个缺点，可设想能够采用公开密钥加密和公共密钥加密。更具体地，电力管理装置 11 根据公开密钥加密进行对可控制设备等的认证。假定电力管理装置（或蓄电池的控制单元等）之后按照 1 ： 1 的基础，向基于公开密钥加密认证成功的可控制设备和 / 或电力存储装置提供供电力管理装置（或蓄电池的控制单元等）和可控制设备使用的公共密钥（即，对每个可控制设备采用不同的密钥）。

[0639] 这种公共密钥具有诸如一天或者一小时的有效期限，在有效期限内，这种公共密钥用于由电力管理装置 11 对可控制设备进行的认证处理。此外，在公共密钥的有效期限结束之后，再使用公开密钥加密进行认证处理，并在电力管理装置和可控制设备之间建立新的公共密钥。

[0640] 通过使用这个方法，能够执行采用一小时仅一次或一天仅一次的计算负荷大的公开密钥加密的处理，并且能够对经常进行的认证采用处理负荷小的公共密钥加密。

[0641] 注意，代替使用电力管理装置 11 和特定可控制设备 125 之间 1 ： 1 的公共密钥，还能够在电力管理装置和要由电力管理装置认证的多个可控制设备之间共享单个组密钥，并将该组密钥用作后续认证处理中的公共密钥。

[0642] 这完成了注册根据本示例变型的可控制设备的方法的说明。

[0643] 现在将详细描述电力管理装置对出现异常的被管理设备进行的处理，同时给出具体示例。

[0644] (1-16) 在发生异常的情况下电力管理装置对被管理设备的操作

[0645] 现在将参考使用具体示例的图 49 到 52 来详细描述电力管理装置对出现异常的被管理设备的操作。图 49 到 52 是用于解释电力管理装置对已出现异常的被管理设备的操作的流程图。

[0646] 首先，将参考图 49 描述电力管理装置对已出现异常的被管理设备的操作的整体流程。

[0647] 电力管理装置 11 的设备管理单元 1121 参考关于当前时间的时间信息，或者参考关于自进行先前操作确认处理经过了多长时间的信息，并判断是否已经到达对被管理设备进行操作确认处理的时间（检查时间）（步骤 S1211）。如果检查时间未到，则设备管理单元

1121 返回步骤 S1211 并等待检查时间到达。

[0648] 此外，当到达检查时间时，设备管理单元 1121 的被管理设备信息获取单元 1507 判断是否已经从每个可控制设备 125 接收到报告出现异常的传感器信息（步骤 S1213）。如果已经接收到报告出现异常的传感器信息，则设备管理单元 1121 执行下述的步骤 S1225。

[0649] 如果没有接收到报告出现异常的传感器信息，则被管理设备信息获取单元 1507 判断是否已经从配电装置 121 接收到报告出现异常的设备信息（步骤 S1215）。如果已经接收到报告出现异常的设备信息，则设备管理单元 1121 执行下述的步骤 S1225。

[0650] 如果没有接收到报告配电装置中出现异常的设备信息，则被管理设备信息获取单元 1507 判断是否已经从可控制插座 123（下文中包括插座扩展装置 127）接收到报告出现异常的设备信息（步骤 S1217）。如果判断出已出现异常，则设备管理单元 1121 执行下述的步骤 S1225。

[0651] 注意，通过执行步骤 S1215 和步骤 S1217 的处理，电力管理装置 11 能够判断出不能与电力管理装置 11 直接进行通信的不可控制设备 126 是否出现异常。

[0652] 接着，被管理设备信息获取单元 1507 从各个可控制设备等收集诸如传感器信息、蓄电池信息和电池信息的设备信息，并将设备信息发送给信息分析单元 1123 的设备状态判断单元 1601 和电力状态判断单元 1603。设备状态判断单元 1601 和电力状态判断单元 1603 将设备信息与所发送信息的历史或者模型实例进行比较（步骤 S1219）。通过这样做，电力管理装置 11 能够检测出出现异常的可控制设备等。被管理设备信息获取单元 1507 和 / 或设备状态判断单元 1601 也能够从应接收到的未接收信息中检测出可控制设备等已出现异常。

[0653] 设备管理单元 1121 参考对设备信息的收集 / 比较处理的结果，并判断是否已经出现问题（步骤 S1221）。如果已出现问题，则设备管理单元 1121 执行下述的步骤 S1225。

[0654] 此外，如果根据设备信息的收集 / 比较处理的结果判断出未出现问题，则设备状态判断单元 1601 判断是否任一设备都没有问题（步骤 S1223）。如果判断结果是对于某些装置未完成验证，则设备管理单元 1121 和信息分析单元 1123 返回步骤 S1219 并继续验证处理。当对全部设备都完成验证时，设备管理单元 1121 结束对被管理设备的操作的验证处理。

[0655] 这里，当通过上述验证处理检测到异常时，信息分析单元 1123 在显示单元 116 上显示警告（步骤 S1225）。电力管理装置 11 切换至在检测到异常时使用的操作模式（错误模式）（步骤 S1227）。

[0656] 此后，设备管理单元 1121 向用户已注册的电话号码或已注册的邮件地址发送报警消息，以通知用户已经出现异常（步骤 S1229）。此后，设备管理单元 1121 判断设定时间段内是否有用户对电力管理装置 11 进行访问（步骤 S1231）。如果在设定时间段内有用户进行访问，则电力管理装置 11 的控制单元 115 根据用户指示开始对可控制设备的操作控制（步骤 S1233）。同时，如果在设定时间内没有用户进行访问，则电力管理装置 11 的控制单元 115 开始自动控制（步骤 S1235）。此后，电力管理装置 11 的控制单元 115 将操作模式切换为由可控制插座控制（步骤 S1237），并且当检测到操作异常时结束该处理。

[0657] 现在将简要描述根据出现异常的装置类型实施的具体处理。

[0658] 当电力管理装置出现异常时

[0659] 首先，将参考图 50 简要描述当电力管理装置 11 自身出现异常时的操作。

[0660] 注意，假定在开始以下说明前用户已经设置了当电力管理装置 11 出现异常时进行何种控制（例如，由可控制插座进行的控制或者稳定状态供应电力的控制）。还假定电力管理装置 11 定期地在局部电力管理系统 1 外部设置的系统管理服务器 33 中备份诸如历史信息、被管理设备的识别信息 (ID) 以及设置条件的各种信息。

[0661] 当电力管理装置 11 自身出现某种异常（步骤 S1241）并且电力管理装置 11 自身停止工作时，由于与电力管理装置 11 的定期通信将会停止，因此系统管理服务器 33 能够检测到电力管理装置 11 出现异常（步骤 S1243）。

[0662] 此后，系统管理服务器 33 参考注册的紧急联系人等，并通知用户出现异常（步骤 S1245）。

[0663] 因为不能与电力管理装置 11 定期通信（步骤 S1247），所以可控制插座 123 和可控制设备 125 也检测到电力管理装置 11 可能出现异常。此后，可控制插座 123 和可控制设备 125 检查电力管理装置 11 的状态（步骤 S1249），并且当掌握电力管理装置 11 出现异常时，可控制插座 123 和可控制设备 125 检查应当切换为哪个模式（步骤 S1251）。此后，可控制插座 123 和可控制设备 125 切换为可控制插座控制模式（步骤 S1253）。

[0664] 更具体地，可控制插座 123 开始控制可控制设备 125 和不可控制设备 126（步骤 S1255），并且可控制设备 125 开始向可控制插座 123 输出电力信息（步骤 S1257）。如果在从可控制设备 125 获得的电力信息中检测到异常，则可控制插座 123 也能够进行诸如停止电力供应的控制。

[0665] 此时，假定由于系统管理服务器 33 所联系的用户重新激活电力管理装置 11 或者对电力管理装置 11 手动地进行某种操作，导致电力管理装置 11 恢复（步骤 S1259）。

[0666] 此时，恢复的电力管理装置 11 的设备管理单元 1121 请求系统管理服务器 33 执行认证处理（步骤 S1261）。如果电力管理装置 11 的认证成功，则系统管理服务器 33 获得备份的设置信息，并将该设置信息发送给电力管理装置 11（步骤 S1263）。

[0667] 接收到该设置信息的电力管理装置 11 根据所接收到的设置信息，自动地连接到作为被管理设备的可控制插座 123 和可控制设备 125（步骤 S1265），并且通知这些设备电力管理装置 11 已恢复。

[0668] 此后，可控制插座 123 和可控制设备 125 切换到电力管理装置控制摸式（步骤 S1267），此后由电力管理装置 11 进行正常控制。

[0669] 当可控制插座出现异常时

[0670] 接着，将参考图 51 简要描述当可控制插座 123 出现异常时的操作。

[0671] 首先，假定可控制插座 123 的传感器或通信单元中的至少一个出现异常（步骤 S1271）。在这种情况下，因为维持从可控制插座 123 到所连接的可控制设备 125 的电力供应（步骤 S1273），所以电力管理装置 11 难以直接检测到异常。然而，通过确定没有接收到应当定期接收到的来自可控制插座 123 的设备信息等，电力管理装置 11 能够检测到可控制插座 123 出现异常（步骤 S1275）。

[0672] 检测到异常的电力管理装置 11 的信息分析单元 1123 通知用户，可控制插座 123 出现异常（步骤 S1277）。更具体地，电力管理装置 11 通过在显示单元 116 上显示出现异常、发出警告声音，或者向用户所注册的电话号码或电子邮件地址发送消息，向用户通知出

现异常。

[0673] 通过对出现问题的可控制插座 123 手动地进行任意操作，被通知的用户将可控制插座 123 恢复到运行状态（步骤 S1279）。

[0674] 这里，假定可控制插座 123 的电力供应控制出现异常（步骤 S1281）。在这种情况下，可控制设备 125 能够检测到可控制插座 123 出现异常，并且在某些情况下，可控制设备 125 也能够停止接收电力供应，并因此停止运转（步骤 S1283）。结果，由于可控制设备 125 向电力管理装置 11 通知可控制插座 123 出现异常，或者由于可控制设备 125 停止操作而引起定期通信停止，因此电力管理装置 11 检测到出现异常（步骤 S1285）。

[0675] 检测到异常的电力管理装置 11 的信息分析单元 1123 通知用户：可控制插座 123 出现异常（步骤 S1287）。更具体地，电力管理装置 11 通过在显示单元 116 上显示出现异常、发出警告声音，或者向用户所注册的电话号码或电子邮件地址发送消息，向用户通知出现异常。

[0676] 通过对出现问题的可控制插座 123 手动地进行操作，被通知的用户将可控制插座 123 恢复到运行状态（步骤 S1289）。

[0677] 当配电装置出现异常时

[0678] 接着，将参考图 52 简要描述当配电装置 121 出现异常时的操作。

[0679] 当配电装置 121 出现异常时（步骤 S1301），配电装置 121 向电力管理装置 11 通知出现异常，和 / 或来自配电装置 121 的定期通信停止。此外，当配电装置 121 出现异常时，向可控制设备 125 的电力供应可能出现问题。为此，可控制设备 125 定期发送的电力信息中也可出现异常（步骤 S1303）。根据这种信息，电力管理装置 11 的信息分析单元 1123 可以检测到配电装置 121 出现异常（步骤 S1305）。

[0680] 检测到异常的电力管理装置 11 的信息分析单元 1123 通知用户：配电装置 121 出现异常（步骤 S1307）。更具体地，电力管理装置 11 通过在显示单元 116 上显示出现异常、发出警告声音，或者向用户所注册的电话号码或电子邮件地址发送消息，向用户通知出现异常。

[0681] 通过对出现问题的配电装置 121 手动地进行操作，被通知的用户将配电装置 121 恢复到运行状态（步骤 S1309）。

[0682] 配电装置 121 再次出现异常（步骤 S1311），并且配电装置 121 向电力管理装置 11 通知出现异常和 / 或来自配电装置 121 的定期通信停止。此外，当配电装置 121 出现异常时，向可控制设备 125 的电力供应可能出现问题。由于这个原因，可控制设备 125 定期发送的电力信息也可出现异常（步骤 S1313）。由于这种信息，假定电力管理装置 11 自身也出现异常（步骤 S1317）。

[0683] 这里，与电力管理装置 11 的定期通信的中断使得系统管理服务器 33 能够检测到电力管理装置 11 出现异常（步骤 S1319）。

[0684] 此后，系统管理服务器 33 参考注册的紧急联系人等，并且通知用户出现异常（步骤 S1321）。

[0685] 在这种情况下，在电力管理装置 11 处，实施在电力管理装置出现异常时执行的上述处理（步骤 S1323）。响应于电力管理装置 11 发生的异常，可控制设备 125 切换到可控制插座控制模式（步骤 S1325）。

[0686] 这里，通过对出现问题的配电装置 121 手动地进行操作，被通知的用户将配电装置 121 恢复到运行状态（步骤 S1327）。此外，由于电力管理装置出现异常时进行的操作，电力管理装置 11 也恢复到运行状态（步骤 S1327）。

[0687] 这完成了在诸如可控制插座 123 或可控制设备 125 的被管理设备出现异常时的电力管理装置 11 的操作的说明。

[0688] (1-17) 当在电力状态中出发生异常时电力管理装置的操作

[0689] 接着，将参考图 53 和 54 描述当局部电力管理系统 1 中的电力状态出现诸如断电或漏电的异常时的电力管理装置 11 的操作。图 53 和 54 是用于解释当电力状态出现异常时电力管理装置的操作的流程图。

[0690] 断电期间电力管理装置的操作

[0691] 首先，将参考图 53 简要描述在发生断电时的电力管理装置的操作。

[0692] 当外部电源出现异常并且发生断电时，停止向配电装置 121 供应外部电力。结果，由于配电装置 121 向电力管理装置 11 通知发生断电，或者从配电装置 121 发送含有异常的设备信息，电力管理装置 11 能够检测出配电装置 121 异常（步骤 S1331）。

[0693] 在检测到发生断电时，信息分析单元 1123 的电力状态判断单元 1603 将当前模式切换为使用发电装置 129、130 和电力存储装置 128 的电力供应模式（已存储的电力供应模式）（步骤 S1333）。更具体地，电力管理装置 11 的控制单元 115 向配电装置 121 发送控制命令，以从外部电力切换为能够在系统 1 内部供应的电力。设备管理单元 1121 根据预先设置的信息，开始确定供应电力的优先级和 / 或确定待分配的电量。信息分析单元 1123 也经由显示单元 116 等向用户通知发生断电。

[0694] 设备管理单元 1121 首先判断待供电的设备是否是可控制设备 125（步骤 S1335）。如果待供电力的设备是可控制设备 125，则设备管理单元 1121 经由控制单元 115 向该设备发送控制命令（步骤 S1337）。更具体地，控制单元 115 向有问题的可控制设备 125 发送请求节能模式或关机的控制命令。

[0695] 同时，如果待供电的设备不是可控制设备 125（也就是说，不可控制设备 126），则设备管理单元 1121 判断待供电的设备是否连接到可控制插座 123（包含插座扩展装置 127）（步骤 S1339）。如果待供电的设备连接到可控制插座 123，则设备管理单元 1121 经由控制单元 115 向可控制插座 123 发送控制命令（步骤 S1341）。更具体地，控制单元 115 向可控制插座 123 发送请求该待供电的设备关机（也就是说，停止向不可控制设备 126 供应电力）的控制命令。

[0696] 如果待供电的设备未连接到可控制插座 123，由于电力管理装置 11 不能控制向该待供电的设备的电力供应，因此电力管理装置 11 使该设备保持原状或者继续当前的电力供应（步骤 S1343）。

[0697] 当结束该确定时，设备管理单元 1121 判断每个设备的设置是否已经完成（步骤 S1345）。如果一个或多个设备的设置尚未完成，则电力管理装置 11 返回步骤 S1335 并继续该处理。同时，如果全部设备的设置已经完成，则在断电期间电力管理装置 11 结束处理。

[0698] 漏电期间电力管理装置的操作

[0699] 接着，将参考图 54 简要描述在发生漏电时的电力管理装置的操作。

[0700] 当发生漏电时，较之于漏电发生之前，预期电力使用趋势将发生改变。因此，通过

将过去的电力使用历史和当前的电力使用相比较，电力管理装置 11 中信息分析单元 1123 的电力状态判断单元 1603 能够检测出发生了漏电（步骤 S1351）。此外，对于系统 1 中存在的设备而言，电力状态判断单元 1603 基于可控制设备 125 的电力使用的理论值和不可控制设备 126 的估计的电力使用量，计算出电力使用理论值，并且通过比较实际电力使用量与该电力使用理论值，能够检测出漏电。注意，可通过过去的使用量估计出不可控制设备 126 的估计的电力使用量。

[0701] 此外，不仅可由电力管理装置 11 而且也可由诸如局部电力管理系统 1 外部存在的安全检查服务器的分析服务器 34 来检测漏电的发生。这意味着在某些情况下，当发生漏电时，分析服务器 34 向电力管理装置 11 通知漏电。

[0702] 当检测出发生漏电时，电力管理装置 11 使用任意方法来指定漏电位置（步骤 S1353），并且控制单元 115 向漏电位置发送电力供应停止命令（步骤 S1355）。信息分析单元 1123 还在显示单元 116 上显示关于发生漏电以及漏电位置的信息（步骤 S1357）。

[0703] 通过执行这种处理，甚至当电力状态出现诸如断电或漏电的异常时，电力管理装置 11 能够保持局部电力管理系统 1 内部各方面的安全。

[0704] (1-18) 电子水印信息的嵌入方法和验证方法的流程

[0705] 接着，将参考图 55 到 58 描述在根据本实施例的局部电力管理系统 1 中执行的嵌入电子水印信息的方法和验证电子水印信息的方法的流程。图 55 和 57 是用于解释根据本实施例的嵌入电子水印信息的方法的流程图。图 56 和 58 是用于解释根据本实施例验证电子水印信息的方法的流程图。

[0706] 使用共享信息的电子水印信息的嵌入方法和验证方法

[0707] 首先，将参考图 55 和 56 来描述使用共享信息的电子水印信息的嵌入方法和验证方法的流程。注意，下面描述物理数据自身被用作设备表征信息的情况。

[0708] 嵌入方法的流程

[0709] 首先，将参考图 55 描述由可控制设备 125 的篡改检测信息生成单元 2031 实施的嵌入方法。

[0710] 可控制设备 125 中的篡改检测信息生成单元 2031 的设备表征信息生成单元 2033 首先从传感器控制单元 2023 和蓄电池控制单元 2027 获得物理数据（步骤 S2001）。此后，设备表征信息生成单元 2033 对所获得的物理数据进行验证（步骤 S2003）。接着，设备表征信息生成单元 2033 判断所获得的物理数据是否正常（步骤 S2005）。

[0711] 如果验证发现物理数据的值超过该物理数据的可取的值的范围，或者表面为明显的异常行为，则设备表征信息生成单元 2033 报告异常（步骤 S2019）。

[0712] 经由验证确认物理数据正常之后，电子水印生成单元 2035 基于该物理数据和共享数据生成电子水印信息（步骤 S2007），并向电子水印嵌入单元 2039 输出所生成的电子水印信息。嵌入位置确定单元 2037 分析该物理数据，确定适于该物理数据的电子水印信息嵌入位置，并将关于所确定的嵌入位置的信息通知电子水印嵌入单元 2039。

[0713] 此后，电子水印嵌入单元 2039 基于关于嵌入位置的信息将电子水印信息嵌入该物理数据（步骤 S2009）。接着，电子水印嵌入单元 2039 对嵌入了电子水印信息的物理数据（这种物理数据以下称为“被嵌入数据”）进行验证（步骤 S2011）。此后，电子水印嵌入单元 2039 检查验证结果（步骤 S2013）。

[0714] 如果被嵌入数据正常，则电子水印嵌入单元 2039 将被嵌入数据发送到电力管理装置 11（步骤 S2015）。电力管理装置 11 将接收到的被嵌入数据发送到局部电力管理系统 1 外部的分析服务器 34。

[0715] 同时，如果在被嵌入数据中发现异常，则电子水印嵌入单元 2039 判断出现异常的次数是否小于指定的阈值（步骤 S2017）。如果出现异常的次数小于指定的阈值，则篡改检测信息生成单元 2031 返回步骤 S2007，并且继续该处理。同时，如果出现异常的次数等于或大于指定的阈值，则篡改检测信息生成单元 2031 报告异常（步骤 S2019）。

[0716] 注意，如果预先确定了电子水印信息的嵌入位置，则可以省略确定嵌入位置的处理、在步骤 S2003 到步骤 S2005 中验证物理数据的处理以及步骤 S2011 到 S2019 中验证被嵌入数据的处理。

[0717] 验证方法的流程

[0718] 接着，将参考图 56 描述，由诸如安全检查服务器的分析服务器 34 中的信息篡改检测单元实施的验证电子水印信息的方法。应当注意，尽管下文中描述了对分析服务器 34 执行的验证方法，但是同样的方法可以由电力管理装置的信息篡改检测单元来执行。

[0719] 分析服务器 34 的信息篡改检测单元的嵌入位置指定单元获取嵌入有电子水印信息的物理数据（步骤 S2021）。此后，嵌入位置指定单元验证所获取的物理数据（步骤 S2023）。接着，嵌入位置指定单元判断所获取的物理数据是否正常（步骤 S2025）。

[0720] 如果验证发现物理数据的值超出该物理数据可取的值的范围或者表明为明显的异常行为，则嵌入位置指定单元报告异常（步骤 S2027）。

[0721] 在经由验证确认物理数据正常之后，嵌入位置指定单元分析该物理数据，指定嵌入电子水印信息的位置（步骤 S2029），并且将关于嵌入位置的位置信息通知给电子水印提取单元。

[0722] 接着，电子水印提取单元基于接收的关于嵌入位置的位置信息从物理数据提取电子水印信息（步骤 S2031）并且将提取的电子水印信息输出至电子水印验证单元。

[0723] 此后，电子水印验证单元基于物理数据和共享数据生成电子水印信息（步骤 S2033）并且通过将提取的电子水印信息与生成的电子水印信息进行比较而验证电子水印信息（步骤 S2035）。如果基于比较验证电子水印信息失败，则电子水印验证单元向电力管理装置 11 通知异常（步骤 S2027）。此外，如果基于比较验证电子水印信息成功，则电子水印验证单元报告验证成功，并且处理正常结束。

[0724] 应当注意，如果预先确定了电子水印信息的嵌入位置，则可省略在步骤 S2023 至步骤 S2025 中验证物理数据的处理、以及指定嵌入位置的处理（步骤 S2029）。

[0725] 使用时间信息和共享信息的电子水印信息的嵌入方法和验证方法

[0726] 接着，将参考图 57 和图 58 描述使用时间信息和共享信息的电子水印信息的嵌入方法和验证方法。应当注意，下面描述物理数据自身被用作设备表征信息的情况。

[0727] 嵌入方法的流程

[0728] 首先，将参考图 57 描述由可控制设备 125 的篡改检测信息生成单元 2031 实施的嵌入方法。

[0729] 应当注意，假设可控制设备 125 经由电力管理装置 11 定期将嵌有电子水印信息的物理数据发送给分析服务器 34，并且在可控制设备 125 与分析服务器 34 之间预先确定数据

发送定时。

[0730] 可控制设备 125 的篡改检测信息生成单元 2031 判断是否已到达预定的数据发送时间（步骤 S2041）。如果未到预定的发送时间，则篡改检测信息生成单元 2031 等待到达该预定时间。如果已经到达预定的发送时间，则设备表征信息生成单元 2033 从传感器控制单元 2023 和蓄电池控制单元 2027 获取物理数据（步骤 S2043）。此后，设备表征信息生成单元 2033 验证获取的物理数据（步骤 2045）。接着，设备表征信息生成单元 2033 判断所获取的物理数据是否正常（步骤 S2047）。

[0731] 如果验证发现物理数据的值超出该物理数据可取的值的范围或者表明为明显的异常行为，则设备表征信息生成单元 2033 报告异常（步骤 S2065）。

[0732] 在经由验证确认物理数据正常之后，嵌入位置确定单元 2037 分析物理数据，确定适于物理数据的电子水印信息的嵌入位置（步骤 S2049），并且将关于所确定的嵌入位置的信息通知给电子水印嵌入单元 2039。

[0733] 接着，电子水印生成单元 2035 获取表明当前时间或发送预定时间的时间信息（步骤 S2051）。此后，电子水印生成单元 2035 基于物理数据、时间信息和共享信息生成电子水印信息（步骤 S2053），并且将生成的电子水印信息输出给电子水印嵌入单元 2039。

[0734] 此后，电子水印嵌入单元 2039 基于关于嵌入位置的信息将电子水印信息嵌入物理数据中（步骤 S2055）。接着，电子水印嵌入单元 2039 验证嵌入有电子水印信息的物理数据（这样的物理数据在下文中称为“被嵌入数据”）（步骤 S2057）。此后，电子水印嵌入单元 2039 检查验证结果（步骤 S2059）。

[0735] 如果被嵌入数据正常，则电子水印嵌入单元 2039 将该被嵌入数据发送给电力管理装置 11（步骤 S2061）。电力管理装置 11 将所接收的嵌入数据发送给局部电力管理系统 1 外部的分析服务器 34。

[0736] 同时，如果在被嵌入数据中发现了异常，则电子水印嵌入单元 2039 判断异常出现的次数是否小于指定的阈值（步骤 S2063）。如果异常出现的次数小于指定的阈值，则篡改检测信息生成单元 2031 返回步骤 S2053，并且处理继续。同时，如果异常出现的次数等于或大于指定的阈值，则篡改检测信息生成单元 2031 报告异常（步骤 S2065）。

[0737] 应当注意，如果预先确定了电子水印信息的嵌入位置，则可省略确定嵌入位置的处理、在步骤 S2045 至步骤 S2047 中验证物理数据的处理以及在步骤 S2057 至步骤 S2063 中验证被嵌入数据的处理。

[0738] 验证方法的流程

[0739] 接着，将参考图 58 描述验证由诸如安全检查服务器的分析服务器 34 中的信息篡改检测单元实施的电子水印信息的方法。

[0740] 应当注意，假设可控制设备 125 经由电力管理装置 11 定期将嵌有电子水印信息的物理数据发送给分析服务器 34，并且在可控制设备 125 与分析服务器 34 之间预先确定数据发送定时。

[0741] 分析服务器的信息篡改检测单元判断是否已到达预定的数据发送时间（步骤 S2071）。如果未到预定的发送时间，则信息篡改检测单元等待到达该预定时间。如果已经到达预定的发送时间，则信息篡改检测单元尝试获取经由电力管理装置 11 从可控制设备 125 发送的物理数据。这里，信息篡改检测单元判断是否能够在指定的时间段内接收到物理数

据（步骤 S2073）。

[0742] 如果未在指定的时间段内接收到物理数据，则信息篡改检测单元将异常通知给电力管理装置 11 的用户（步骤 S2089）。同时，如果在预定的时间段内接收到物理数据，则嵌入位置指定单元验证所获取的物理数据（步骤 S2075）。此后，嵌入位置指定单元判断所获取的物理数据是否正常（步骤 S2077）。

[0743] 如果验证发现物理数据的值超出该物理数据可取的值的范围或者表明为明显的异常行为，则嵌入位置指定单元报告异常（步骤 S2089）。

[0744] 在经由验证确认物理数据正常之后，嵌入位置指定单元分析物理数据，指定嵌入电子水印信息的位置（步骤 S2079），并且将关于嵌入位置的位置信息通知给电子水印提取单元。电子水印提取单元基于关于嵌入位置的位置信息从物理数据提取电子水印信息并且将所提取的电子水印信息输出至电子水印验证单元。

[0745] 此后，电子水印验证单元获取表明当前时间或者发送预定时间的时间信息（步骤 S2081）。

[0746] 此后，电子水印验证单元基于物理数据、时间信息和共享数据生成电子水印信息（步骤 S2083）并且通过将提取的电子水印信息与生成的电子水印信息进行比较以验证电子水印信息（步骤 S2085）。如果基于比较验证电子水印信息失败，则电子水印验证单元报告异常（步骤 S2089）。此外，如果基于比较验证电子水印信息成功，则电子水印验证单元报告验证成功，并且处理正常结束。

[0747] 应当注意，如果预先确定了电子水印信息的嵌入位置，则可省略在步骤 S2075 至步骤 S2077 中验证物理数据的处理、以及指定嵌入位置的处理（步骤 S2079）。

[0748] 通过进行上述处理，可以在位于分析服务器 34 和可控制设备 125 之间的电力管理装置 11 的控制功能受到损害时检测到异常。通过使电力使用子水印信息，还可以检测由攻击者在通信路径上进行的对物理数据的篡改。另外，电力管理装置 11 仅仅中介 (mediate) 物理数据的发送，并且可以检测在分析服务器 34 与可控制设备 125 之间的路径上的对物理数据的篡改，而不需要发送或接收用于防止篡改的特定数据。

[0749] 甚至当电力管理装置 11 的控制功能受到损害时，也可以防止攻击者篡改物理数据的攻击。另外，通过使用该方法，可以为物理数据增添用于检测篡改的功能，而不丢失物理数据的统计特性。

[0750] (1-19) 分析服务器的作用

[0751] 用作局部电力管理系统 1 的电力中心的电力管理装置 11 被连接到装备有蓄电池的各种可控制设备等。电力管理装置 11 通过基于从各种设备获得的电力信息控制配电装置 121 来控制配电。电力管理装置 11 能够实时地掌握连接至系统 1 的设备的电力消耗，并且集中管理系统 1 内的包括通过诸如光伏发电的自然能量的家庭发电生成的电力的电力使用状态。电力管理装置 11 还能够将电力消耗可视化，这希望使用户抑制能量的浪费消耗。

[0752] 但是，由于局部电力管理系统 1 是控制局部电网的网络系统，所以重要的是在系统配置和服务中使用安全技术。近年来，对于装配有蓄电池的设备，用户通常用较次的产品代替蓄电池组电池，和 / 或使用绕过对设备认证的伪造芯片。这可能导致问题，例如质量下降，从而导致起火。由根据本实施例的局部电力管理系统 1 处理的“蓄电池”包括多种设备，

如存在于系统中的电力存储装置和电动交通工具，并且重要的是保持这样的设备安全。

[0753] 以下是能够对电力管理装置 11 进行的外部攻击的一些设想示例，该电力管理装置 11 形成局部电力管理系统 1 的外部与该系统 1 的内部之间的接口。

[0754] - 引入导致设备或蓄电池异常操作的非法命令（病毒）；

[0755] - 接管对电力管理装置的控制；

[0756] - 特洛伊木马攻击；

[0757] - 经由电力管理装置对另一设备或系统的攻击；

[0758] -DoS 攻击。

[0759] 为了保护免受这样的外部攻击，过去使用了下列措施：

[0760] - 防止预先预测的非法操作；

[0761] - 使用预先定义的病毒模式文件检测病毒；

[0762] - 监视执行文件的行为以及检测非法文件以保护免受未知的攻击。

[0763] 但是，由于这样的措施是响应于计算机上的行为而使用的，所以难以使用这样的措施来监视诸如蓄电池的物理装置，因此很难说这样的措施提供了足够的保护。此外，由于想到可与电力管理装置连接的蓄电池和设备会经常更新，所以极可能针对攻击的对策会变得极其复杂并且预先难以想象攻击的内容。

[0764] 针对伪造蓄电池的一个对策是将认证芯片集成到蓄电池模块中并且仅与质量得到保证的蓄电池连接。但是，近年来，用于使认证芯片的功能变得无效的技术得到了发展，并且伪造芯片绕过认证的情况变得越来越普遍。如果从安装在较次蓄电池组电池上的伪造芯片经由设备发送的蓄电池状态（电压、电流、剩余电荷等）不正确（即，如果数字信息错误），则电力管理装置不能正确地控制电网，从而导致出现事故的风险很高。在这种情况下，应当停止设备的操作或者应当排除有问题的蓄电池，但是没有用于实现这样的机制的现有技术。

[0765] 由于以上原因，需要用于避免对连接到电力管理装置或系统的设备 / 蓄电池的攻击（病毒感染）以及伴随蓄电池劣化或伪造产品的风险的技术。下面描述如下方法：该方法能够使用从连接至系统的蓄电池或设备输出的传感器信息和多种历史信息而检测对系统的上述类型攻击的存在以及蓄电池的劣化等。

[0766] 下面描述的检测攻击的存在以及蓄电池的劣化等的方法主要使用从各设备输出的诸如传感器信息等的物理数据以及历史信息，以使用计算物理估计进行判断以及使用启发式统计方法进行高速判断。通过这样做，可以检测未知的攻击以及从源头避免风险。

[0767] 在本实施例中，设置在局部电力管理系统 1 外部的分析服务器 34 被用作用于检测攻击以及避免风险的设备。假设分析服务器 34 的功能之一是对局部电力管理系统执行安全检查的功能。因此，以下描述的分析服务器 34 是用作安全检查服务器的服务器。

[0768] 分析服务器 34 基于从电力管理装置发送的各种设备和蓄电池的传感器信息、执行命令信息、预先注册在分析服务器 34 中的设备 / 蓄电池信息、使用环境信息和使用历史信息，实现下列功能。

[0769] - 排除绕过认证的复制品以及已经劣化并且其操作变得危险的蓄电池；

[0770] - 保护免受启发式外部攻击；

[0771] - 通过基于当前状态、输入以及关于外部环境的信息的估计验证合法性；

[0772] - 生成和更新由电力管理装置中的防病毒系统使用的病毒定义文件。

[0773] 此外，如上所述，分析服务器 34 还能够配备有以下功能：验证嵌入在从各种设备和蓄电池发送的设备表征信息中的篡改检测信息（电子水印信息）。通过使用篡改检测信息，还可以检查电力管理装置是否已被接管。

[0774] 这里，可给出电压、电流、温度、湿度、时间、使用设备信息、用户等作为上述传感器信息的示例，并且可给出指令命令、执行文件、设备 / 蓄电池参数等作为执行命令信息的示例。此外，可给出制造商、型号、制造商编号等作为预先注册在分析服务器 34 中的设备 / 蓄电池信息的示例，并且可给出家庭信息、位置、自有设备信息等作为使用环境信息的示例。可给出过去的设备 / 蓄电池传感器信息、执行命令信息、使用时间、使用频率等作为上述使用历史信息的示例。

[0775] (1-20) 分析服务器的配置

[0776] 接着，将参考图 59 至图 62 具体描述分析服务器 34 的配置，该分析服务器根据本实施例为安全检查服务器。图 59 是用于说明根据本实施例的分析服务器的配置的框图。图 60 是用于说明根据本实施例的分析服务器中包括的信息篡改检测单元的配置的框图。图 61 是用于说明根据本实施例的分析服务器中包括的第一验证单元的配置的框图。图 62 是用于说明根据本实施例的分析服务器中包括的第二验证单元的配置的框图。

[0777] 分析服务器的总体配置

[0778] 首先，将参考图 59 描述根据本实施例的分析服务器 34 的整体配置。

[0779] 如图 59 所示，根据本实施例的分析服务器 34 主要包括广域通信单元 3001、信息篡改检测单元 3003、获取数据验证单元 3005 和存储单元 3013。

[0780] 广域通信单元 3001 是用于在局部电力管理系统 1 和另一服务器等之间通过广域网 2 交换信息的通信装置。

[0781] 信息篡改检测单元 3003 例如由 CPU、ROM、RAM 等实现。当用于检测信息是否已被篡改的数据被嵌入到由分析服务器 34 从电力管理装置 11 获取的信息中时，信息篡改检测单元 3003 验证该数据并且检测信息是否已被篡改。这里，嵌入这样的信息的数据的一个示例可以为电子水印。

[0782] 当检测到信息被篡改时，信息篡改检测单元 3003 将检测结果通知给电力管理装置 11 或用户本人。通过这样做，电力管理装置 11 或者电力管理装置 11 的用户能够将出现信息篡改的设备从系统 1 内部排除。

[0783] 获取数据验证单元 3005 例如由 CPU、ROM、RAM 等实现。获取数据验证单元 3005 验证从电力管理装置 11 获取的各种信息，并且如上所述，是提供用于保护电力管理装置 11 不受外部攻击的各种功能的处理单元。

[0784] 如图 59 所示，获取数据验证单元 3005 还包括获取数据验证控制单元 3007、第一验证单元 3009 和第二验证单元 3011。

[0785] 在分析和验证由分析服务器 34 从电力管理装置 11 获取的各种数据时，获取数据验证控制单元 3007 进行控制。更具体地，获取数据验证控制单元 3007 判断如何将以下描述的第一验证单元 3009 的验证和第二验证单元 3011 的验证组合，以分析和验证所获取的数据。相应地，以下描述的第一验证单元 3009 和第二验证单元 3011 在获取数据验证控制单元 3007 的控制下执行各种验证处理。

[0786] 第一验证单元 3009 例如由 CPU、ROM 和 RAM 等实现。第一验证单元 3009 基于统计处理、使用启发式方法分析和验证由分析服务器 34 获取的各种类型信息。

[0787] 第一验证单元 3009 主要具有下述两个功能 :

[0788] (i) 通过将从电力管理装置获取的数据与从具有相似电力使用环境的另一电力管理装置获取的数据进行比较,检测存在对电力管理装置的攻击、蓄电池或者各种设备或传感器存在异常的功能 ;

[0789] (ii) 在从电力管理装置获取的数据中根据与先前使用历史数据的比较,而检测存在对电力管理装置的攻击、蓄电池或者各种设备或传感器存在异常的功能。

[0790] 为了实现以上给出的功能 (i),第一验证单元 3009 使用从处于验证中的电力管理装置 11 获取的“蓄电池型号 /ID 信息和电力状态信息、历史”和“设备型号 /ID 信息和如温度的传感器信息、历史”或者“电力管理装置的执行文件”。第一验证单元 3009 不仅使用从处于验证中的电力管理装置获取的上述信息,而且使用未处于验证中的其它电力管理装置 11 获取的上述信息。通过比较和验证这样的数据,第一验证单元 3009 判断是否存在对处于验证中的电力管理装置的攻击和 / 或在蓄电池 / 设备或传感器中是否存在异常。

[0791] 为实现以上给出的功能 (ii),第一验证单元 3009 从处于验证中的电力管理装置 11 获取“蓄电池型号 /ID 信息和电力状态信息”和“设备型号 /ID 信息和如温度的传感器信息”或者“电力管理装置的执行文件”。第一验证单元 3009 还使用处于验证中的电力管理装置 11 的“蓄电池电力状态信息历史”、“设备的传感器信息历史”和“电力管理装置的执行文件历史”。通过比较和验证这样的数据,第一验证单元 3009 判断是否存在对处于验证中的电力管理装置的攻击和 / 或在蓄电池 / 设备或传感器中是否存在异常。

[0792] 第一验证单元 3009 还包括验证“电力管理装置的执行文件”中的命令信息的功能,并且可用于在命令信息被确定为异常时从被确定为异常的命令信息中提取病毒模式。第一验证单元 3009 使用所提取的病毒模式并生成关于该病毒的病毒定义文件。

[0793] 在判断为设备的传感器信息、执行文件、命令信息等中存在异常时,第一验证单元 3009 可以与第二验证单元 3011 共享该信息,或者可以将该信息发送给第二验证单元 3011。通过共享或发送该信息,第二验证单元可以更新仿真中使用的参数并且可以进一步提高仿真精度。

[0794] 第二验证单元 3011 例如由 CPU、ROM、RAM 等实现。第二验证单元 3011 使用所获取的数据通过仿真 (计算物理估计) 来分析并验证由分析服务器 34 获取的各种信息。

[0795] 第二验证单元 3011 主要包括如下功能 :通过利用计算物理量的估计而实现的高精度判断,来检测蓄电池 / 设备或传感器的异常。

[0796] 第二验证单元 3011 从处于验证中的电力管理装置 11 获取系统 1 中的“蓄电池型号 /ID 信息和电力状态信息、历史”和“设备型号 /ID 信息和如温度的传感器信息、历史”。另外,第二验证单元 3011 从处于验证中的电力管理装置 11 获取蓄电池 / 设备的电气规格和特征信息。第二验证单元 3011 基于获取的设备信息、电气规格和特征信息以及使用历史信息进行仿真,以计算表明这些设备操作正常的指标 (在下文中称为“正常操作范围”)。第二验证单元 3011 比较并验证所计算的正常操作范围和已获得的上述各种数据,并且判断是否存在针对处于验证中的电力管理装置的攻击以及蓄电池 / 设备或传感器是否存在异常。

[0797] 存储单元 3013 是设置在根据本实施例的分析服务器 34 中的存储装置的一个示例。存储单元 3013 存储关于由分析服务器 34 存储的各个密钥以及由分析服务器 34 存储的各个数字签名、证书等的信息。在存储单元 3013 中还可以记录各历史信息。另外，存储单元 3013 还可以适当地存储处理期间应当由根据本实施例的分析服务器 34 存储的各参数和中间处理进程，或者各数据库等。分析服务器 34 的各处理单元能够自由地对存储单元 3013 进行读写。

[0798] 信息篡改检测单元的配置

[0799] 接着，将参考图 60 描述信息篡改检测单元 3003 的配置。

[0800] 如图 60 所示，信息篡改检测单元 3003 还包括嵌入位置指定单元 3021、电子水印提取单元 3023 和电子水印验证单元 3025。

[0801] 利用根据本实施例的局部电力管理系统 1，可以在诸如电流、电压、温度和湿度等的物理数据中或者在使用这些物理数据计算出的各种信息中嵌入适合这些信息的电子水印数据。通过验证电子水印数据，能够与局部电力管理系统 1 进行双向通信的分析服务器 34 能够检测物理数据（其在下文中包括使用物理数据计算出的各种信息）是否被篡改。

[0802] 嵌入位置指定单元 3021 例如由 CPU、ROM、RAM 等实现。通过使用预定的信号处理电路分析嵌有电子水印的物理数据，嵌入位置指定单元 3021 根据对应于该数据的信号的特征指定电子水印信息的嵌入位置。在指定电子水印信息的嵌入位置时，嵌入位置指定单元 3021 将关于指定嵌入位置的信息通知给电子水印提取单元 3023。应当注意，如果在可控制设备 125 等与分析服务器 34 之间预先确定了电子水印的嵌入位置，则可无需执行嵌入位置的指定处理。

[0803] 电子水印提取单元 3023 例如由 CPU、ROM、RAM 等实现。电子水印提取单元 3023 基于关于由嵌入位置指定单元 3021 提供的嵌入位置的信息从物理数据中提取电子水印信息。电子水印提取单元 3023 将从物理数据中提取出的电子水印发送给下文描述的电子水印验证单元 3025。

[0804] 电子水印验证单元 3025 例如由 CPU、ROM、RAM 等实现。电子水印验证单元 3025 首先基于与可控制设备 125 共享的共享信息等以及由电子水印提取单元 3023 提取的物理数据生成电子水印信息。为生成电子水印信息，使用哈希函数、伪随机数生成器、公共密钥加密、共享密钥加密（例如，消息认证码 MAC）等。此后，电子水印验证单元 3025 将生成的电子水印信息与由电子水印提取单元 3023 提取的电子水印信息进行比较。

[0805] 如果生成的电子水印信息和提取的电子水印信息相同，则电子水印验证单元 3025 判断出由可控制设备 125 等生成的物理数据等未被篡改。同时，如果所生成的电子水印信息和所提取的电子水印信息不相同，则电子水印验证单元 3025 判断出物理数据被篡改。

[0806] 如果物理数据被篡改，则电子水印验证单元 3025 通知电力管理装置 11 或者用户本人。通过这样做，电力管理装置 11 或者用户本人能够将操作被修改的可控制设备 125 等排除在局部电力管理系统 1 之外。

[0807] 此外，如上所述，如果电子水印信息是通过使用物理数据和共享信息并且使用时间信息生成的，则还可以验证管理局部电力管理系统 1 的电力管理装置是否被接管。

[0808] 第一验证单元的配置

[0809] 接着，将参考图 61 具体描述第一验证单元 3009 的配置。

[0810] 如上所述，第一验证单元 3009 基于从电力管理装置 11 发送的蓄电池和设备的传感器信息和执行命令信息、在分析服务器 34 中预先注册的关于蓄电池和设备的信息、使用环境信息和使用历史信息而提取表征量。此后，第一验证单元 3009 基于所提取的表征量高速检测差别和异常。

[0811] 如图 61 所示，第一验证单元 3009 包括验证控制单元 3031、操作判断单元 3033、数据库管理单元 3035、病毒定义文件管理单元 3037 和共享信息生成单元 3039。第一验证单元 3009 还包括电力管理装置数据库 3041、判断词典 3043 和病毒定义文件数据库 3045。

[0812] 验证控制单元 3031 例如由 CPU、ROM、RAM 等实现。验证控制单元 3031 控制启发式验证处理并且与第一验证单元 3009 的各处理单元合作，其中，启发式验证处理使用由第一验证单元 3009 执行的统计处理。

[0813] 操作判断单元 3033 例如由 CPU、ROM、RAM 等实现。操作判断单元 3033 输入从待验证的电力管理装置 11 获取的诸如传感器信息和执行命令信息的各种信息，并且基于处于验证中的电力管理装置 11 或其它电力管理装置 11 的历史信息等判断处于验证中的电力管理装置 11 的操作是正常还是异常。由操作判断单元 3033 执行的判断处理在后文描述。

[0814] 数据库管理单元 3035 例如由 CPU、ROM、RAM 等实现。数据库管理单元 3035 将从电力管理装置 11 发送的诸如新蓄电池和设备的传感器信息、执行命令信息以及历史信息的各种信息存储在数据库 3041 中，并且还更新判断词典 3043。数据库管理单元 3035 定期比较指定的电力管理装置 11 的统计与其它电力管理装置 11 的数据的统计，并且测试是否存在蓄意生成的数据。

[0815] 病毒定义文件管理单元 3037 例如由 CPU、ROM、RAM 等实现。病毒定义文件管理单元 3037 将已经被操作判断单元 3033 判断为异常的执行命令信息定义为病毒模式，并且生成病毒定义文件。病毒定义文件管理单元 3037 将生成的病毒定义文件存储在病毒定义文件数据库 3045 中以更新数据库，并且还经由验证控制单元 3031 将生成的病毒定义文件发送至外部。

[0816] 共享信息生成单元 3039 收集关于已被操作判断单元 3033 检测为异常的电力管理装置 11 的信息（例如关于蓄电池 / 设备的传感器信息、执行命令信息、关于蓄电池 / 设备的设备信息、使用历史信息等）作为共享信息。此后，共享信息生成单元 3039 经由验证控制单元 3031 和获取数据验证控制单元 3007 将生成的共享信息输出至第二验证单元 3011。

[0817] 通过使用共享信息来更新用于仿真的设置信息（参数等），第二验证单元 3011 能够进一步提高仿真精度。

[0818] 电力管理装置数据库 3041 是存储在第一验证单元 3009 中的数据库的一个示例。在该数据库中存储各种信息，例如关于蓄电池和设备的设备信息、使用环境信息和每个电力管理装置 11 的使用历史信息。

[0819] 判断词典 3043 是存储在第一验证单元 3009 中的另一数据库并且在操作判断单元 3033 启发式地判决操作时存储关于表征量的信息。这样的表征量是在提供特定条件（设备信息、使用环境信息等）时关于典型传感器信息的统计并且基于电力管理装置数据库 3041 而生成。

[0820] 病毒定义文件数据库 3045 是存储在第一验证单元 3009 中的又一数据库。病毒定义文件数据库 3045 存储由病毒定义文件管理单元 3037 生成的病毒定义文件。

[0821] 这完成了对第一验证单元 3009 的配置的具体描述。

[0822] 第二验证单元的配置

[0823] 接着，将参考图 62 具体描述第二验证单元 3011 的配置。

[0824] 如上所述，第二验证单元 3011 通过基于随时间和使用环境的变化、使用历史、使用状态和蓄电池的特征信息进行仿真来计算正常操作范围，并且高速检测差别和异常。第一验证单元 3009 进行的验证是使用来自虚拟环境等的统计信息的高速判断方法，而第二验证单元 3011 进行的验证是耗时的。但是，第二验证单元 3011 可以高精度地计算真品的质量劣化。

[0825] 第二验证单元 3011 包括使用从第一验证单元 3009 输出的共享信息来将在进行仿真时使用的各设置信息（参数）更新为适当值的功能。

[0826] 如图 62 所示，第二验证单元 3011 还包括估计特征值计算单元 3051、数据库 3053 和数据判断单元 3055。

[0827] 估计特征值计算单元 3051 例如由 CPU、ROM、RAM 等实现。估计特征值计算单元 3051 基于从待验证的电力管理装置 11 获取的设备信息、电气规格和特征信息以及使用历史信息进行仿真，以计算估计特征值。估计特征值是表明设备是否正确操作的指标（即，正常操作范围）。当进行仿真时，估计特征值计算单元 3051 获取数据库 3053 中注册的用于仿真的各参数。

[0828] 数据库 3053 是存储在第二验证单元 3011 中的数据库，并且存储估计特征值计算单元 3051 进行仿真时使用的各设置信息（参数）。如上所述，数据库 3053 中存储的参数由第二验证单元 3011 使用从第一验证单元 3009 输出的共享信息进行更新。

[0829] 数据判断单元 3055 例如由 CPU、ROM、RAM 等实现。数据判断单元 3055 将从待验证的电力管理装置 11 获取的各数据与由估计特征值计算单元 3051 计算的估计特征值进行比较，并且判断从待验证的电力管理装置 11 获取的各数据。通过使用任意逻辑，数据判断单元 3055 能够检测蓄电池 / 设备或传感器的异常，作为一个示例，当实际值和估计特征值之间的差异等于或大于指定阈值时或者该差异等于或小于该阈值时，数据判断单元 3055 能够判断在设备中出现异常。

[0830] 在第二验证单元 3011 中，物理仿真中使用的参数能够被纠正为更加真实的值。还可以将这样的信息发送给蓄电池或设备制造商，以将预先未想到的故障通知给制造商。

[0831] 这完成了对第二验证单元 3011 的配置的具体描述。

[0832] 以上描述了根据本实施例的分析服务器 34 的功能的一个示例。上述的组成部件可以使用通用部件和 / 或电路来构建，或者可以由专用于各组成部件的功能的硬件来构建。可选地，各组成部件的功能可以都由 CPU 等执行。因此，当实施本实施例时，可以根据主导的技术水平适当改变使用的配置。

[0833] 应当注意，用于实现上述根据本实施例的分析服务器的功能的计算机程序可以在个人计算机等中创建和安装。也可以提供存储有这样的计算机程序的计算机可读记录介质。例如，记录介质可以是磁盘、光盘、磁光盘、闪速存储器等。上述计算机程序也可以通过例如网络发布，而不使用记录介质。

[0834] (1-21) 指定待排除的蓄电池的处理

[0835] 接着，将参考图 63 描述由具有上述功能的分析服务器 34 执行的用于指定待排除

的蓄电池的处理。图 63 是用于说明待排除的蓄电池的示图。

[0836] 图 63 中示出的表是局部电力管理系统 1 中使用的蓄电池的可想到的状态的列表。如图 63 的顶部所示，局部电力管理系统 1 中使用的蓄电池包括存储电力的一个或多个电池、用于控制一个或多个电池的电路板以及该电路板上设置的认证芯片。电池和包括认证芯片的电路板的可想到的状态可大致分为表中所示的七种情况。

[0837] 情况 1 至情况 3 是由正品电池和正品电路板组成的蓄电池中可能出现的状态。情况 4 至情况 7 是使用假冒电池的蓄电池中可能出现的状态。

[0838] 在七种情况中，情况 1、情况 2 和情况 4 的电池特征没有问题，并且输出正确的设备状态。由于归入这些情况中的蓄电池在估计范围内劣化或者为具有不成问题的特征或信息的副本，所以这样的蓄电池出现在局部电力管理系统中时不会引起大的问题。

[0839] 但是，对于归入情况 3 和情况 5 至 7 中的蓄电池，当电池的特征或设备信息与具有正常使用的正品的情况比较时生成差异，并且由于这样的产品存在多种风险，所以需要将这样的蓄电池排除在局部电力管理系统 1 之外。

[0840] 由于该原因，通过使用上述多种验证处理，根据本实施例的分析服务器 34 能够指定应当被排除的上述蓄电池。

[0841] 随后将具体描述由分析服务器 34 执行的用于指定待排除的蓄电池的处理。

[0842] (1-22) 保护电力管理装置免受非法攻击的方法

[0843] 接着，将参考图 64 描述保护电力管理装置免受非法攻击的方法的整体流程。图 64 是用于说明保护电力管理装置免受非法攻击的方法的流程图。

[0844] 应当注意，在以下说明开始之前，假设已设置电力管理装置 11 以注册防止非法攻击的服务（即，由分析服务器 34 提供的服务）并且已预先设置这样的服务的执行频率、定时等。

[0845] 电力管理装置 11 的系统管理单元 1125 首先判断是否已到达用于检查非法攻击的存在的定时（步骤 S3001）。如果未到达该检查定时，则电力管理装置 11 的系统管理单元 1125 等待将到达的该检查定时。如果已到达该检查定时，则电力管理装置 11 的系统管理单元 1125 使用到目前为止存储在电力管理装置 11 中的攻击模式文件（病毒定义文件）搜索系统（步骤 S3003）。

[0846] 当在模式检查中存在问题时，电力管理装置 11 的系统管理单元 1125 在电力管理装置 11 中存储的设备排除列表中注册有问题的设备，并且控制单元 115 从系统中排除有问题的设备（步骤 S3005）。

[0847] 如果在模式检查中不存在问题，则电力管理装置 11 的设备管理单元 1121 从包括连接至系统的蓄电池的各设备收集诸如传感器信息和执行命令信息的各种信息（步骤 S3007）。此后，电力管理装置 11 的设备管理单元 1121 经由相互认证来访问分析服务器 34（步骤 S3009）。当已建立连接时，电力管理装置 11 对电力管理装置的 ID、每个设备的蓄电池 ID、蓄电池的输出信息、电力管理装置的传感器信息和执行命令信息进行加密，并且将加密的信息发送至分析服务器 34（步骤 S3011）。

[0848] 分析服务器 34 的获取数据验证单元 3005 判断在从电力管理装置 11 发送的各种数据中是否存在任何异常（步骤 S3013）。当不存在异常时，获取数据验证单元 3005 将关于电力管理装置 11 的所获取的数据添加至数据库中（步骤 S3015）并且将分析结果通知给电

力管理装置 11(步骤 S3017)。

[0849] 同时,当在步骤 S3013 中识别出异常时,分析服务器 34 的获取数据验证单元 3005 生成病毒定义文件(步骤 S3019)。分析服务器 34 的获取数据验证单元 3005 检查在识别出异常的电力管理装置 11 中是否出现很多异常(步骤 S3021)。当判断出出现很多异常并且电力管理装置 11 已成为攻击等的发射台时,分析服务器 34 向系统管理服务器 33 通知异常(步骤 S3023)。已收到报告的系统管理服务器 33 例如通过将涉及的装置置于黑名单中而排除该装置(步骤 S3025)。分析服务器 34 还将步骤 S3019 中生成的分析结果和病毒定义文件发送至电力管理装置 11(步骤 S3027)。电力管理装置 11 的系统管理单元 1125 接收该结果并且进行适当处理,例如在存在病毒定义文件时更新该病毒定义文件(步骤 S3029)。

[0850] 这完成了对保护电力管理装置免受非法攻击的方法的整体流程的说明。

[0851] (1-23) 排除蓄电池的方法

[0852] 接着,将参考图 65 描述由分析服务器 34 执行的用于指定待排除的蓄电池的处理以及由电力管理装置 11 执行的用以排除这样的蓄电池的处理。图 65 是用于说明排除蓄电池的方法的流程图。

[0853] 根据本实施例的分析服务器 34 基于从电力管理装置 11 发送的信息检测在蓄电池中是否存在异常,并且在出现了异常时通知电力管理装置 11。已收到关于异常的通知的电力管理装置 11 进行一系列操作,例如停止向异常蓄电池供应电力。

[0854] 应当注意,在以下说明开始之前,假设已设置电力管理装置 11 以注册排除蓄电池风险的服务(即,由分析服务器 34 提供的服务)并且已预先设置这样的服务的执行频率、定时等。

[0855] 电力管理装置 11 的系统管理单元 1125 首先判断是否已到达用于检查蓄电池风险的定时(步骤 S3031)。如果未到达该检查定时,则电力管理装置 11 的系统管理单元 1125 等待将到达的该检查定时。如果已到达该检查定时,则电力管理装置 11 的设备管理单元 1121 请求包括蓄电池的可控制设备 125 等发送蓄电池信息(蓄电池初级信息)。作为响应,包括蓄电池的各可控制设备 125 将蓄电池信息发送给电力管理装置 11(步骤 S3033)。电力管理装置 11 检查是否已从每个设备获取了蓄电池信息(步骤 S3035)。应当注意,尽管不是绝对必须从每个设备获取蓄电池信息,但是优选检查所有设备。

[0856] 电力管理装置 11 的设备管理单元 1121 经由相互认证来访问分析服务器 34(步骤 S3037)。当已建立连接时,电力管理装置 11 将电力管理装置的 ID、每个设备的蓄电池 ID 以及蓄电池的初级信息发送至分析服务器 34(步骤 S3039)。

[0857] 分析服务器 34 的获取数据验证单元 3005 使用从电力管理装置 11 发送的各种数据计算估计特征值,并且将获取的数据与计算的估计特征值进行比较。此后,分析服务器 34 的获取数据验证单元 3005 将得到的结果通知给电力管理装置 11(步骤 S3041)。

[0858] 电力管理装置 11 的系统管理单元 1125 判断得到的结果(步骤 S3043)。当该结果为不存在异常时,电力管理装置 11 的设备管理单元 1121 检查从传感器收集的物理信息(步骤 S3045) 并且如果不存在问题则结束处理。

[0859] 当在步骤 S3043 中存在异常时,电力管理装置 11 的控制单元 115 向配电装置 121 发出关于具有存在异常的蓄电池的设备的电力供应停止命令(步骤 S3047)。配电装置 121 根据来自电力管理装置 11 的命令停止向这样的设备的电力供应(步骤 S3049)。电力管理

装置 11 的系统管理单元 1125 将存在异常的设备的 ID 置于撤销列表上并且设备管理单元 1121 断开设备的信息网络（步骤 S3051）。

[0860] 通过执行上述处理，分析服务器 34 能够指定待排除的蓄电池，并且电力管理装置 11 能够从系统中排除此类待排除的蓄电池。

[0861] (1-24) 由获取数据验证单元进行的验证处理

[0862] 接着，将参考图 66A 和图 66B 描述分析服务器 34 的获取数据验证单元 3005 进行的验证处理的整体流程。图 66A 和图 66B 为用于说明由获取数据验证单元进行的验证的流程图。

[0863] 分析服务器 34 的获取数据验证单元 3005 的获取数据验证控制单元 3007 首先获取从电力管理装置 11 发送的各种数据（步骤 S3061）。接着，获取数据验证控制单元 3007 使用预定过滤器测试所获取的数据（步骤 S3063）。作为示例，过滤器可以针对从指定电力管理装置 11 发送大量信息的 DoS 攻击提供保护，可以用作防火墙，和 / 或可以拒绝非标准通信。

[0864] 如果在对获取的数据进行的过滤处理中检测到异常，则获取数据验证控制单元 3007 输出异常判断（步骤 S3083），实施指定的报警处理（步骤 S3085），并且结束流程。作为一个例子，可以针对系统管理服务器 33 或与讨论的电力管理装置有关的另一服务器执行该报警处理。

[0865] 同时，如果在对获取的数据进行的过滤处理中未检测到异常，则获取数据验证控制单元 3007 对所获取的数据实施简化的判断处理（步骤 S3065）。假设简化的判断包括由分析服务器 34 检测预先了解的病毒模式，由第一验证单元 3009 执行简化的判断，和 / 或针对典型使用进行匹配，这样的处理通常高速执行。当可以在该阶段明确确认操作正常时，输出正常判断（步骤 S3081）并且结束流程。

[0866] 同时，如果该简化判断判断出存在异常或者如果无法判断，则获取数据验证控制单元 3007 判断使用以下描述的三个判断处理（标号为模式 1 至模式 3）中的哪一个（步骤 S3067）。

[0867] 模式 1 是选择链接判断处理的模式，该链接判断处理使用第一验证单元 3009 和第二验证单元 3011 的组合。

[0868] 例如，获取数据验证控制单元 3007 首先经由第一验证单元 3009 的统计处理进行判断（步骤 S3069），并且还从发送的信息中掌握蓄电池 / 设备的物理特征。这里，获取数据验证控制单元 3007 判断处理路径（步骤 S3071）并且判断是要输出最终结果（步骤 S3075）还是执行第二验证单元 3011 的验证（步骤 S3073）。当还执行第二验证单元 3011 的验证时，第二验证单元 3011 基于从第一验证单元 3009 接收的共享信息（即，物理特征）更新仿真中使用的物理参数，并且基于发送的信息执行仿真。另外，第一验证单元 3009 基于通过第二验证单元 3011 的验证获得的发现来更新判断词典，并且基于统计处理再次执行判断。

[0869] 还可以选择如下判断处理 :在由验证单元之一进行的判断中明确建立应当更加详细研究的点，然后将该点反馈给由另一验证单元进行的判断。这样，模式 1 是通过第一验证单元 3009 与第二验证单元 3011 的互补使用来提高判断精度的方法。

[0870] 模式 2 是选择线性判断处理的模式，其中，第一验证单元 3009 的验证和第二验证单元 3011 的验证按该顺序进行。

[0871] 更具体地，获取数据验证控制单元 3007 首先使用能够在相对较短的处理时间内进行判断的第一验证单元 3009 实施验证（步骤 S3077），并且，如果判断结果不正常，则切换到需要较长处理时间的第二验证单元 3011 的验证（步骤 S3079）。这里，假设第一验证单元 3009 的验证是比简化判断中的验证更详细的研究。

[0872] 当使用模式 2 时，如果由第一验证单元 3009 的验证生成“正常”判断，则获取数据验证控制单元 3007 输出正常判断（步骤 S3081）并且流程结束。

[0873] 在图 66A 中，假设了首先实施相对较快的第一验证单元 3009 的验证的情况，但是也可以首先实施第二验证单元 3011 的验证。

[0874] 模式 3 是选择并行判断处理的模式，其中，同时使用第一验证单元 3009 的验证和第二验证单元 3011 的验证。

[0875] 获取数据验证控制单元 3007 确定执行第一验证单元 3009 和第二验证单元 3011 两者的验证还是仅使用这些验证单元之一执行验证，并且确定研究什么属性（步骤 S3087）。第一验证单元 3009（步骤 S3089）和第二验证单元 3011（步骤 S3091）执行各自的研究，并且获取数据验证控制单元 3007 基于来自这两个处理单元的研究结果执行最终判断（步骤 S3093）。

[0876] 应当注意，尽管可以执行上述三种方法（模式）之一，但是也可以并行执行这三种方法。还可以根据要研究的属性信息和 / 或传感器信息的范围等自适应地分配这些方法。还应当可以通过并行使用多个模式 1 至 3 代替单独使用模式 1 至模式 3 来生成潜在高速模型。

[0877] (1-25) 由第一验证单元进行的验证处理的流程

[0878] 接着，将参考图 67 描述第一验证单元的验证处理的流程。图 67 是用于说明第一验证单元的验证处理的流程图。

[0879] 第一验证单元 3009 的验证控制单元 3031 首先获取要验证的电力管理装置 11 的蓄电池 / 传感器信息和执行命令信息中的至少之一作为验证数据（步骤 S3101）。接着，操作判断单元 3033 执行调整所获取信息（例如，蓄电池或设备的传感器信息）的数据格式的预处理（步骤 S3103）。

[0880] 此后，操作判断单元 3033 指定特定的属性信息（例如，设备信息、使用环境信息），并且根据这些属性从已由预处理调整后的数据（蓄电池或设备的传感器信息，执行命令信息）中提取表征量（步骤 S3105）。由于在提取表征量时指定的属性信息的典型表征量是预先根据要验证的电力管理装置或其它电力管理装置的使用历史计算出的，所以所指定属性信息的典型表征量会存储在判断词典中。

[0881] 应当注意，表征量如下：

[0882] - 由未处于验证中的电力管理装置的蓄电池 / 传感器信息和使用历史给出的表征量；

[0883] - 由处于验证中的电力管理装置的蓄电池 / 传感器信息 / 历史给出的表征量；

[0884] - 未处于验证中的电力管理装置的执行命令的特征；

[0885] - 处于验证中的电力管理装置的执行命令的特征；

[0886] 接着，第一操作判断单元 3033 将指定属性信息的典型表征量和计算出的表征量进行比较（步骤 S3107）并且输出判断结果（步骤 S3109）。作为一个示例，操作判断单元

3033 能够在这两个表征量之间相关度低时判断出出现异常，并且在相关度高时能够判断出状态正常。

[0887] 另一操作判断单元 3033 也可以针对相同的表征量或不同的表征量执行同样的处理（步骤 S3111 至步骤 S3115）并且输出判断结果。

[0888] 此后，验证控制单元 3031 可以基于来自每个操作判断单元 3033 的判断结果给出正常 / 异常的最终判断（步骤 S3117）。例如，验证控制单元 3031 可以在每个操作判断单元 3033 给出正常 / 异常的判断时给出多数判断。可替换地，验证控制单元 3031 可以使用以下方法：通过对于正常使用权重 1 且对于异常使用权重 0 来计算和，并且在该和等于或大于阈值时给出正常的最终判断。当计算相关度或函数值时，验证控制单元 3031 可得到采用了与以上相同的权重的和，然后使用阈值进行判断或使用某类型函数。

[0889] 验证控制单元 3031 将如上所述获得的总体判断结果输出至获取数据验证控制单元 3007（步骤 S3119）并结束验证处理。获取数据验证控制单元 3007 将获得的验证结果输出至电力管理装置、用户本人和提供其它服务的服务器等。

[0890] 应当注意，作为示例，操作判断单元 3033 可以使用诸如最近邻近原则、感知器、神经网络、支撑矢量机、多变量分析、或提升 (Boosting) 等方法作为判断函数。判断函数的参数可以预先基于关于另一电力管理装置 11 的数据和 / 或物理数据而通过学习确定。

[0891] 应当注意，如果通过上述处理最终识别出异常，则病毒定义文件管理单元 3037 从识别出异常的执行命令信息中提取模式，并且生成病毒定义文件。

[0892] (1-26) 由数据库管理单元进行的测试处理

[0893] 接着，将参考图 68 描述第一验证单元 3009 的数据库管理单元 3035 的测试处理。图 68 是用于说明数据库管理单元的测试处理的流程图。

[0894] 在数据库管理单元 3035 中，将关于从指定的电力管理装置 11 获取的数据的统计定期与关于从另一电力管理装置获取的数据的统计进行比较，并且进行是否存在蓄意生成的数据的测试。

[0895] 为了通过操作判断单元 3033 检测异常操作，数据库管理单元 3035 预先从自多个电力管理装置收集的各种信息（例如，蓄电池或设备的传感器信息）正常地提取用于比较目的的表征量。

[0896] 这里，存在恶意的电力管理装置 11 发送被篡改的蓄电池或设备的传感器信息等以操纵表征量的风险。因为这个原因，通过将从具有指定属性信息（例如，设备信息和使用环境信息）的指定电力管理装置的使用历史信息提取出的表征量与具有相同属性信息的多个其它电力管理装置的使用历史提取出的表征量进行比较，病毒定义文件管理单元 3037 可检测出这种攻击。

[0897] 首先，关于指定的属性信息，数据库管理单元 3035 首先获得要被判断为恶意或正常的电力管理装置的传感器信息或执行命令信息（步骤 S3121），并且从获取的信息提取表征量（步骤 S3123）。数据库管理单元 3035 从具有相同属性信息的多个其它电力管理装置获取同一信息（步骤 S3125），并且使用相同方法提取表征量（步骤 S3127）。

[0898] 接着，数据库管理单元 3035 比较已提取的两个表征量并且判断当前关注的指定电力管理装置是否在非法操纵表征量（步骤 S3129），并且输出最终结果（步骤 S3131）。可替换地，数据库管理单元 3035 可以针对其它属性执行相同的比较和判断，然后确定最终结

果。应当注意，先前所列的判断函数之一被用于表征量的比较和判断，其中，通过学习预先计算用于此函数的参数。

[0899] 当判断结果为电力管理装置是恶意时，则分析服务器 34 通知拥有该电力管理装置 11 的用户和 / 或电力公司的服务提供服务器等。

[0900] (1-27) 数据库的更新以及判断词典的生成

[0901] 接着，将参考图 69 简要描述由数据库管理单元 3035 进行的数据库的更新和判断词典的生成。图 69 是用于说明由数据库管理单元进行的数据库的更新和判断词典的生成的示图。

[0902] 数据库管理单元 3035 将来自电力管理装置 11 的新的传感器信息和执行命令信息等存储在电力管理装置数据库 3041 中，并且还生成由操作判断单元 3033 使用的判断词典 3043。

[0903] 定期从电力管理装置 11 发送的传感器信息和执行命令信息以及在注册期间从电力管理装置 11 发送的设备信息、使用环境信息等经由验证控制单元 3031 被存储在电力管理装置数据库 3041 中。还基于传感器信息计算指定电力管理装置 11 的使用时间、使用频率等并将其存储在电力管理装置数据库 3041 中。

[0904] 针对指定属性信息中的各属性，基于多个电力管理装置 11 的传感器信息、执行命令信息等所提取的表征量被存储在由操作判断单元 3033 使用的判断词典 3043 中。由于假设在起始阶段少数样本存储在判断词典 3043 中，所以从电力管理装置 11 发送关于各设备的物理数据并且估计表征量。此外，由于对于指定属性信息而言样品数量可能少，所以在一些情况下，可以从物理数据提取表征量并将其用于校正判断词典 3043 中存储的表征量。

[0905] (1-28) 管理病毒定义文件的方法

[0906] 接着，将参考图 70 简要描述由病毒定义文件管理单元 3037 执行的管理病毒定义文件的方法。图 70 是用于说明由病毒定义文件管理单元执行的管理病毒定义文件的方法的流程图。

[0907] 病毒定义文件管理单元 3037 将在由操作判断单元 3033 进行的判断中被判断为异常的执行命令信息定义为病毒模式，以生成病毒定义文件。此后，病毒定义文件管理单元 3037 将生成的病毒定义文件存储在病毒定义文件数据库 3045 中。

[0908] 在生成病毒定义文件之前，首先，操作判断单元 3033 判断出某个电力管理装置 11 的操作异常 (步骤 S3141)。此后，病毒定义文件管理单元 3037 分析被操作判断单元 3033 判断为异常的执行命令信息并提取模式 (步骤 S3143)。

[0909] 接着，病毒定义文件管理单元 3037 基于提取的模式生成文件 (病毒定义文件) (步骤 S3145) 并且将生成的定义文件存储在病毒定义文件数据库 3045 中。病毒定义文件管理单元 3037 将生成的定义文件经由获取数据验证控制单元 3007 发送至电力管理装置 11(步骤 S3149)。每个电力管理装置 11 和分析服务器 34 能够使用该定义文件作为检测病毒的过滤器。

[0910] 病毒定义文件管理单元 3037 分析包括执行命令信息的电力管理装置 11 的使用历史信息，其中从该执行命令信息中提取模式。结果，如果从电力管理装置 11 频繁发生异常，则在一些情况下，电力管理装置 11 被认作为恶意攻击者并且被注册在黑名单中 (步骤 S3151)。病毒定义文件管理单元 3037 也可以向电力公司报告存在这样的电力管理装置 11。

[0911] 注意，当电力管理装置被注册在黑名单中时，拒绝接收来自所注册的电力管理装置的通信和 / 或警告其它电力管理装置。

[0912] (1-29) 指定待排除的蓄电池的方法的流程

[0913] 接着，将参考图 71A 至图 72 说明由获取数据验证单元 3005 实施以指定待排除的蓄电池的方法的流程。图 71A 至图 72 是用于说明由获取数据验证单元实施以指定待排除的蓄电池的方法的流程图。

[0914] 首先，将参考图 71A 至图 71C 说明指定对应于图 63 中的情况 3、5 和 6 的蓄电池的过程。

[0915] 应当注意，在以下说明开始之前，假设已设置电力管理装置 11 以预定排除蓄电池风险的服务（即，由分析服务器 34 提供的服务）并且预先设置这样的服务的执行频率、定时等（步骤 S3161）。

[0916] 如果检查蓄电池风险的定时已到，则电力管理装置 11 的系统管理单元 1125 请求可控制设备 125 执行性能检查（步骤 S3163），该可控制设备 125 为由电力管理装置 11 管理的被管理设备。

[0917] 可控制设备 125 的主部件于是请求与其连接的蓄电池获取与关于蓄电池的电压 / 电流 / 剩余电荷 / 阻抗 / 负载等有关的临时状态信息（即电池特征）D1 和设备信息 D2（步骤 S3165）。

[0918] 连接至可控制设备 125 的蓄电池获取信息 D1 和 D2（步骤 S3167）并且将这些信息和蓄电池的 ID 信息经由可控制设备 125 的主部件发送至电力管理装置 11（步骤 S3169）。

[0919] 电力管理装置 11 的设备管理单元 1121 将获取的信息存储在电力管理装置 11 中存储的数据库中（步骤 S3171）。电力管理装置 11 还向分析服务器 34 发出特定查询（步骤 S3173）。此后，电力管理装置 11 与分析服务器 34 进行认证（步骤 S3175）并且与分析服务器 34 建立通信路径。

[0920] 接着，电力管理装置 11 的系统管理单元 1125 将获取的信息 (D1、D2 和蓄电池的 ID 信息）发送至分析服务器 34（步骤 S3177）。

[0921] 分析服务器 34 中的获取数据验证单元 3005 的第二验证单元 3011 使用获取的数据来执行特征估计计算（步骤 S3179）以计算关于信息 D1 和 D2 的估计特征值。此后，第二验证单元 3011 计算实际测量值与估计值之间的差异并且判断出结果（步骤 S3181）。接着，分析服务器 34 将获得的判断结果发送至电力管理装置 11（步骤 S3183）。

[0922] 这里，针对各情况，步骤 S3181 中获得的判断结果预期如下 :

[0923] （情况 3）

[0924] 针对 D1 的差异 :在指定范围之外 ;针对 D2 的差异 :在指定范围之外。

[0925] （情况 5）

[0926] 针对 D1 的差异 :在指定范围之外 ;针对 D2 的差异 :在指定范围之外。

[0927] （情况 6）

[0928] 针对 D1 的差异 :在指定范围之外 ;针对 D2 的差异 :在指定范围之外。

[0929] 已获取此判断结果的电力管理装置 11 执行用于处理异常的处理（步骤 S3185）。更具体地，电力管理装置 11 的设备管理单元 1121 命令配电装置 121 停止向出现了异常的可控制设备 125 供应电力（步骤 S3187）。配电装置 121 接收该命令并且停止向可控制设备

125 供应电力（步骤 S3189）。

[0930] 同时，电力管理装置 11 的系统管理单元 125 向用户发出警告（步骤 S3191）并且更新撤销列表（步骤 S3193）。此后，电力管理装置 11 断开所涉及的可控制设备 125 的网络（步骤 S3195）。

[0931] 应当注意，尽管在图 71A 中示出了分析服务器 34 指定待排除的蓄电池的处理，但是，如果电力管理装置 11 具有计算估计特征值的功能，则可执行图 71C 中示出的处理代替图 71A 中的步骤 S3177 至 S3183。更具体地，电力管理装置 11 从分析服务器 34 请求计算估计特征值所需的信息，例如特征值（步骤 S3201）。在接收到此请求时，分析服务器 34 将计算估计特征值所需的信息发送至电力管理装置 11（步骤 S3203）。此后，电力管理装置 11 使用所获取的信息计算估计特征值（步骤 S3205）并且判断出结果（步骤 S3207）。通过以这种方式执行处理，电力管理装置 11 也可以指定待排除的蓄电池。

[0932] 接着，将参考图 72 描述用于指定和排除对应于情况 7 的蓄电池的流程。一直到指定对应于情况 7 的蓄电池的处理与图 71A 中示出的步骤 S3161 至 S3183 相同。但是，对于对应于情况 7 的蓄电池的判断结果如下。

[0933] （情况 7）

[0934] 针对 D1 的差异：在指定范围之外；针对 D2 的差异：在指定范围之内。

[0935] 已获取以上判断结果的电力管理装置 11 执行用于处理异常的处理（步骤 S3211）。更具体地，电力管理装置 11 的设备管理单元 1121 将传感器检查命令和增加检查频率的命令发送至可控制设备 125（步骤 S3213）。在收到此命令时，可控制设备 125 执行收到的命令并且请求传感器执行测量（步骤 S3215）。结果，传感器输出关于警告的传感器信息（步骤 S3217）。

[0936] 已获取关于警告的传感器信息的电力管理装置 11 命令配电装置 121 停止向出现异常的可控制设备 125 供应电力（步骤 S3219）。配电装置 121 接收该命令并停止向可控制设备 125 供应电力（步骤 S3221）。

[0937] 同时，电力管理装置 11 的系统管理单元 1125 向用户发出警告（步骤 S3223）并更新撤销列表（步骤 S3225）。此后，电力管理装置 11 断开所涉及的可控制设备 125 的网络（步骤 S3227）。

[0938] 这完成了对指定待排除的蓄电池的方法和排除蓄电池的方法的流程的描述。

[0939] 由于上述分析服务器 34 的存在，可以保护电力管理装置 11 免受已有的攻击以及未知的攻击。根据本实施例的分析服务器 34 的获取数据验证单元 3005 具有能够进行启发式的或者基于物理分析的判断的功能，这意味着当未出现问题时能够高速进行判断。

[0940] 此外，通过使用由获取数据验证单元 3005 生成的验证结果，可以指定已识别出从合法蓄电池和非法蓄电池（如复制品）中的任一个获得的物理信息或数字信息的差异的设备。通过这样做，可以从局部电力管理系统 1 中移除有问题的蓄电池，或者停止向这样的蓄电池供应电力。为蓄电池制定了多种安全措施，但是即使在经由这些安全措施无法控制时，也可以经由本发明来确保保持安全。

[0941] (1-30) 当存在多个电力管理装置时的处理

[0942] 接着，将参考图 73 至图 75 描述在局部电力管理系统 1 中存在多个电力管理装置 11 时的处理。

[0943] 这里，将参考图 73 至图 75 描述多个电力管理装置 11 的使用。如上所述，电力管理装置 11 担当对局部电力管理系统 1 中的设备等的电力供应的总管理者。这意味着，如果电力管理装置 11 出故障或者由于软件升级而停用，则无法使用局部电力管理系统 1 中的设备等。为做好针对此类情形的准备，优选使用多个电力管理装置 11。但是，电力管理装置 11 担当电力相关信息的总管理者并且控制局部电力管理系统 1 中的各设备等。这意味着，需要某些措施来使多个电力管理装置 11 安全且高效地执行复杂的管理和控制。一个可想到的措施是图 73 至图 75 所示的方法。

[0944] 控制操作

[0945] 首先，将参考图 73 描述使用多个电力管理装置 11 控制设备等的方法。应当注意，通过信息管理单元 112 中包括的系统管理单元 1125 的功能来实现多个电力管理装置 11 的合作操作。

[0946] 如图 73 所示，首先，系统管理单元 1125 检查是否有两个或更多个电力管理装置 11 正在运行（步骤 S4001）。在进行检查时，系统管理单元 1125 使用局部通信单元 111 的功能来查询其它电力管理装置 11 的系统管理单元 1125 并检查这些电力管理装置 11 是否正在运行。当有两个或更多个电力管理装置 11 正在运行时，系统管理单元 1125 的处理进入步骤 S4003。同时，在没有其它电力管理装置 11 正在运行时，系统管理单元 1125 的处理进入步骤 S4009。

[0947] 当处理从步骤 S4001 进入到步骤 S4003 时，系统管理单元 1125 将指定的电力管理装置 11 设置为父装置并将其余电力管理装置 11 设置为子装置（步骤 S4003）。例如，当预先确定了用于将电力管理装置设置为父装置的基于优先级的顺序时，具有最高优先级等级的电力管理装置 11 被设置为父装置。应当注意，这里使用的表述“父装置”和“子装置”是指电力管理装置 11 的属性。通过设置该属性，在控制设备等时，具有“子装置”属性的电力管理装置 11 将控制信号发送至具有“父装置”属性的电力管理装置 11（步骤 S4005）。

[0948] 当从多个子装置向父装置发送了控制信号时，父装置的系统管理单元 1125 基于多数判决或由父装置进行的判断（随机地或者根据预定条件），确定要发送至设备等的控制信号（步骤 S4007）。一旦确定了控制信号，控制单元 115 将系统管理单元 1125 所确定的控制信号发送至设备等，以使该设备等根据控制信号执行处理（步骤 S4011）并结束该系列处理。同时，在处理已从步骤 S4001 进入到步骤 S4009 时，控制单元 115 将自生成的控制信号发送至设备等，以使该设备等根据控制信号进行处理（步骤 S4009）并结束该系列处理。

[0949] 这样，系统管理单元 1125 具有用于设置每个电力管理装置 11 的属性的功能以及用于选择控制信号的功能。系统管理单元 1125 能够使用这样的功能高效地控制设备等。在一个或更多个电力管理装置 11 已损坏或者由于更新目的已停用时，还可以使另一个电力管理装置 11 继续电力管理，从而避免设备等变得不可用的情况。

[0950] 更新期间的操作

[0951] 接着，将参考图 74 和图 75 描述对定义电力管理装置 11 的基本操作的软件（或“固件”）进行更新的方法。应当注意，对固件的更新过程由系统管理单元 1125 的功能实现。这里，假设局部电力管理系统 1 中有 N 个电力管理装置 11 正在运行。

[0952] 如图 74 所示，系统管理单元 1125 首先检查是否有两个或更多个电力管理装置 11 正在运行（步骤 S4021）。当有两个或更多个电力管理装置 11 正在运行时，系统管理单元

1125 的处理进入步骤 S4023。同时，在没有其它电力管理装置 11 正在运行时，系统管理单元 1125 结束关于更新的一系列过程。

[0953] 当处理进入到步骤 S4023 时，系统管理单元 1125 从合作操作中移除待更新的第一电力管理装置 11 并执行更新（步骤 S4023）。这样做时，已从合作操作中被移除的电力管理装置 11 的系统管理单元 1125 从系统管理服务器 33 获取最新的固件并且将旧的固件更新为最新的固件。当完成了对固件的更新时，合作操作的其余电力管理装置 11 检查已完成更新的电力管理装置 11 的操作（步骤 S4025、S4027）。

[0954] 如果电力管理装置 11 操作正常，则处理进入到步骤 S4029。同时，如果更新后的电力管理装置 11 操作不正常，则处理进入到步骤 S4031。当处理进入到步骤 S4029 时，包括更新后的电力管理装置 11 的多个电力管理装置 11 的系统管理单元 1125 使更新后的电力管理装置 11 返回到合作操作中（步骤 S4029），并且更换待更新的电力管理装置 11。此时，检查是否针对所有 N 个电力管理装置 11 完成了更新（步骤 S4033），并且在 N 个设备的更新完成时，更新处理结束。

[0955] 同时，当未针对所有 N 个电力管理装置 11 完成更新时，处理返回至步骤 S4023 并且对下一个要更新的电力管理装置 11 执行更新过程。这样，重复执行步骤 S4023 至步骤 S4029 中的处理直到完成对所有 N 个电力管理装置 11 的更新。但是，当处理从步骤 S4027 进入步骤 S4031 时，进行更新取消过程（步骤 S4031），并且结束关于更新的一系列过程。

[0956] 这里，将参考图 75 描述更新取消过程。

[0957] 如图 75 所示，当开始更新取消过程时，更新后的电力管理装置 11 的系统管理单元 1125 将更新后的电力管理装置 11 的固件返回到更新前的状态（步骤 S4041）。此后，合作操作的其余电力管理装置 11 的系统管理单元 1125 检查已返回至更新前的状态的电力管理装置 11 是否正常操作（步骤 S4043、S4045）。

[0958] 如果返回至更新前的状态的电力管理装置 11 正常操作，则处理进入到步骤 S4047。同时，如果返回至更新前的状态的电力管理装置 11 操作不正常，则更新取消过程结束于此状态。当处理进入到步骤 S4047 时，包括返回至更新前的状态的电力管理装置 11 在内的多个电力管理装置 11 的系统管理单元 1125 将返回至更新前的状态的电力管理装置 11 返回到合作操作（步骤 S4047）并且更新取消过程结束。

[0959] 这样，在更新期间进行如下过程：使要更新的电力管理装置 11 与合作操作分离，并且在执行更新后确认操作正常时使电力管理装置 11 返回合作操作。如果更新失败，还执行如下过程：在电力管理装置返回至更新前状态后检查正常操作，并且如果确认了操作正常，则将电力管理装置 11 返回至合作控制。通过使用这种配置，能够进行更新而不影响合作操作的电力管理装置 11 并且保证电力管理装置 11 的安全操作。

[0960] (2) 第二实施例

[0961] (2-1) 第二实施例概述

[0962] 局部电力管理系统是向低能源社会转型的一个标志，但是目前，由于安装所需要的工作的原因，这样的系统仍有待变得普遍。这种情形意味着，将其它有吸引力的方面加入到系统安装和使用中以鼓励更多用户安装系统从而实现低能源社会很重要。这样的附加吸引力的一个示例为提供与局部电力管理系统链接的娱乐（例如游戏）。

[0963] 目前在售的多数视频游戏是虚构的。尽管有些游戏（例如关于历史事件或运动的

游戏）使用真实人物和场所的名字和 / 或在游戏视频中使用实际镜头，但是游戏自身还是与实际社会或现实生活没有联系。由于该原因，在下文描述的本发明第二实施例中，提出了具有故事情节的现实生活游戏，在该故事情节中，游戏内容自身能够导致在单独的局部电力管理系统（例如，家庭系统）中降低能源使用。

[0964] 另外，过去的游戏仅能够以诸如积分、在游戏中收集的物品以及打通的关数等无形资产的形式吸引用户以及提供满足和成就感。但是，利用诸如以下描述的与系统链接的娱乐，能够在实际的局部电力管理系统的操作中实现有效的游戏可玩性和游戏中的策略。通过这样做，根据本实施例的与系统链接的娱乐具有能导致现实世界利益（例如对电力的实际控制，降低电力消耗，有益于降低 CO_2，以及从电力售卖中获利）的方面，并且同时具有切实的效果，从而用户能够获得现实世界的知识。

[0965] 从以上应当看出，通过使用以下描述的与系统链接的娱乐，用户能够在进行环保行为（例如降低电力消耗）时得到乐趣。

[0966] 应当注意，尽管本实施例是应用于局部电力管理系统的示例，但是，还可以将本发明应用于任何与现实世界链接的游戏并具有切实效果。

[0967] 由电力管理装置 11 的服务提供单元 118 以及存在于局部电力管理系统 1 之外的服务提供服务器 31（游戏服务提供服务器）实现与系统链接的娱乐，该服务提供单元 118 操作以被链接到电力管理装置 11 的各处理单元。此外，通过操作能够连接至电力管理装置 11 的可控制设备 125，用户能够享受如游戏所呈现的与系统链接的娱乐。

[0968] (2-2) 服务提供单元的配置

[0969] 首先，将参考图 76 和图 77 描述电力管理装置 11 的服务提供单元 118 的配置。图 76 和图 77 是用于说明电力管理装置的服务提供单元的配置的框图。

[0970] 应当注意，假设根据本实施例的电力管理装置 11 包括根据本发明第一实施例的电力管理装置 11 的处理单元，并且能够实现与根据第一实施例的电力管理装置 11 相同的功能。

[0971] 服务提供单元 118 例如由 CPU、ROM、RAM 等实现。如图 76 所示，服务提供单元 118 包括游戏服务提供单元 1181 和“其它服务”提供单元 1182。

[0972] 游戏服务提供单元 1181 例如由 CPU、ROM、RAM 等实现。游戏服务提供单元 1181 包括游戏控制单元 1701、素材库 1707 和内容库 1709。

[0973] 游戏控制单元 1701 例如由 CPU、ROM、RAM 等实现。游戏控制单元 1701 是链接到素材库 1707 和游戏服务提供服务器 31 的处理单元并且进行游戏的基本设置，如游戏的背景故事和阶段。此外，当执行存储在内容库 1709 和 / 或游戏服务提供服务器 31 中的游戏程序时，游戏控制单元 1701 控制游戏程序的执行，以控制游戏如何进展。游戏控制单元 1701 包括现实世界构建单元 1703 和虚拟世界构建单元 1705。

[0974] 现实世界构建单元 1703 例如由 CPU、ROM、RAM 等实现。现实世界构建单元 1703 是指存储在电力管理装置 11 的存储单元 113 等中的数据库，并且构建集成有关于实际的局部电力管理系统 1 的信息的现实世界。

[0975] 虚拟世界构建单元 1705 例如由 CPU、ROM、RAM 等实现。虚拟世界构建单元 1705 构建在内容程序中预先提供的虚拟世界。

[0976] 游戏控制单元 1701 在将现实世界构建单元 1703 与虚拟世界构建单元 1705 彼此

链接的同时实现与系统链接的娱乐。

[0977] 游戏控制单元 1701 能够访问电力管理装置 11 中的数据库并且还具有对于电力管理装置 11 的控制执行路径。

[0978] 由游戏控制单元 1701 控制的游戏在人物中包括另一局部电力管理系统 1 的成员，并且使得用户能够享受对战或者作为角色扮演游戏的成员远程操作游戏。应当注意，当允许其它系统的成员参与时，应当优选防止此类其它系统的成员访问本系统 1 的现实世界。

[0979] 素材库 1707 是设置在游戏服务提供单元 1181 中的数据库。与游戏内容中出现的诸如虚拟家具、虚拟设备和人物的素材以及在游戏期间出现的物品等有关的信息被记录在素材库 1707 中。应当注意，素材库 1707 可存在于游戏服务提供服务器 31 中。

[0980] 内容库 1709 是设置在游戏服务提供单元 1181 中的另一数据库。在内容库 1709 中存储能够由电力管理装置 11 执行的游戏内容的各种实际程序。

[0981] 图 77 示出内容库 1709 中存储的游戏内容的一个示例。下面简要描述游戏内容的特定示例。

[0982] 房间装饰（现实世界游戏）

[0983] 该游戏具有以下构思：自房间的当前布局改变家具和家用设备的布局，搭配窗帘和地毯，购买新的家具和家用设备，以及争取生成具有最佳色彩和品位的内部设计。该游戏使得用户能够掌握设备所使用的总电量如何随着改变房间布局而变化，或者掌握当购买并安装了新的家用设备时电量发生什么变化。这里，提供能够显示具有现实世界属性（如制造商、设计和电力消耗）的物品的库。这样的库可以存储在游戏服务提供服务器 31 中。对于与现实世界链接的改进的物品，可以实施“结果应用模式”（在该模式中，游戏结果被应用于现实世界系统）。

[0984] 送别电老虎 (The Power Eaters)（现实世界 + 虚拟世界游戏）

[0985] 该游戏显示当前房间中的当前电力使用并且关闭不需要的灯。该游戏还允许用户通过调整照明、音量等来争取降低电力和 / 或从售卖更多电力中获利。结果应用模式可针对该游戏的该部分实施。游戏还具有虚拟世界的概念，在该虚拟世界中，“电老虎”四处游走，将灯打开，而用户尽其最大可能争取打败该“电老虎”。

[0986] 终极生活方式冒险队（现实世界 + 虚拟世界游戏）

[0987] 该游戏由如下阶段组成：用户打算使用实际家庭中存在的设备来实现终极低消耗生活方式的阶段，以及用户打算使用虚拟家庭中的设备达到终极生活方式的阶段。

[0988] 拯救地球！重现绿色大工程（虚拟世界游戏）

[0989] 该游戏具有以下构思：用户争取从由 CO2 排放引起的全球变暖危机中存活下来。用户装扮国家环境大臣的角色并通过各关，同时掌握国内公众意见并与其它国家谈判。这是智力游戏，该智力游戏能够使用现实世界的统计和情形来实现关于环境的先进知识。

[0990] 角色扮演游戏（现实世界 + 虚拟世界游戏）

[0991] 该游戏具有仅第一层与现实世界链接的阶段，而其它阶段提供匹配形式的虚拟环境（例如，花园、储藏室和密闭室），然后在其中开展故事。在现实世界阶段中，能够对可以反映在电力状态上的游戏结果实施结果应用模式。

[0992] (2-3) 链接到数据库

[0993] 接着，将参考图 78 描述与电力管理装置 11 的数据库的链接，在该数据库中存储表

明现实世界的局部电力管理系统 1 的状态的各种信息。图 78 是用于说明与电力管理装置中的数据库的链接的示图。

[0994] 作为示例，以下示出的数据被存储在电力管理装置 11 中所存储的数据库中。

[0995] - 可控制设备的设备信息、电动交通工具、发电装置、电力存储装置、设备的蓄电池、可控制插座、插座扩展装置等；

[0996] - 关于上述装置的电力信息（使用 / 电力存储状态）和位置信息；

[0997] - 注册的用户和访问权利；

[0998] - 电费信息和账户信息；

[0999] - 时间、天气、温度。

[1000] 通过使用这些数据，游戏控制单元 1701 在游戏中再现现实世界。

[1001] 通过布置这些设备，现实世界构建单元 1703 能够构想游戏场景的整体建筑平面图。例如，通过假设具有冰箱等表示就餐区域，具有个人计算机或灯表示私人房间，具有洗衣机表示浴室或洗手间区域，具有电动交通工具表示车库，并且具有灯表示走廊，可以构想建筑平面图。现实世界构建单元 1703 基于这样的假设确定建筑平面图，并且从素材库 1707 布置代表设备、家具等的物品。

[1002] 现实世界构建单元 1703 基于注册的用户信息确定游戏人物。在现实世界中，实际设备和物品属性是链接的，使得可以显示这些设备并且在结果应用模式中执行诸如切断电源的动作。因此，当用户选择了显示屏幕等上显示的诸如设备图标的对象时，显示在数据库中所写入的各种信息，例如所选设备的设备信息、电力信息等。

[1003] 由于当游戏中仅使用现实世界时游戏场景会受限，所以虚拟世界构建单元 1703 将游戏内容中预先设置的虚拟世界加入到基于现实世界设置的游戏场景中，以配置更多游戏场景（故事背景）。

[1004] 在图 78 中，示出在显示装置的显示区域中显示现实世界的状态。用户能够在操作主要角色时享受该阶段的游戏。

[1005] (2-4) 与系统链接的娱乐的安全性

[1006] 接着，将参考图 79 描述与系统链接的娱乐的安全性。图 79 是用于说明与系统链接的娱乐的安全性的示图。

[1007] 在执行本游戏的系统中，优选关注关于安全性的以下三点：

[1008] (1) 由于电力管理装置上的游戏接受匿名第三方参加，或者由于来自使用这些连接的恶意第三方的攻击，所以存在以下风险：电力管理装置损坏、对结果应用模式的控制权受到损害、电力管理装置中的保密信息泄露等。

[1009] (2) 从恶意的第三方设备执行电力管理装置上的游戏并且实施有害行为。

[1010] (3) 电力管理装置和与售卖电力相关的服务提供服务器（电力销售管理服务器）之间的保密信息（账户 / 收费信息等）泄露。

[1011] 安全风险 1

[1012] 首先，当电力管理装置上的游戏所接受的匿名第三方参与时，该游戏被设计成将该参与限制于仅由虚拟世界构成的阶段，从而防止从游戏中泄露电力管理装置中的保密信息。

[1013] 接着，为了阻止来自恶意第三方的攻击，必需防止第三方随意地控制电力管理装

置。为此，通过将病毒移除软件安装至电力管理装置中，来检测和 / 或移除第三方攻击。通过使用电子水印来防止电力管理装置被接管以及通过使用分析服务器 34 来根据执行历史检测可疑的重复攻击等并防止执行和 / 或切断连接，可提供进一步的保护以免受攻击。

[1014] 安全风险 2

[1015] 设备和玩家检查成员是否为被允许玩该游戏的合法成员。即使该成员是合法成员，但是由于小孩优选不参与诸如售电的行为，所以访问游戏自身被分成多个级别并且进行成员是否具有访问权利和 / 或是否能够实施结果应用模式的设置。当允许其它用户玩游戏时，则执行控制以防止故事使用现实世界信息。

[1016] 因此，在电力管理装置中预先设置设备和用户，指定访问级别，并且对于设备和用户两者实施认证。该认证能够使用与第一实施例中示出的使用公开密钥或公共密钥或者两者的方法相同的方案。优选还在游戏中包括用于以指定间隔实施认证的配置。优选还在没有访问权限的用户使用该游戏时防止数据库被访问。

[1017] 安全风险 3

[1018] 优选在售卖电力期间而不是仅仅对于本游戏实施安全措施。如果由局部电力管理系统 1 通过因特网进行的服务认证起作用，则这应该不成问题。

[1019] (2-5) 与系统链接的娱乐的流程

[1020] 接着，将参考图 80 至图 81B 描述由根据本实施例的电力管理装置 11 提供的与系统链接的娱乐的流程。图 80 至图 81B 是用于说明与系统链接的娱乐的流程的流程图。注意，图 80 至图 81B 用于说明作为与系统链接的娱乐的一个示例的游戏。

[1021] 注意，在以下说明开始之前，假设希望玩与局部电力管理系统 1 链接的游戏的用户通过操作显示终端（例如，诸如电视机的显示设备，或者诸如移动电话或移动游戏控制台的便携式设备）玩该游戏，该显示终端具有显示屏并且能够连接至电力管理装置 11。用户用以玩游戏的设备也可以是电力管理装置 11 自身。

[1022] 首先，将参考图 80 描述整体流程。

[1023] 首先，用户接通显示终端 125 的电力以激活终端自身（步骤 S5001）。在激活终端后，用户选择用于启动游戏的诸如图标的对象，从而请求电力管理装置 11 启动游戏。

[1024] 接收到请求的电力管理装置 11 实施对显示终端进行认证的处理，以判断请求启动游戏的显示终端是否是由电力管理装置 11 自身管理的被管理设备（步骤 S5003）。此外，如图 81A 和图 81B 具体所示，由于提供给用户的游戏的功能根据显示终端是否为被管理设备而不同，所以电力管理装置 11 检查设置信息（步骤 S5005）并且确认能提供哪些功能。此后，电力管理装置 11 启动游戏程序（步骤 S5007）并且将必要信息类型发送至显示终端。

[1025] 显示终端接收从电力管理装置 11 发送的数据类型并且将游戏的初始画面显示在显示终端 125 的显示屏幕上（步骤 S5009）。用户选择代表游戏并且显示在初始画面上的诸如图标的对象（步骤 S5011），以指定用户希望玩的游戏内容。这里，显示屏幕上显示的游戏为允许用户执行的除内容库 1709 等中存储的游戏之外的游戏。

[1026] 用户操作显示终端 125 的输入装置（鼠标、键盘、触摸板等）以开始游戏（步骤 S5013）。根据显示终端上的游戏进展，电力管理装置 11 载入各数据、准备数据和 / 或存储游戏内容（步骤 S5015）。

[1027] 存在以下情况 :在游戏期间的任意时间，用户请求开始结果应用模式，在该结果应

用模式中，游戏结果被应用于实际系统（步骤 S5017）。接收到请求的电力管理装置 11 检查是否可由发出结果应用模式的开始请求的用户执行结果应用模式（步骤 S5019）。在检查设置信息等以检查用户的访问权和执行权从而确认执行风险后（步骤 S5020），电力管理装置 11 向显示终端呈现在结果应用模式之外的可执行动作的范围（步骤 S5021）。

[1028] 在显示终端处，在显示屏幕上显示从电力管理装置 11 呈现的内容并邀请用户选择执行内容（步骤 S5023）。显示终端将用户的选择的内容通知给电力管理装置 11。

[1029] 根据用户的选择结果，电力管理装置 11 向配电装置发出针对该选择结果的适当执行指令（步骤 S5025）。电力管理装置 11 更新日志信息（步骤 S5027）并且通知用户结果应用模式的执行已结束（步骤 S5029）。

[1030] 接着，将参考图 81A 和图 81B 描述与系统链接的娱乐的具体流程。

[1031] 如前所述，用户操作执行游戏的设备以开始游戏，电力管理装置 11 的游戏服务提供单元 1181 等待从显示终端发送对游戏的启动请求（步骤 S5031）。

[1032] 当从显示终端发送了游戏开始请求时，电力管理装置 11 实施对发送了游戏开始请求的显示终端的设备认证（步骤 S5033）。通过这样做，电力管理装置 11 能够检查已请求游戏开始的显示终端是否是由电力管理装置 11 自身管理的被管理设备（步骤 S5035）。

[1033] 当显示终端不是被管理设备时，电力管理装置 11 的游戏服务提供单元 1181 检查是否允许电力管理装置 11 的用户开始游戏（步骤 S5037），并且如果不允许电力管理装置 11 的用户执行游戏，则处理结束。如下所述，当允许电力管理装置 11 的用户执行游戏时，电力管理装置 11 的游戏服务提供单元 1181 实施步骤 S5039。

[1034] 同时，如果显示终端是被管理设备，或者显示终端虽然不是被管理设备但是已从电力管理装置 11 的用户获得允许来执行游戏，则电力管理装置 11 的游戏服务提供单元 1181 进行用户认证（步骤 S5039）。

[1035] 如果电力管理装置 11 的游戏服务提供单元 1181 已确认用户是电力管理装置 11 中注册的成员，则根据用户的控制权的级别设置游戏的访问级别和结果应用模式的控制级别（步骤 S5041）。

[1036] 接着，电力管理装置 11 的游戏服务提供单元 1181 启动游戏的主程序（步骤 S5043）并且使游戏的初始显示显示在用户所使用的显示终端上。

[1037] 一旦显示终端的用户选择了用户希望玩的游戏内容，选择结果被发送至电力管理装置 11，使得电力管理装置 11 的游戏服务提供单元 1181 能够指定选择的游戏内容（步骤 S5045）。

[1038] 电力管理装置 11 的游戏服务提供单元 1181 检查指定的内容是否能够由显示终端的用户访问以及结果应用模式是否能够实施（步骤 S5047）。

[1039] 当游戏用户不具有访问权或者不具有实施结果应用模式的授权时，电力管理装置 11 的游戏服务提供单元 1181 进行设置，使得在游戏被激活时不可访问数据库和实施结果应用模式（步骤 S5049）。

[1040] 当游戏用户具有访问权并且能够实施结果应用模式时，电力管理装置 11 访问数据库并且收集被管理设备的设备信息和电力信息（步骤 S5051）。

[1041] 游戏服务提供单元 1181 的游戏控制单元 1701 使用步骤 S5051 中收集的各种信息来构建游戏的诸如故事背景的基本设置（步骤 S5053）。当结束对基本设置的构建时，游戏

控制单元 1701 基于所设置的故事背景对选择的游戏内容进行执行控制（步骤 S5055）。当此发生时，电力管理装置 11 和显示终端进行交互式通信，使得电力管理装置 11 在终端的显示器上显示游戏画面并且从显示终端发送用户所输入的信息。此外，在该时间期间，电力管理装置 11 的游戏控制单元 1701 判断是否进行了请求结束游戏、暂停游戏等的处理（步骤 S5057）。

[1042] 在用户选择了诸如结束游戏、暂停游戏等的状态后，如果游戏是可激活结果应用模式的内容，则电力管理装置 11 的游戏服务提供单元 1181 检查用户是否希望切换到结果应用模式（步骤 S5059）。

[1043] 如果用户选择不切换到结果应用模式，则电力管理装置 11 的游戏服务提供单元 1181 检查是否保存游戏内容并且结束游戏程序。

[1044] 此外，当切换到结果应用模式时，电力管理装置 11 的游戏服务提供单元 1181 确认用户是否具有结果应用模式的执行权（步骤 S5061）。如果用户不具有结果应用模式的执行权，则电力管理装置 11 的游戏服务提供单元 1181 结束游戏程序。

[1045] 当用户具有结果应用模式的执行权时，电力管理装置 11 的游戏服务提供单元 1181 基于从激活到当前点的游戏内容提取能够对实际设备实施的控制（步骤 S5063）并且向用户显示列表。

[1046] 在显示列表之前，电力管理装置 11 的游戏服务提供单元 1181 应当优选实施风险检查。更具体地，游戏服务提供单元 1181 应当查询分析服务器 34 以基于可控制的内容及其历史检查该控制是否可疑，并且从上述提取的列表中删除可疑控制。通过这样做，除了关于网络攻击等的风险之外，可以检查与关断设备（例如家用设备，如冰箱）电源的命令有关的风险，其中对这些设备优选不中断连接。

[1047] 游戏用户从显示终端的显示屏幕上显示的列表中选择用户希望实施的项目，例如“关闭设备 A”。选择结果被发送到电力管理装置 11 并且电力管理装置 11 能够指定该项目内容（步骤 S5065）。

[1048] 此后，根据用户的选择结果，电力管理装置 11 根据该选择结果向配电装置 121、可控制插座 123、可控制设备 125 等发出执行指令（步骤 S5067）。电力管理装置 11 更新日志信息（步骤 S5069）并且检查所有控制是否均已执行（步骤 S5071）。

[1049] 电力管理装置 11 从命令目标设备接收执行的结束，并且如果所有控制均已执行，则向用户显示结束消息（步骤 S5073）。电力管理装置 11 检查游戏是否要结束或者继续（步骤 S5075），并且在游戏继续时返回步骤 S5055。同时，在游戏要结束时，电力管理装置 11 结束游戏。

[1050] 通过根据上述流程进行处理，电力管理装置能够向用户提供与局部电力管理系统链接的娱乐，例如游戏。结果，由于局部电力管理系统的有吸引力的应用，与系统链接的娱乐能够实际地对电力和 CO_2 的减少作出贡献。

[1051] 硬件配置

[1052] 接着，将参考图 82 具体描述根据本发明实施例的电力管理装置 11 的硬件配置。图 82 是用于说明根据本发明实施例的电力管理装置 11 的硬件配置的框图。

[1053] 电力管理装置 11 主要包括 CPU 901、ROM 903 和 RAM 905。此外，电力管理装置 11 还包括主机总线 907、桥 909、外部总线 911、接口 913、输入装置 915、输出装置 917、存储装

置 919、驱动器 921、连接端口 923 和通信装置 925。

[1054] CPU 901 用作算术处理装置和控制装置，并且根据 ROM 903、RAM905、存储装置 919 或可移动记录介质 927 中记录的各种程序来控制电力管理装置 11 的总体操作或者部分操作。ROM 903 存储由 CPU 901 使用的程序、操作参数等。RAM 905 主要存储 CPU 901 的执行中使用的程序以及在该执行期间适当变化的参数等。这些部件经由由内部总线（如 CPU 总线等）构成的主机总线 907 而彼此连接。

[1055] 主机总线 907 通过桥 909 连接至外部总线 911，例如 PCI（外围组件互连 / 接口）。

[1056] 输入装置 915 是由用户操作的操作部件，例如鼠标、键盘、触摸板、按钮、开关和操作杆。此外，输入装置 915 可以是使用例如红外光或其它无线电波的远程控制部件（所谓的远程控制），或者可以是符合电力管理装置 11 的操作的外部连接装置 929，例如移动电话或 PDA。此外，输入装置 915 基于例如用户利用以上操作部件输入的信息而生成输入信号，并且由用于将输入信号输出至 CPU 901 的输入控制电路构成。电力管理装置 11 的用户能够将各种数据输入电力管理装置 11 并且能够通过操作该输入装置 915 指示电力管理装置 11 执行处理。

[1057] 输出装置 917 由能够将获取的信息在视觉上或者听觉上通知给用户的装置构成。这样的装置的示例包括 :显示装置，例如 CRT 显示装置、液晶显示装置、等离子显示装置、EL 显示装置和灯，音频输出装置，例如扩音器和耳机，打印机，移动电话，传真机等。例如，输出装置 917 输出通过由电力管理装置 11 执行的各种处理获得的结果。更具体地，显示装置以文本或图像形式显示通过由电力管理装置 11 执行的各种处理获得的结果。另一方面，音频输出装置将音频信号（如再现的音频数据和声音数据）转换成模拟信号，并输出该模拟信号。

[1058] 存储装置 919 是被配置为电力管理装置 11 的存储单元的示例的用于存储数据的装置，并用于存储数据。存储装置 919 例如由诸如 HDD（硬盘驱动器）的磁存储装置、半导体存储装置、光存储装置或磁光存储装置构成。存储装置 919 存储将被 CPU 901 执行的程序、各种数据和从外部获得的各种数据。

[1059] 驱动器 921 是用于记录介质的读取器 / 写入器，并且嵌入电力管理装置 11 中或者外部地连接至电力管理装置 11 上。驱动器 921 读取所连接的可移动记录介质 927（如磁盘、光盘、磁光盘或半导体存储器）中记录的信息，并且将所读取的信息输出至 RAM 905。此外，驱动器 921 能够写所连接的可移动记录介质 927，例如磁盘、光盘、磁光盘或半导体存储器。可移动记录介质 927 为例如 DVD 介质、HD-DVD 介质或蓝光介质。可移动记录介质 927 可以是致密闪存 (CF，注册商标）、闪速存储器、SD 存储卡（安全数字存储卡）等。可替换地，可移动记录介质 927 可以例如为装配有非接触式 IC 芯片或电子设备的 IC 卡（集成电路卡）。

[1060] 连接端口 923 是用于允许装置直接连接至电力管理装置 11 的端口。连接端口 923 的示例包括 USB（通用串行总线）端口、IEEE 1394 端口、SCSI（小型计算机系统接口）端口等。连接端口 923 的其它示例包括 RS-232C 端口、光学音频终端、HDMI（高清晰度多媒体接口）端口等。通过连接至该连接端口 923 的外部连接的装置 929，电力管理装置 11 从外部连接的装置 929 直接获得各种数据并且向外部连接的装置 929 提供各种数据。

[1061] 通信装置 925 是例如由用于连接至通信网络 931 的通信装置构成的通信接口。通信装置 925 例如为有线或无线 LAN（局域网）、蓝牙（注册商标）、WUSB（无线 USB）的通信

卡等。可替换地，通信装置 925 可以是用于光通信的路由器、用于 ADSL（非对称数字用户线）的路由器、用于各种通信的调制解调器等。该通信装置 925 例如能够根据因特网上的预定协议（如 TCP/IP）与其它通信装置发送和接收信号等。连接至通信装置 925 的通信网 931 由经由有线或无线连接的网络等构成，例如可以为因特网、家庭 LAN、红外通信、无线波通信、卫星通信等。

[1062] 到此为止，已示出能够实现根据本发明实施例的电力管理装置 11 的功能的硬件配置的示例。每个上述结构器件可以使用通用材料构成，或者可以由专用于每个结构器件的功能的硬件构成。因此，要使用的硬件配置能够根据实行本发明时的技术水平而适当变化。

[1063] 由于根据本发明实施例的可控制设备 125 和分析服务器 34 的硬件配置与根据本发明实施例的电力管理装置 11 的配置相同，所以省略其具体描述。

[1064] 尽管已参考附图具体描述了本发明的优选实施例，但是本发明不限于以上示例。本领域技术人员应当理解，依据设计要求以及其它因素，只要各种变型、组合、子组合和替选方案在所附权利要求书及其等同内容的范围内，则可以进行这些变型、组合、子组合和替选方案。

[1065] 本申请包含与 2010 年 1 月 25 日向日本专利局提交的日本优先权专利申请 JP 2010-013672 中公开的主题相关的主题，该优先权专利申请的整体内容通过引用合并于此。

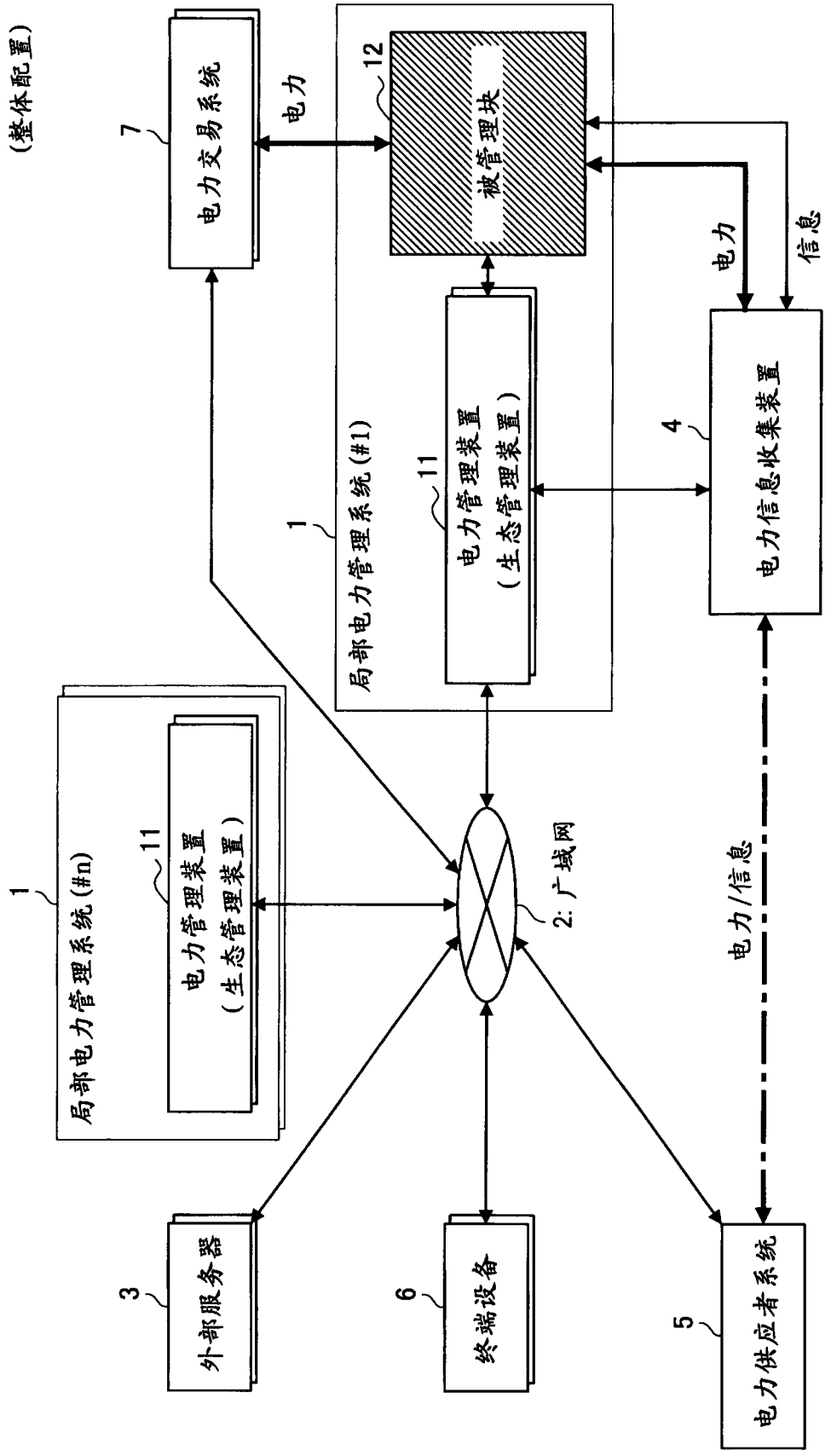

(整体配置)
7
电力交易系统
电力
12
被管理块
局部电力管理系统(#1)
1
11
电力管理装置
(生态管理装置)
电力
信息
4
电力信息收集装置
局部电力管理系统(#n)
1
11
电力管理装置
(生态管理装置)
2: 广域网
电力/信息
3
外部服务器
6
终端设备
5
电力供应者系统

图 1

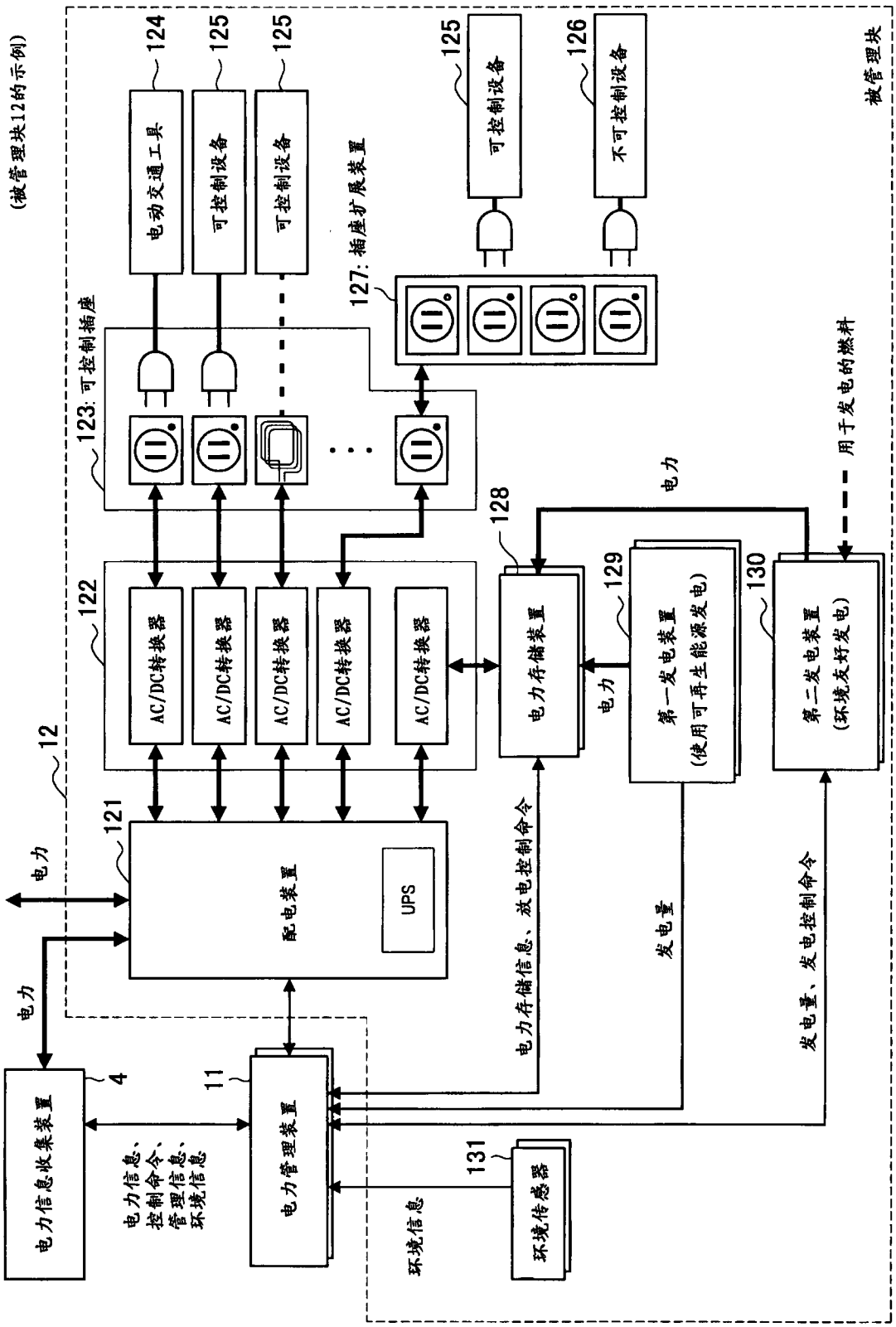

(被管理块12的示例)
被管理块
电动交通工具
可控制设备
可控制设备
可控制设备
不可控制设备
124
125
125
125
126
127: 插座扩展装置
123: 可控制插座
122
AC/DC转换器
AC/DC转换器
AC/DC转换器
AC/DC转换器
AC/DC转换器
128
电力存储装置
129
第一发电装置
(使用可再生能源发电)
130
第二发电装置
(环境友好发电)
电力
电力
用于发电的燃料
12
121
电力
配电装置
UPS
电力存储信息、放电控制命令
发电量
发电量、发电控制命令
电力
4
11
电力信息收集装置
电力信息、
控制命令、
管理信息、
环境信息
电力管理装置
131
环境信息
环境传感器

图 2

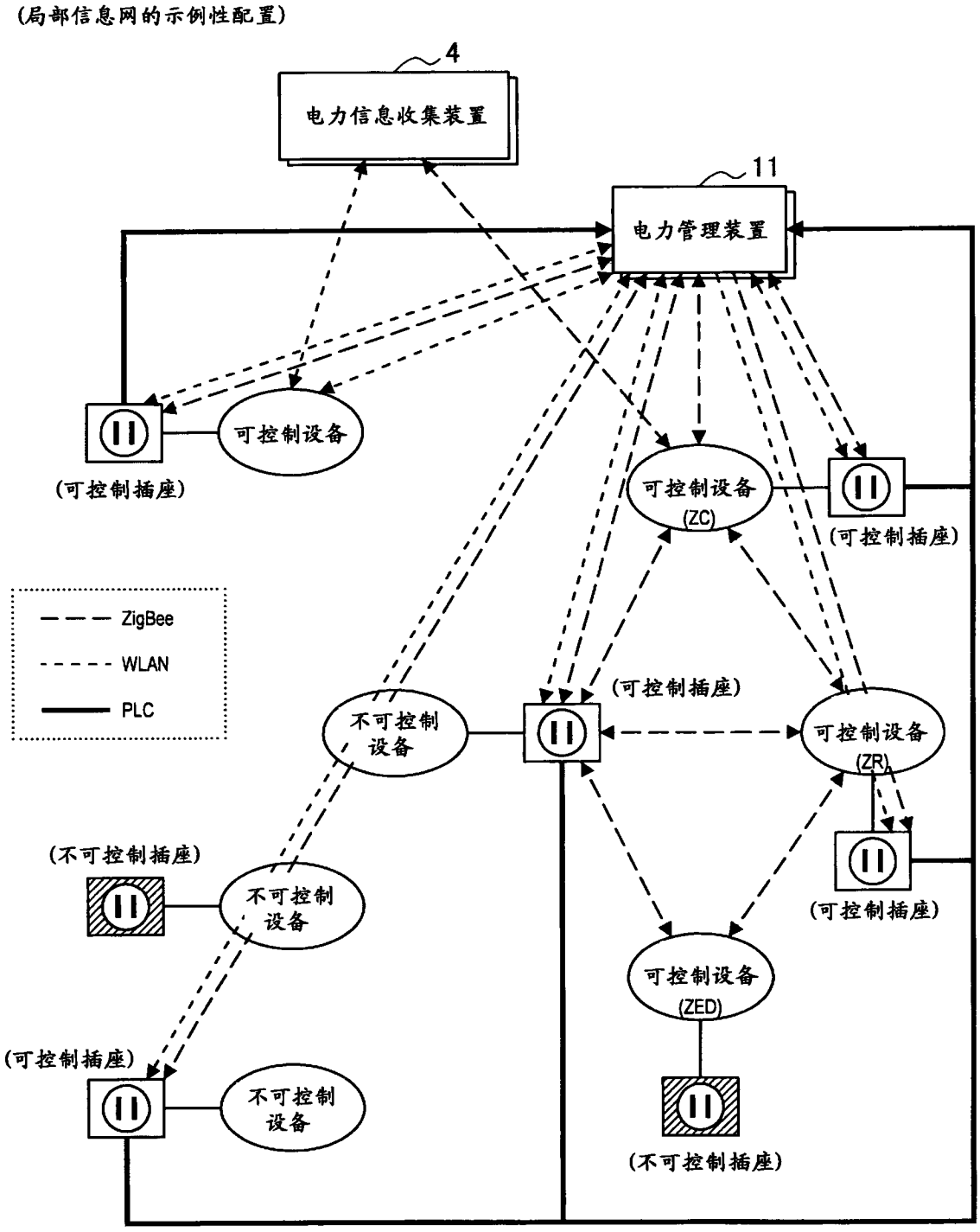

(局部信息网的示例性配置)
4
电力信息收集装置
11
电力管理装置
可控制设备
(可控制插座)
可控制设备
(ZC)
(可控制插座)
ZigBee
WLAN
PLC
(可控制插座)
不可控制
设备
可控制设备
(ZR)
(不可控制插座)
不可控制
设备
(可控制插座)
可控制设备
(ZED)
(可控制插座)
不可控制
设备
(不可控制插座)

图 3

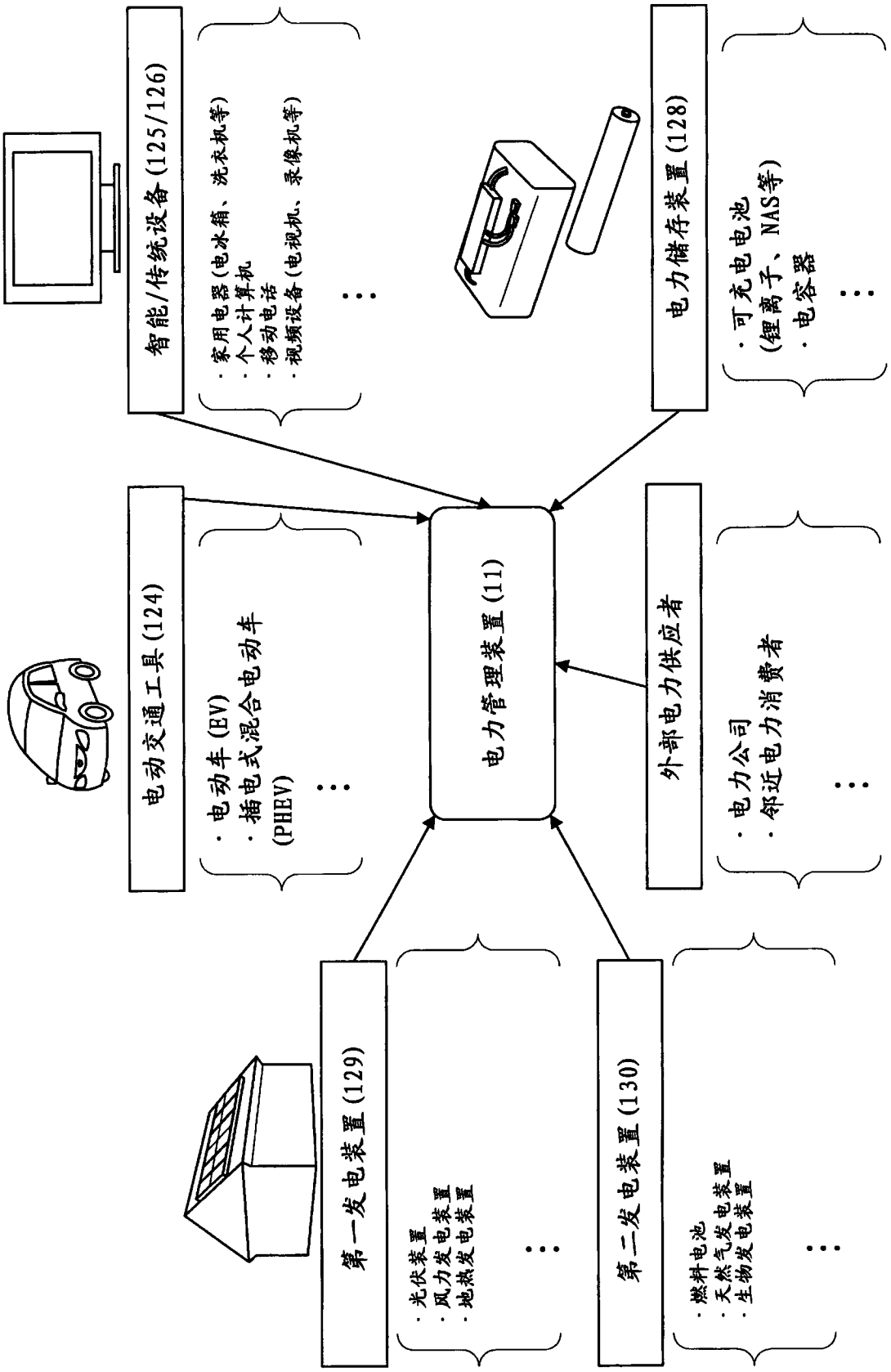

智能/传统设备(125/126)
·家用电器(电冰箱、洗衣机等)
·个人计算机
·移动电话
·视频设备(电视机、录像机等)
电力储存装置(128)
·可充电电池
(锂离子、NAS等)
·电容器
电动交通工具(124)
·电动车(EV)
·插电式混合电动车
(PHEV)
电力管理装置(11)
外部电力供应者
·电力公司
·邻近电力消费者
第一发电装置(129)
·光伏装置
·风力发电装置
·地热发电装置
第二发电装置(130)
·燃料电池
·天然气发电装置
·生物发电装置

图 4

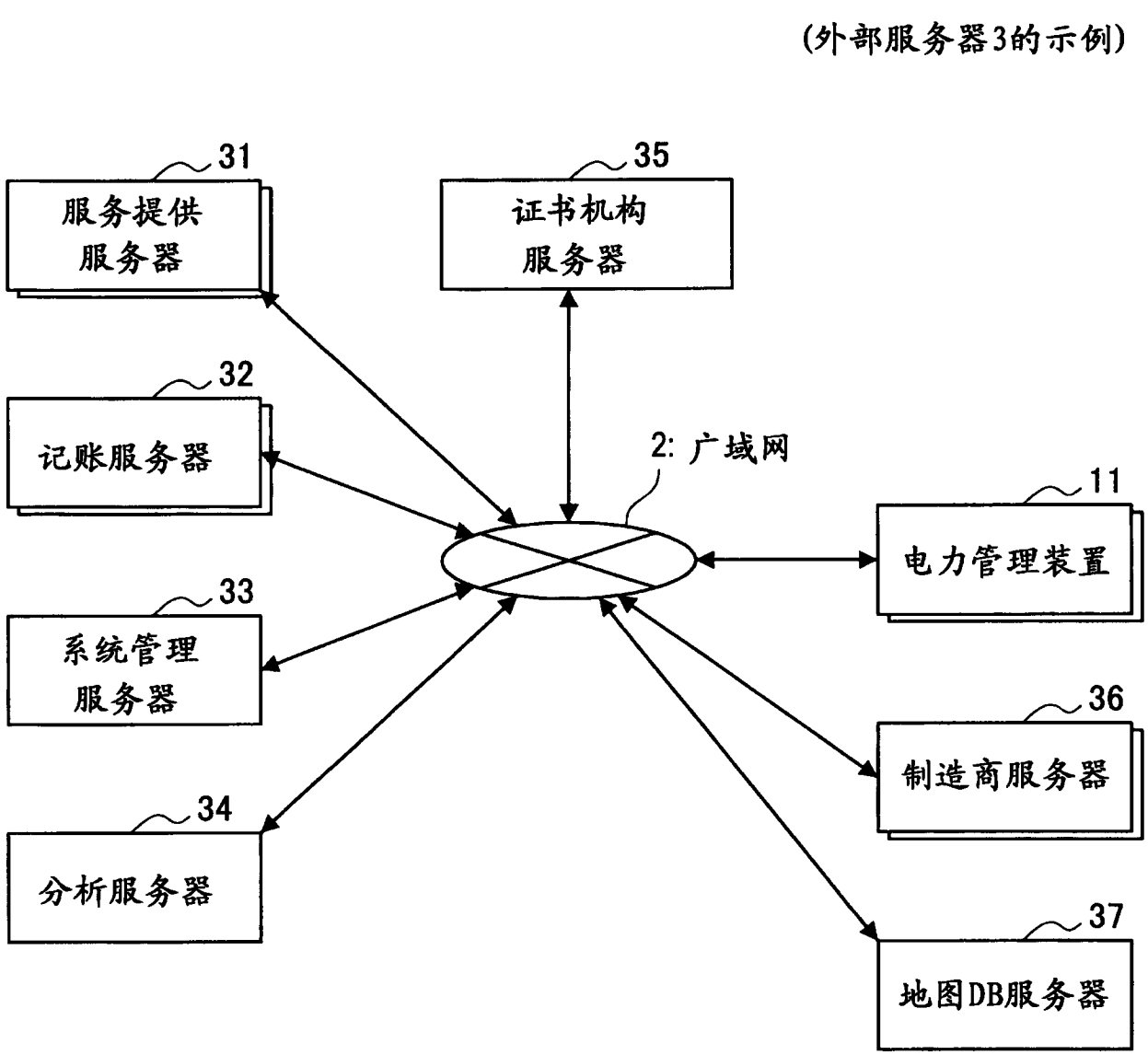

(外部服务器3的示例)
31
服务提供
服务器
35
证书机构
服务器
32
记账服务器
2: 广域网
11
电力管理装置
33
系统管理
服务器
36
制造商服务器
34
分析服务器
37
地图DB服务器

图 5

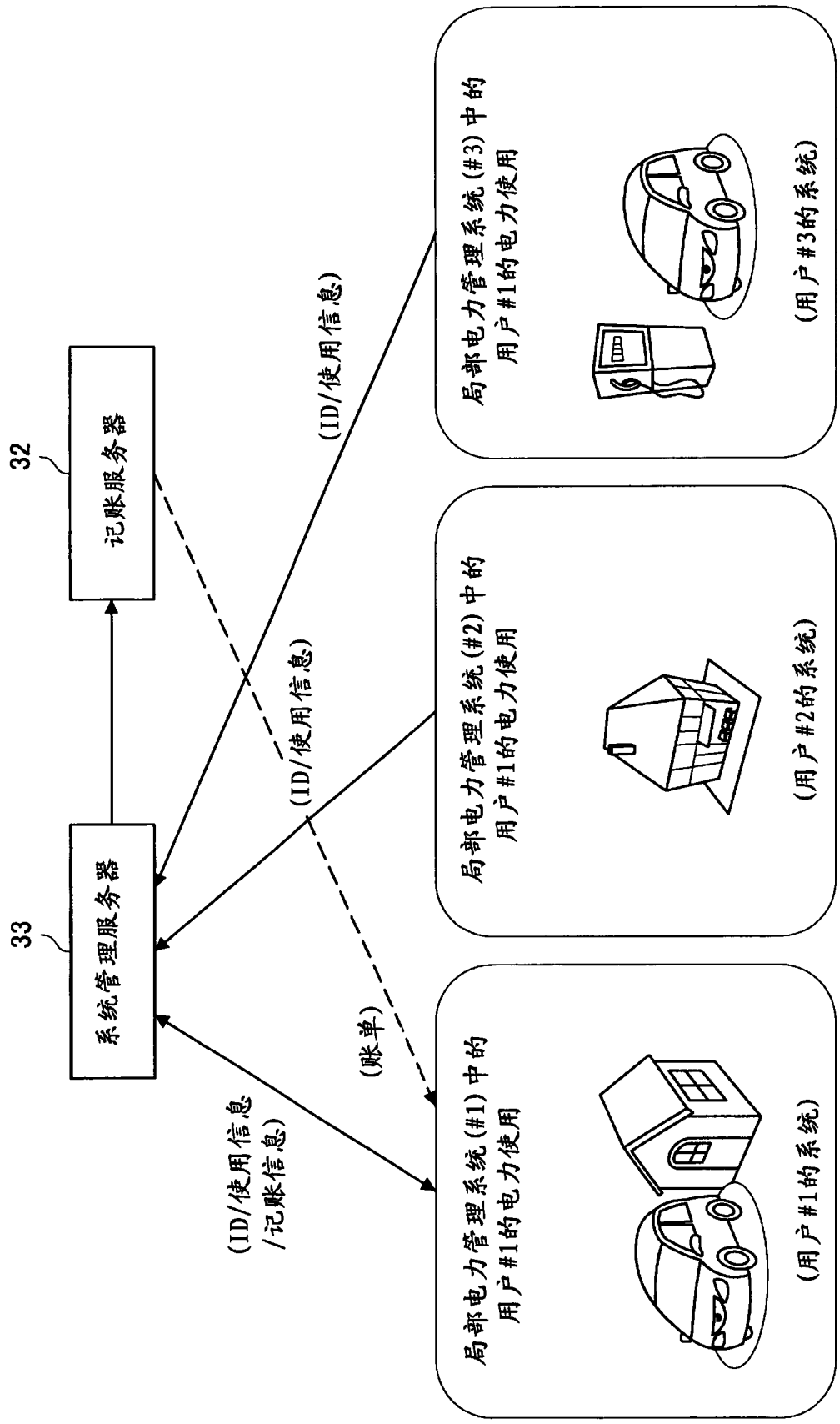

32
记账服务器
33
系统管理服务器
(ID/使用信息)
(ID/使用信息)
(账单)
(ID/使用信息
/记账信息)
局部电力管理系统(#3)中的
用户#1的电力使用
(用户#3的系统)
局部电力管理系统(#2)中的
用户#1的电力使用
(用户#2的系统)
局部电力管理系统(#1)中的
用户#1的电力使用
(用户#1的系统)

图 6

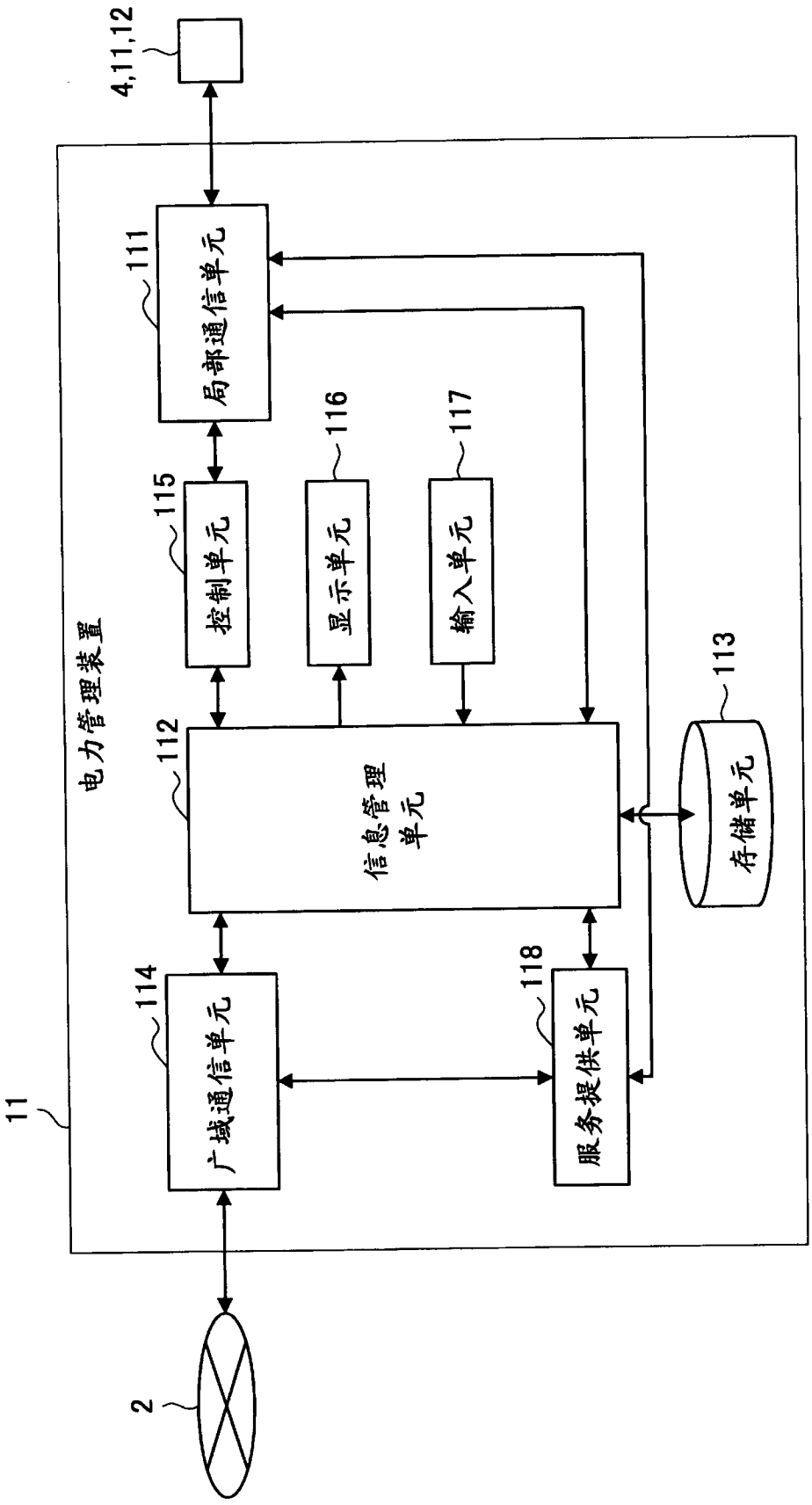

4,11,12
111
局部通信单元
115
控制单元
116
显示单元
117
输入单元
113
存储单元
112
信息管理单元
电力管理装置
114
广域通信单元
118
服务提供单元
11
2

图 7

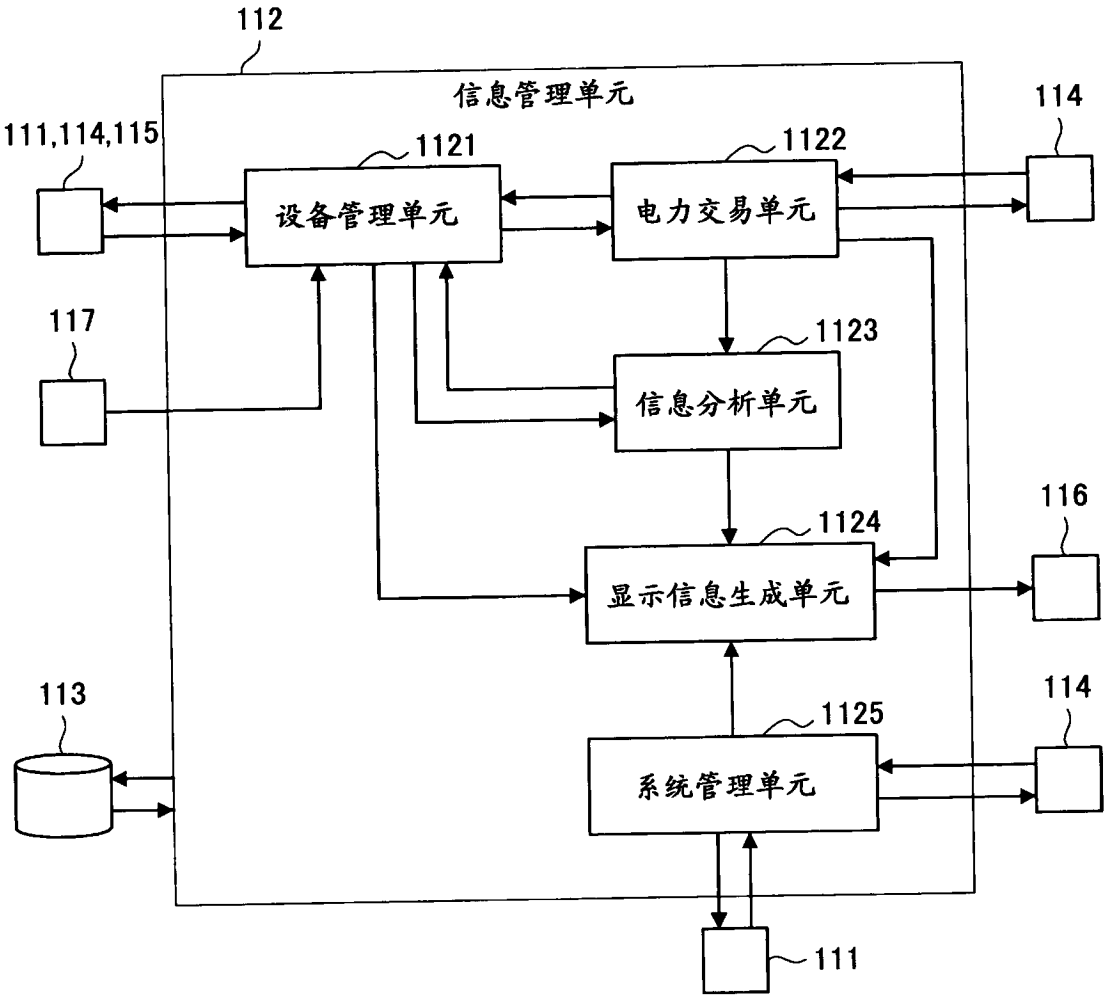

112
信息管理单元
111,114,115
1121
设备管理单元
1122
电力交易单元
114
117
1123
信息分析单元
116
1124
显示信息生成单元
113
1125
系统管理单元
114
111

图 8

部件	主要功能概况
设备管理单元 1121	设备注册、设备认证、管理设备ID、管理设备的操作设置/服务设置、 掌握设备的操作状态/使用状态、收集环境信息、掌握使用状态 （以设备、整体系统或具体块为单位）等
电力交易单元 1122	获取市场交易数据/个体交易数据、售卖订单/购买订单的定时控制、 履行售卖订单/购买订单、管理交易日志等
信息分析单元 1123	分析发电数据、分析电力储存数据、学习生活模式、分析电力消费数据 (以设备、整体系统或具体块为单位)、估计电力消费模式、 估计电力储存模式、估计放电模式、估计发电模式、 计算当前CO_2排放量、估计未来CO_2排放量、计算节电模式、 计算低CO_2排放量模式、计算产生节电/低CO_2排放量的设备配置/设备布置等
显示信息生成单元 1124	生成与设备相关的信息、与电力相关的信息、与环境相关的信息、 与交易数据相关的信息、与分析结果相关的信息等
系统管理单元 1125	管理/更新固件版本、访问限制、防病毒措施等

图 9

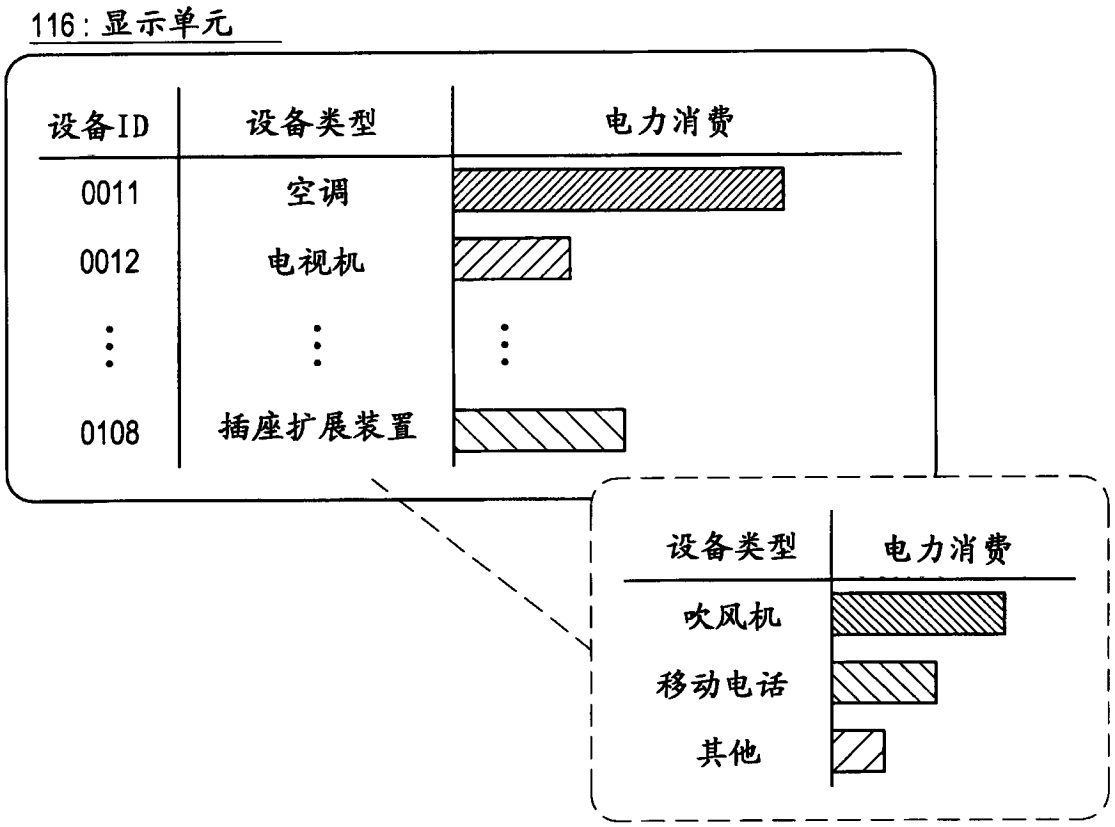

116：显示单元
设备ID
设备类型
电力消费
0011
空调
0012
电视机
0108
插座扩展装置
设备类型
电力消费
吹风机
移动电话
其他

图 10

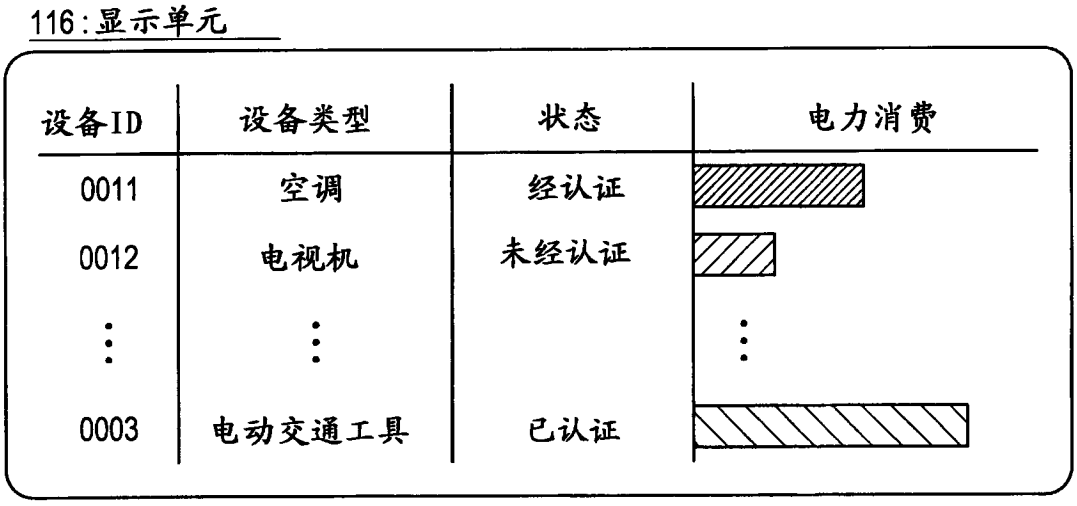

116：显示单元
设备ID
设备类型
状态
电力消费
0011
空调
经认证
0012
电视机
未经认证
0003
电动交通工具
已认证

图 11

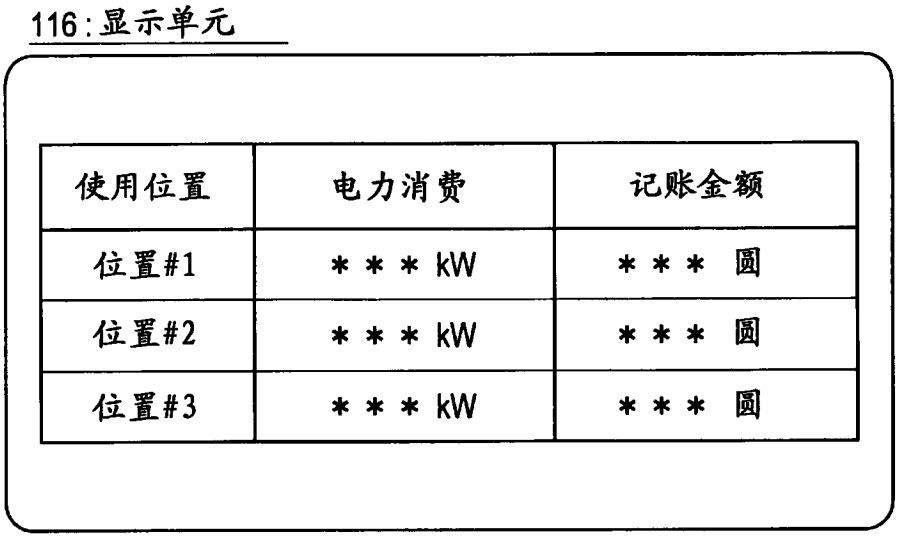

116:显示单元
使用位置
电力消费
记账金额
位置#1
＊＊＊ kW
＊＊＊ 圆
位置#2
＊＊＊ kW
＊＊＊ 圆
位置#3
＊＊＊ kW
＊＊＊ 圆

图 12

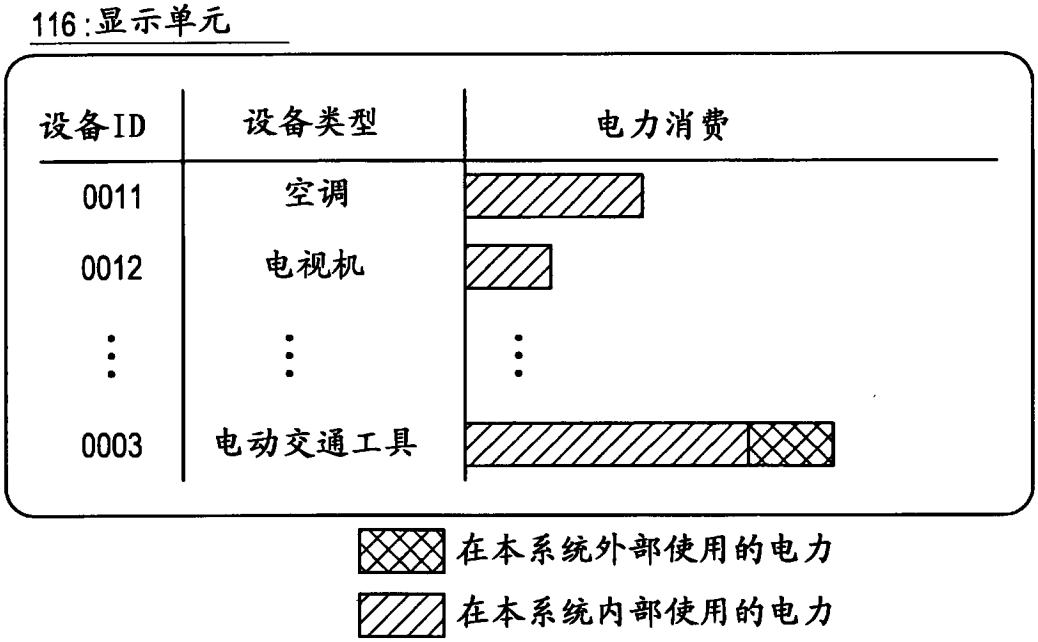

116:显示单元
设备ID
设备类型
电力消费
0011
空调
0012
电视机
0003
电动交通工具
在本系统外部使用的电力
在本系统内部使用的电力

图 13

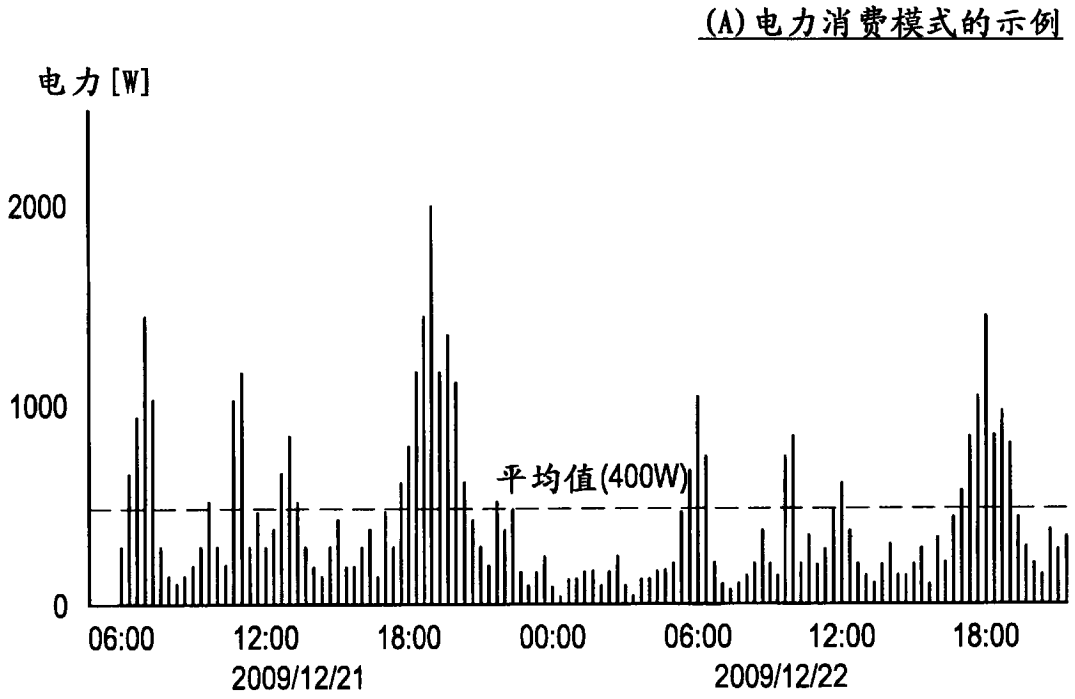

(A)电力消费模式的示例
电力[W]
2000
1000
0
平均值(400W)
06:00
12:00
18:00
00:00
06:00
12:00
18:00
2009/12/21
2009/12/22

图 14

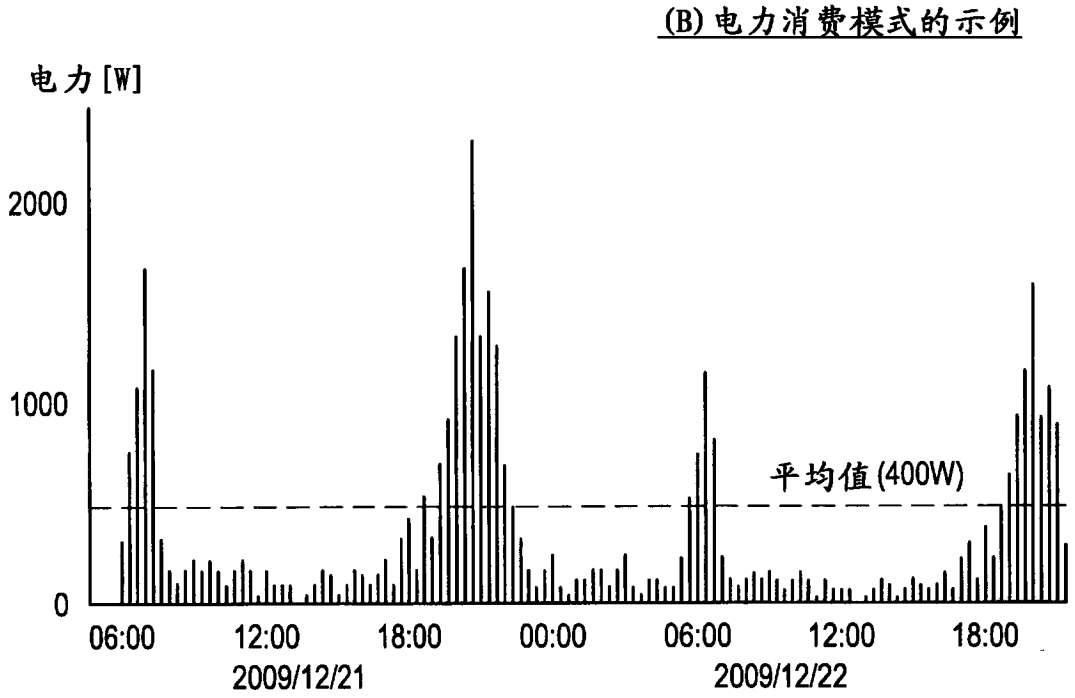

(B)电力消费模式的示例
电力[W]
2000
1000
0
平均值(400W)
06:00
12:00
18:00
00:00
06:00
12:00
18:00
2009/12/21
2009/12/22

图 15

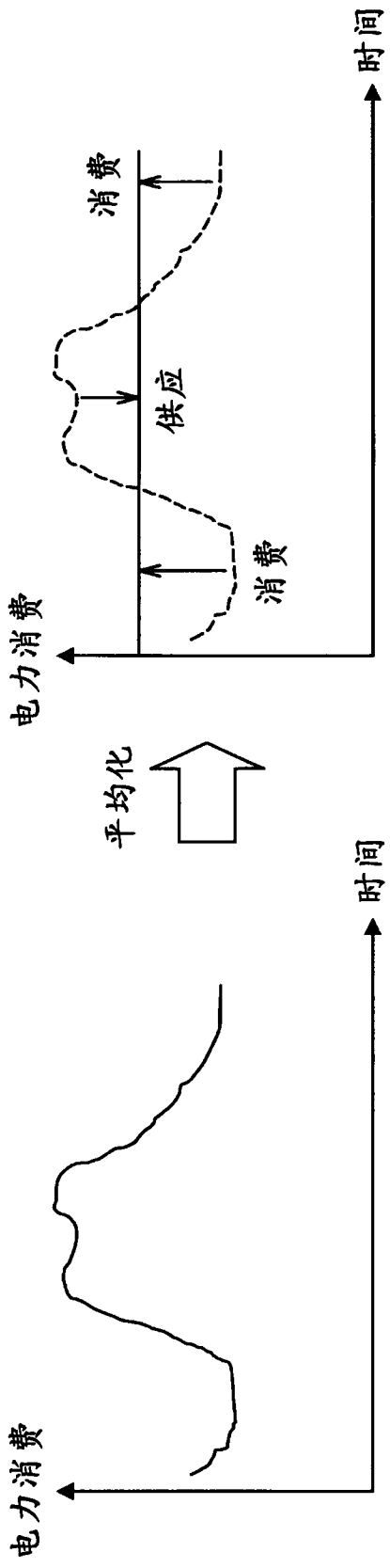


图 16

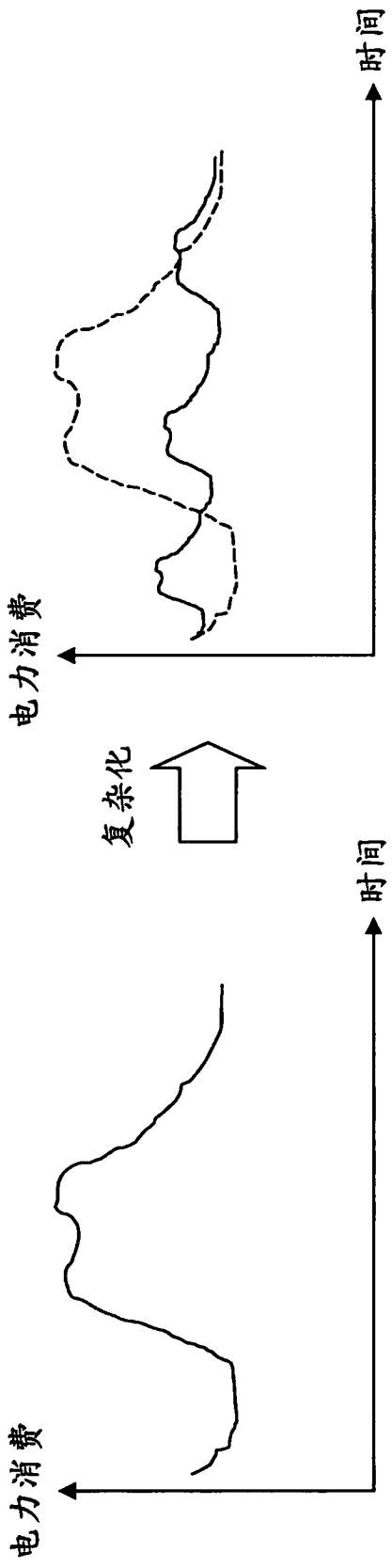


图 17

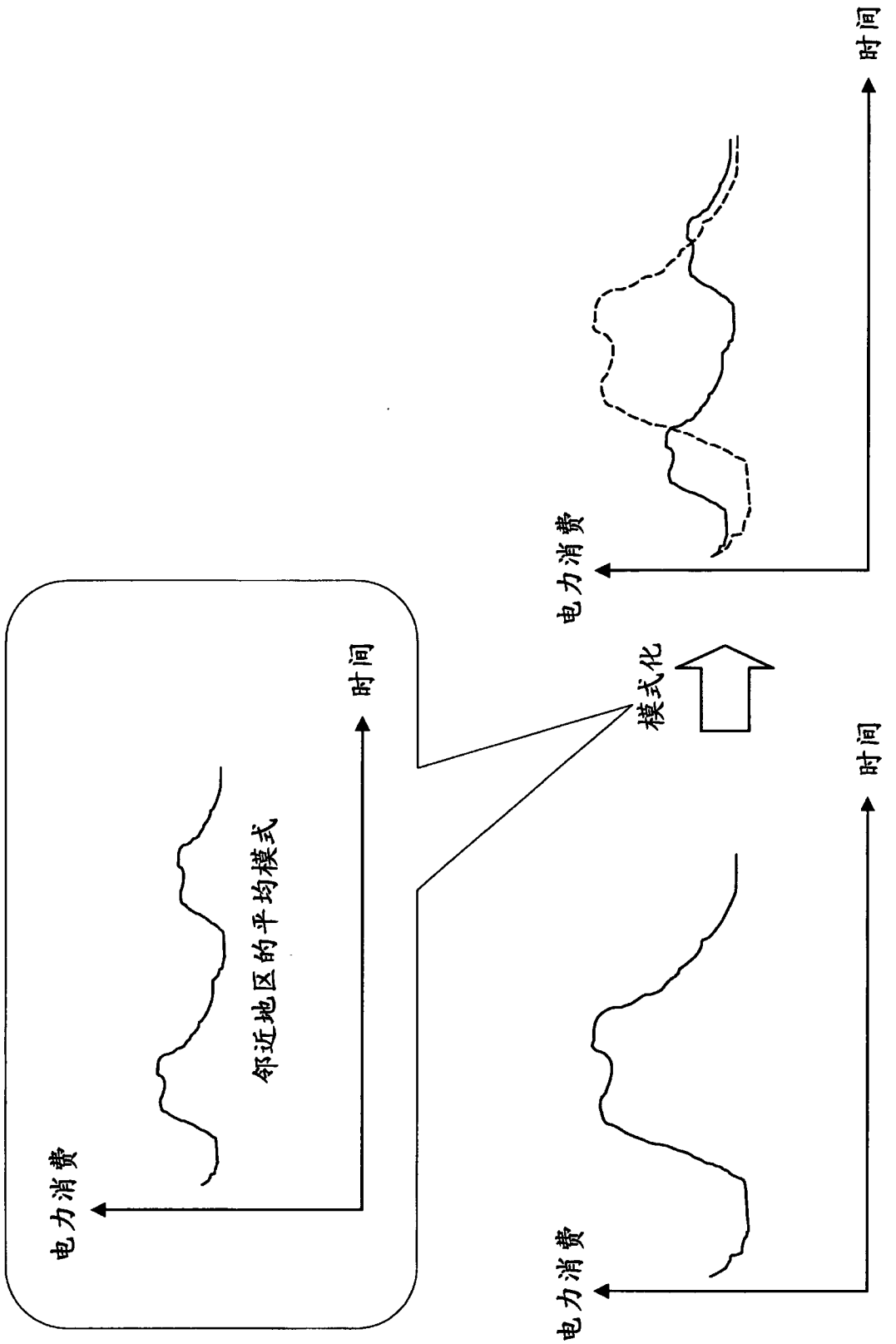


图 18

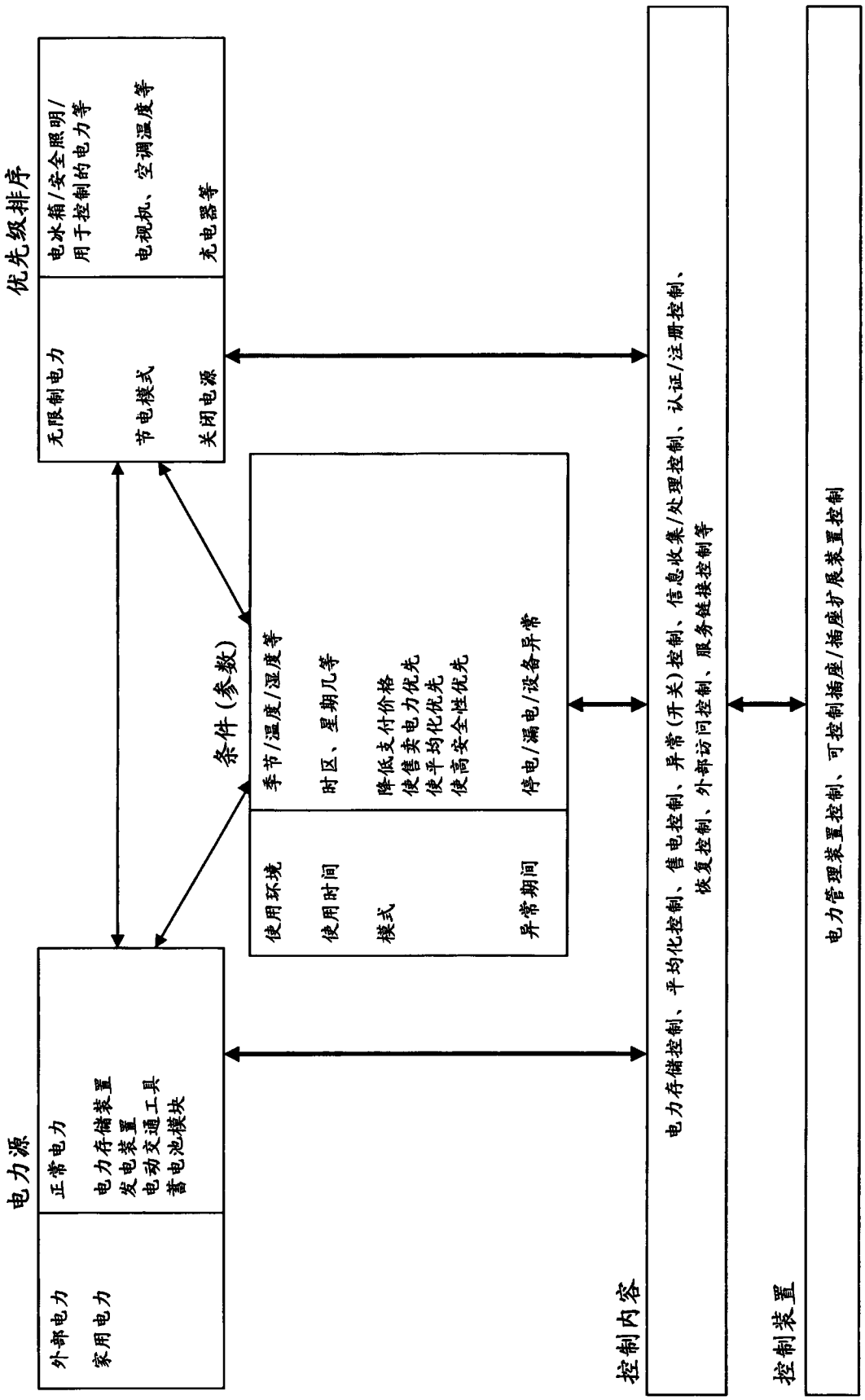

优先级排序
无限制电力
节电模式
关闭电源
电冰箱/安全照明/用于控制的电力等
电视机、空调温度等
充电器等
条件（参数）
季节/温度/湿度等
时区、星期几等
降低支付价格
使售卖电力优先
使平均化优先
使高安全性优先
停电/漏电/设备异常
使用环境
使用时间
模式
异常期间
电力源
正常电力
电力存储装置
发电装置
电动交通工具
蓄电池模块
外部电力
家用电力
控制内容
电力存储控制、平均化控制、售电控制、异常（开关）控制、信息收集/处理控制、认证/注册控制、
恢复控制、外部访问控制、服务链接控制等
控制装置
电力管理装置控制、可控制插座/插座扩展装置控制

图 19

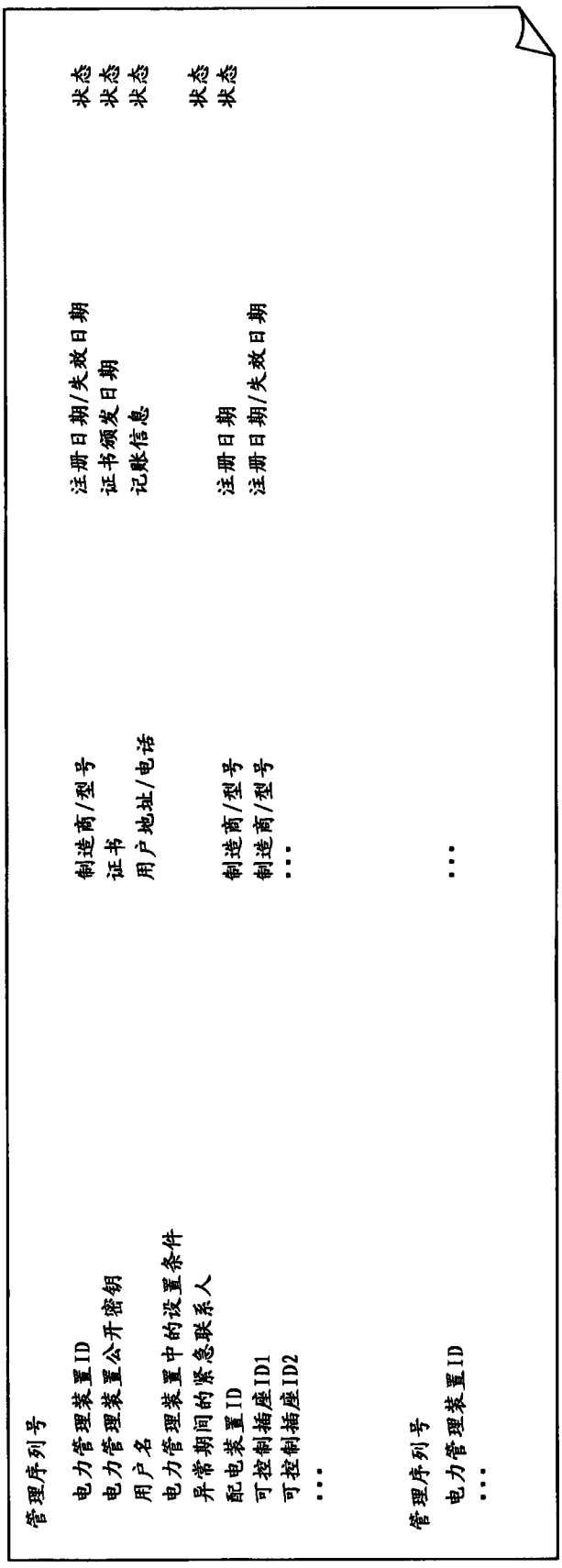

管理序列号
电力管理装置ID
电力管理装置公开密钥
用户名
电力管理装置中的设置条件
异常期间的紧急联系人
配电装置ID
可控制插座ID1
可控制插座ID2
...
制造商/型号
证书
用户地址/电话
...
注册日期/失效日期
证书颁发日期
记账信息
状态
状态
状态
管理序列号
电力管理装置ID
...
制造商/型号
...
注册日期
注册日期/失效日期
状态
状态

图 20

插座类型	被连接设备类型	电力信息通信装置	设备认证装置	电力供应控制
可控制插座	可控制设备	· 来自被连接设备的ZigBee · 来自可控制插座的ZigBee或PLC	· 来自被连接设备的ZigBee	· 从电力管理装置发送到配电装置的控制命令 · 可能来自可控制插座的有限控制
可控制插座	不可控制设备	· 来自可控制插座的ZigBee或PLC	· 无	· 从电力管理装置发送到配电装置的控制命令 · 可能来自可控制插座的有限控制
不可控制插座	可控制设备	· 来自被连接设备的ZigBee	· 来自被连接设备的ZigBee	· 从电力管理装置发送到配电装置的控制命令
不可控制插座	不可控制设备	· 无	· 无	· 恒定电力供应

图 21

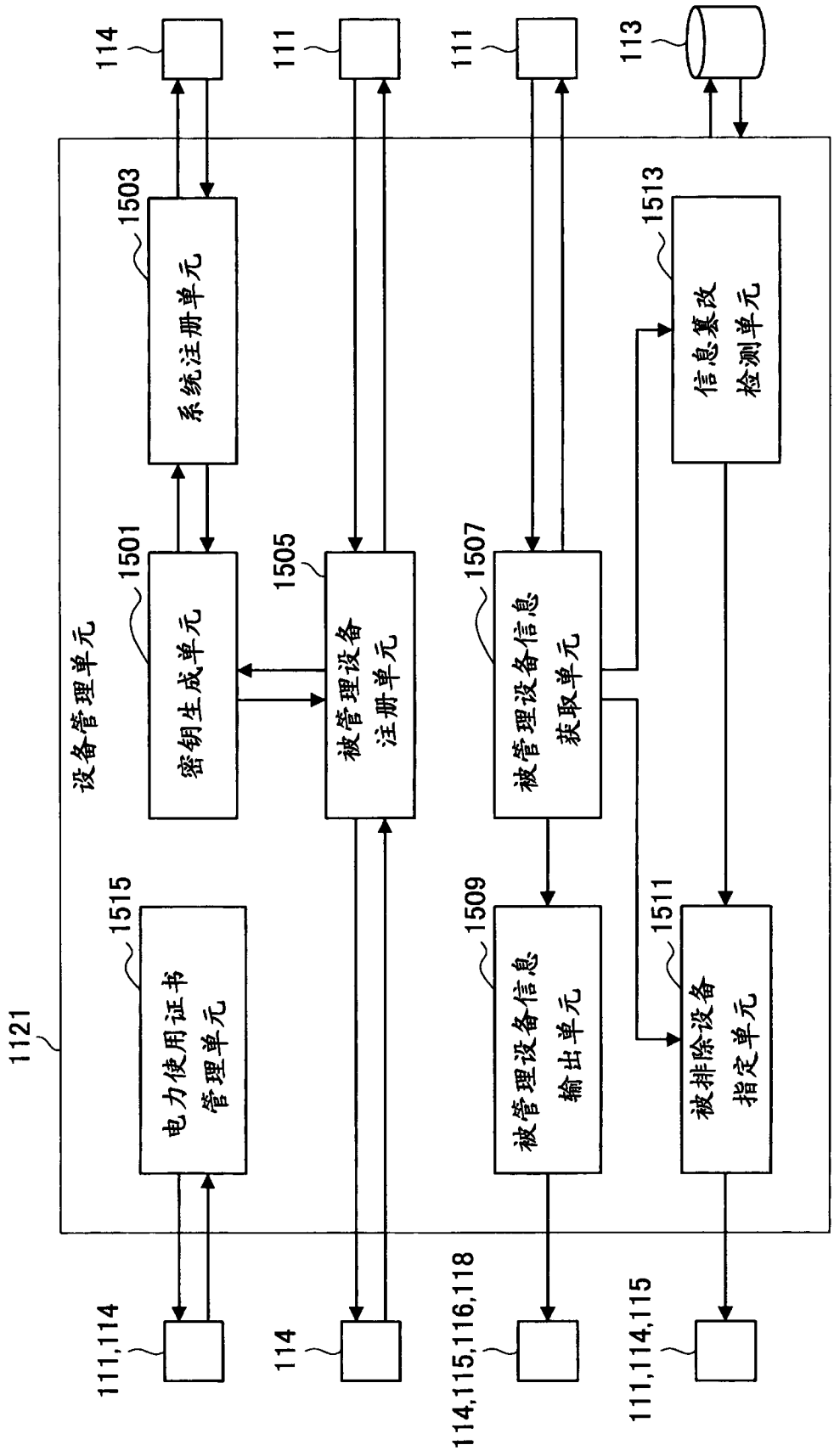

114
111
111
113
1503
系统注册单元
1513
信息篡改
检测单元
1501
密钥生成单元
1505
被管理设备
注册单元
1507
被管理设备信息
获取单元
设备管理单元
1515
电力使用证书
管理单元
1509
被管理设备信息
输出单元
1511
被排除设备
指定单元
1121
111,114
114
114,115,116,118
111,114,115

图 22

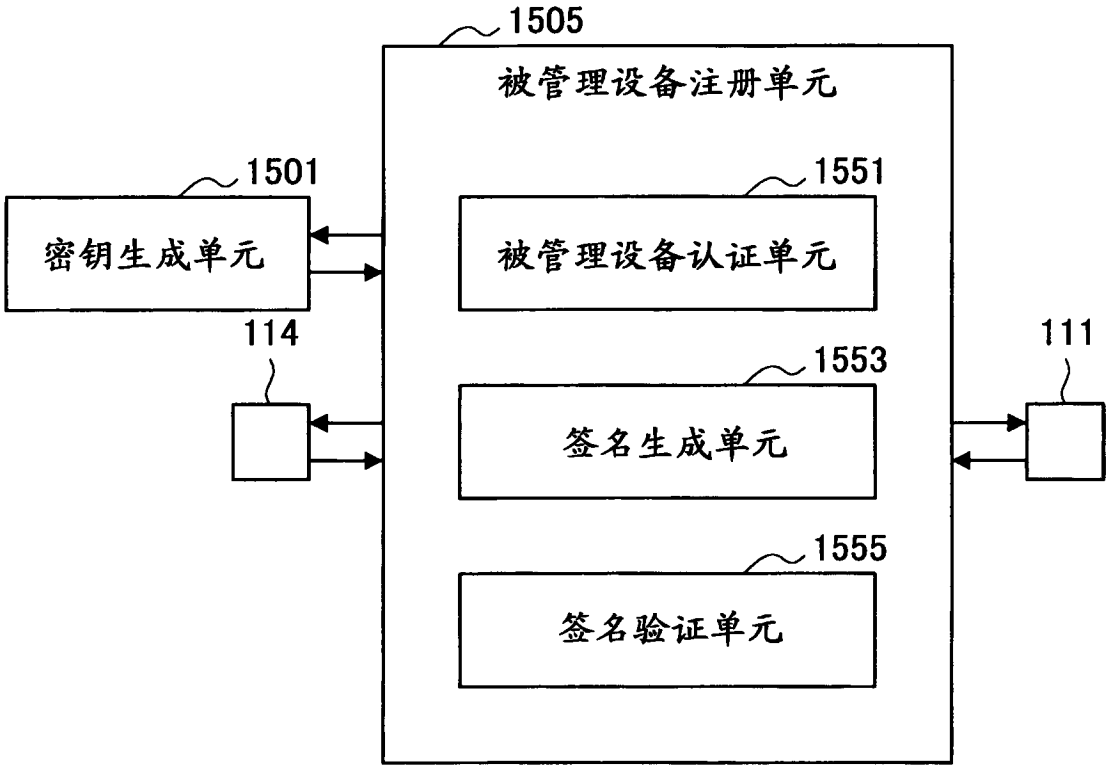

1505
被管理设备注册单元
1501
密钥生成单元
1551
被管理设备认证单元
114
1553
签名生成单元
111
1555
签名验证单元

图 23

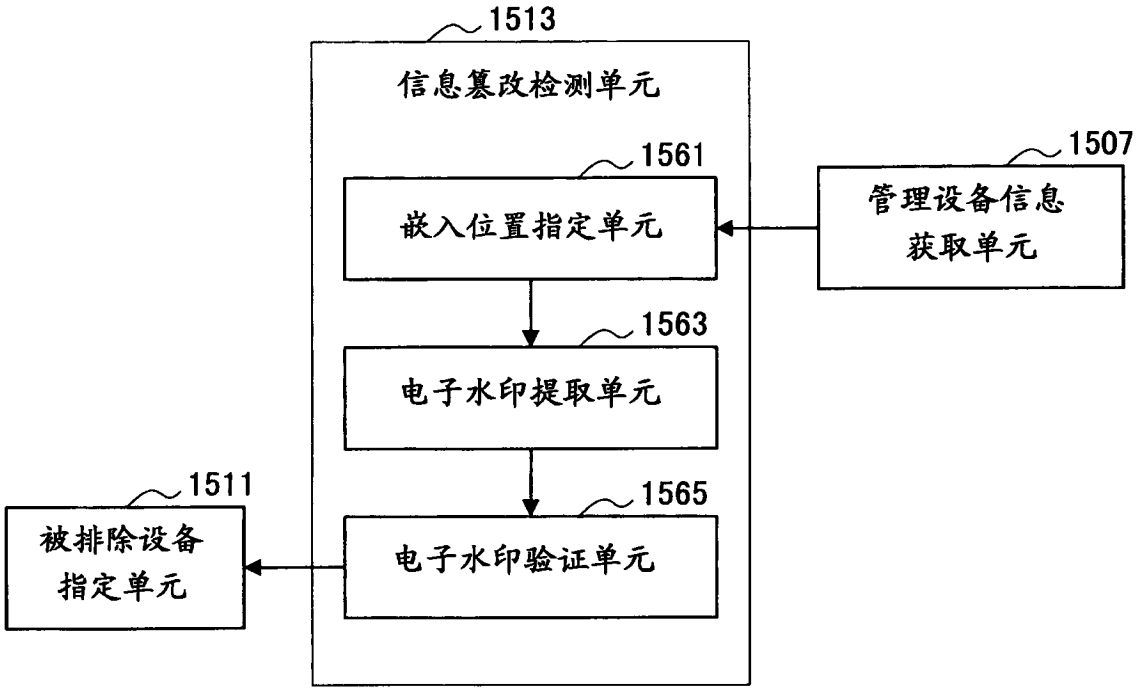

1513
信息篡改检测单元
1561
嵌入位置指定单元
1507
管理设备信息
获取单元
1563
电子水印提取单元
1511
被排除设备
指定单元
1565
电子水印验证单元

图 24

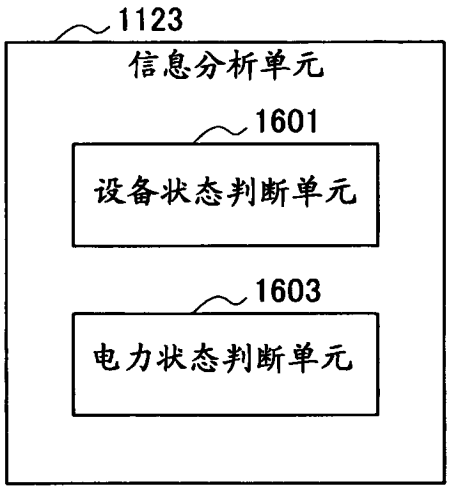


图 25

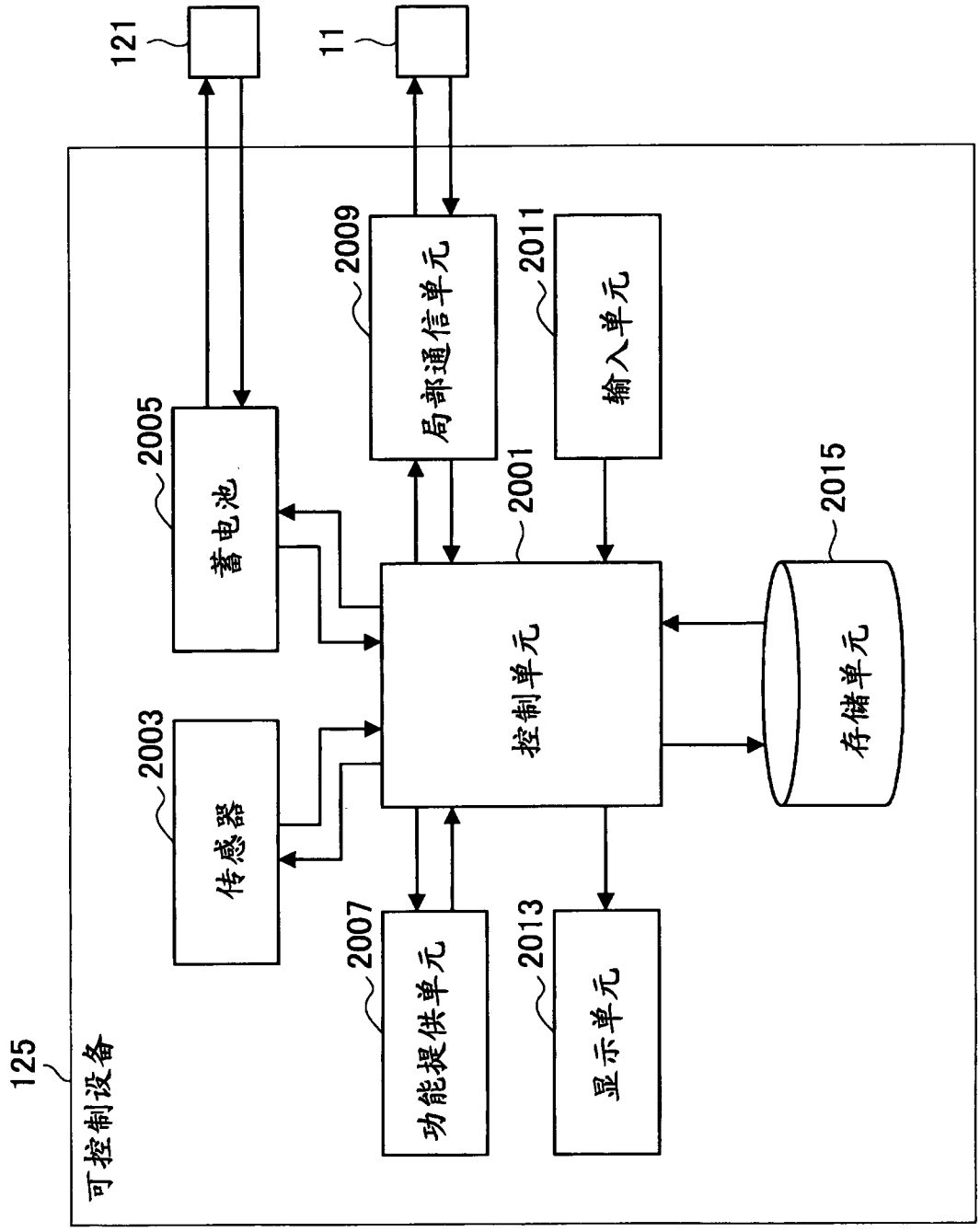

121
11
2009
局部通信单元
2011
输入单元
2005
蓄电池
2001
控制单元
2015
存储单元
2003
传感器
2007
功能提供单元
2013
显示单元
125
可控制设备

图 26

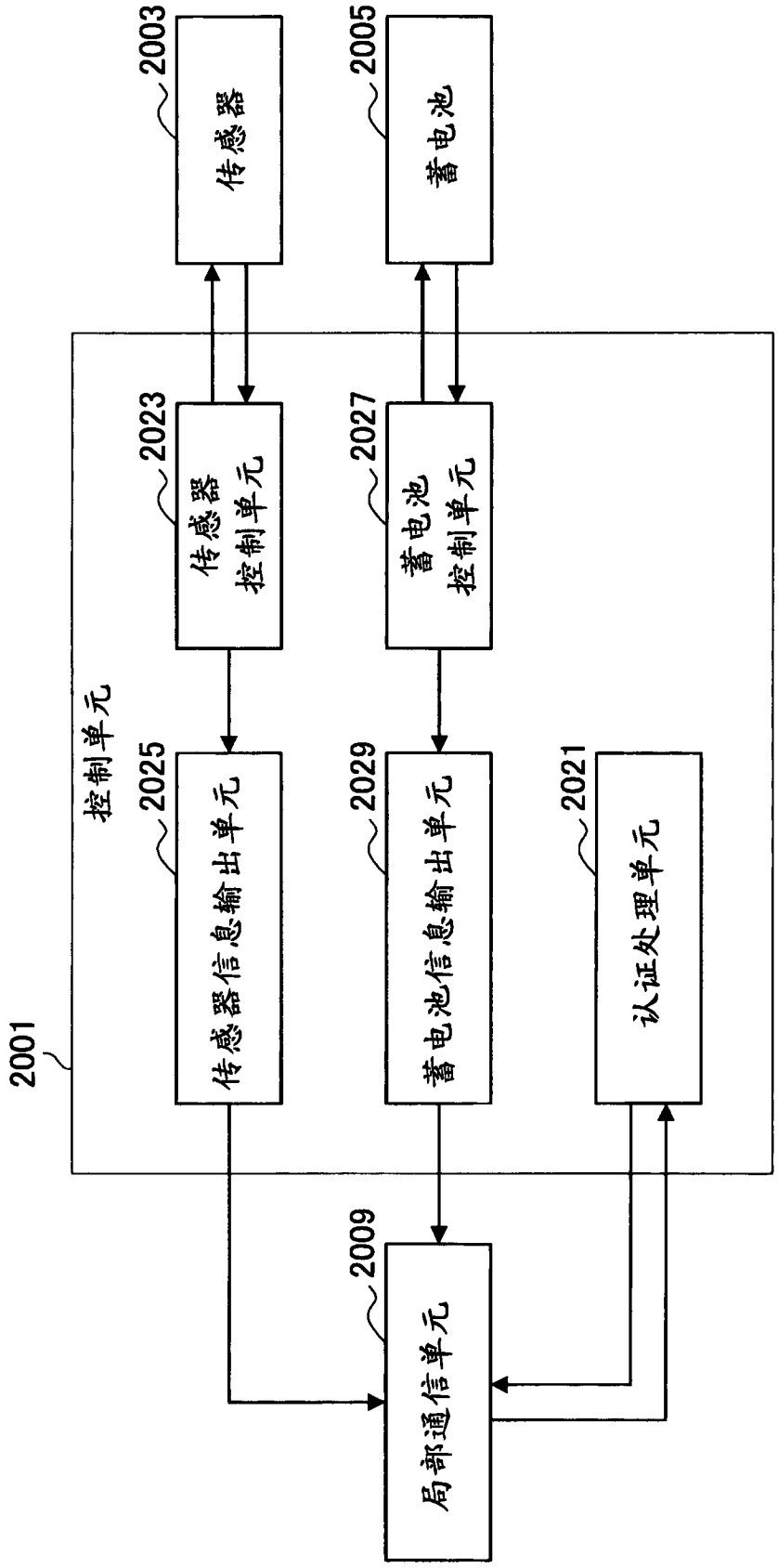

2003
传感器
2005
蓄电池
2023
传感器控制单元
2027
蓄电池控制单元
控制单元
2025
传感器信息输出单元
2029
蓄电池信息输出单元
2021
认证处理单元
2001
2009
局部通信单元

图 27

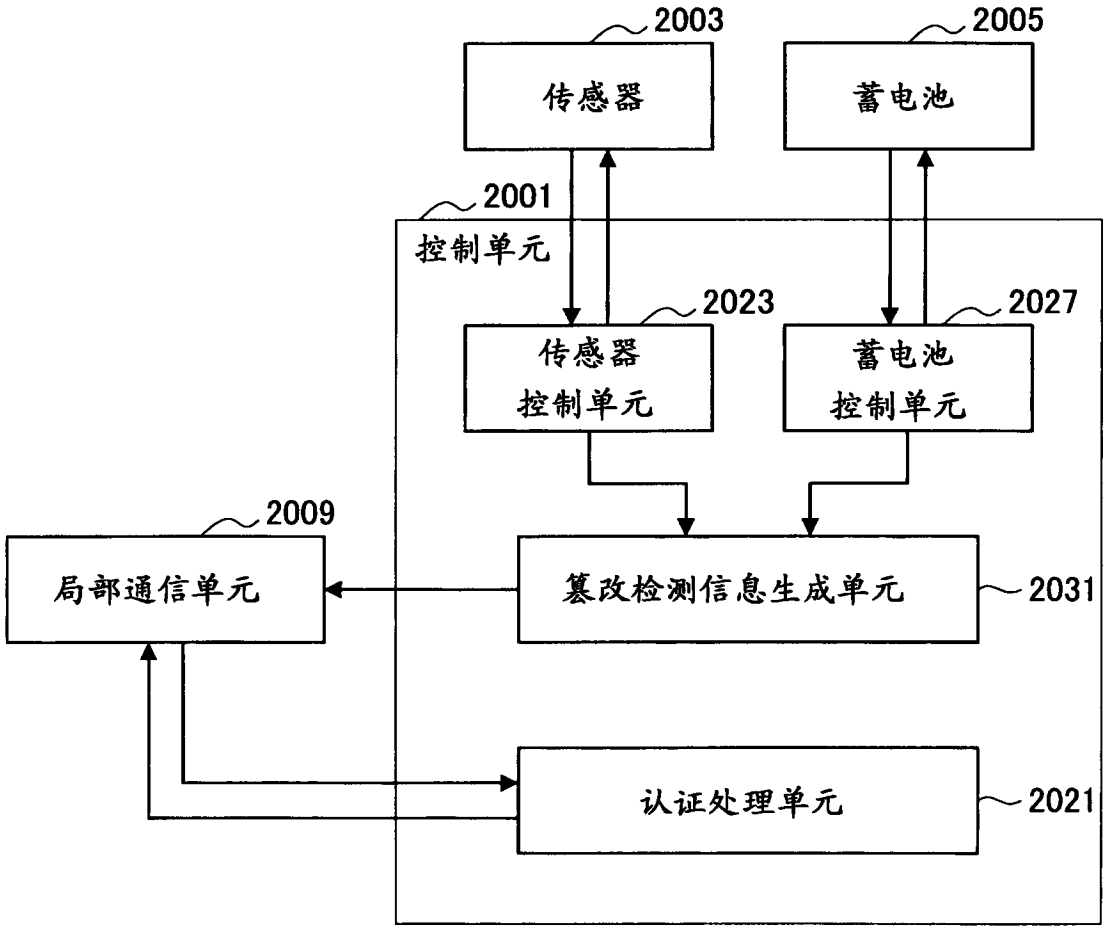

2003
传感器
2005
蓄电池
2001
控制单元
2023
传感器
控制单元
2027
蓄电池
控制单元
2009
局部通信单元
篡改检测信息生成单元
2031
认证处理单元
2021

图 28

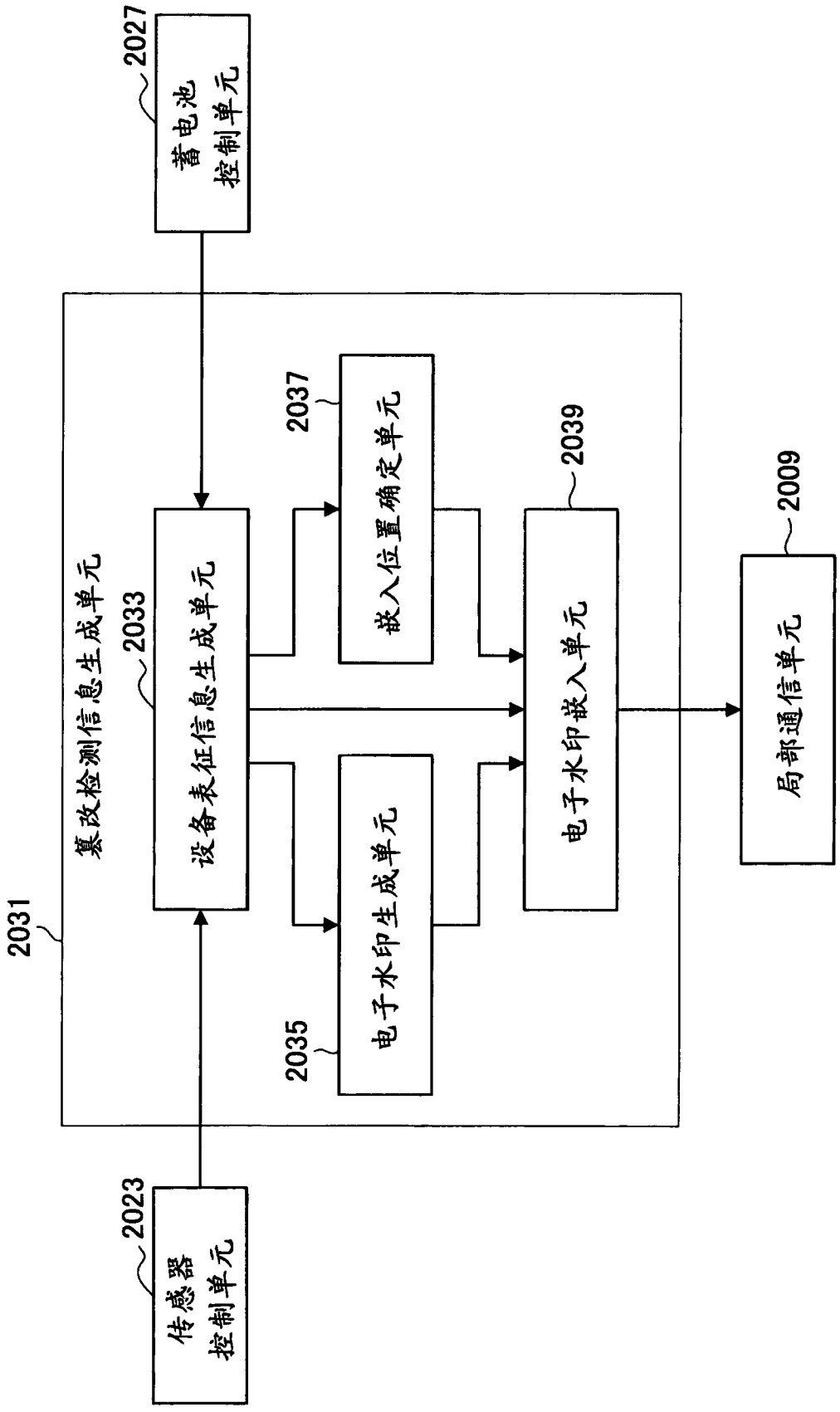

2027
蓄电池控制单元
篡改检测信息生成单元
2031
2033
设备表征信息生成单元
2037
嵌入位置确定单元
2039
电子水印嵌入单元
2009
局部通信单元
2035
电子水印生成单元
2023
传感器控制单元

图 29

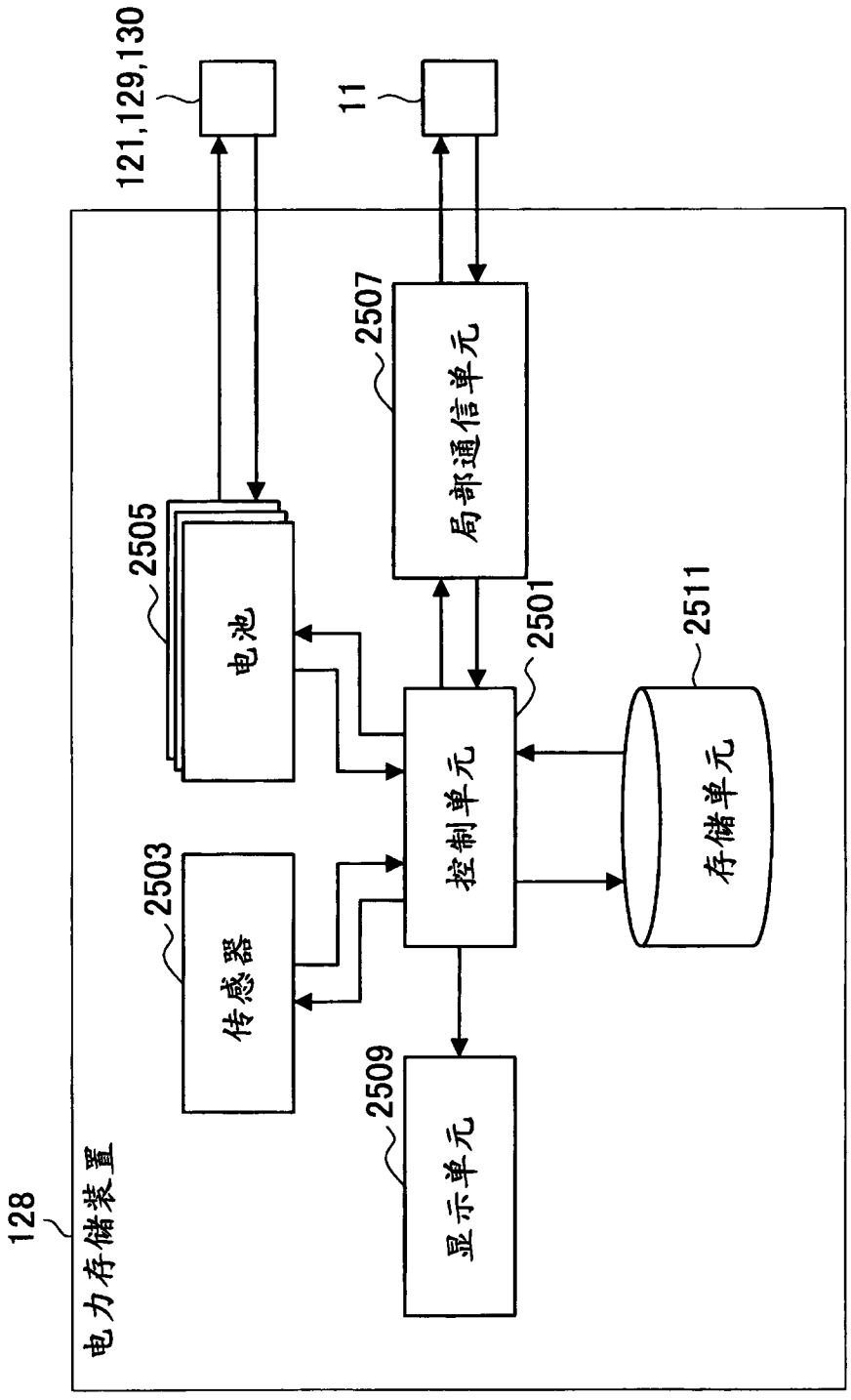

121,129,130
11
2507
局部通信单元
2505
电池
2501
2511
控制单元
存储单元
2503
传感器
2509
显示单元
128
电力存储装置

图 30

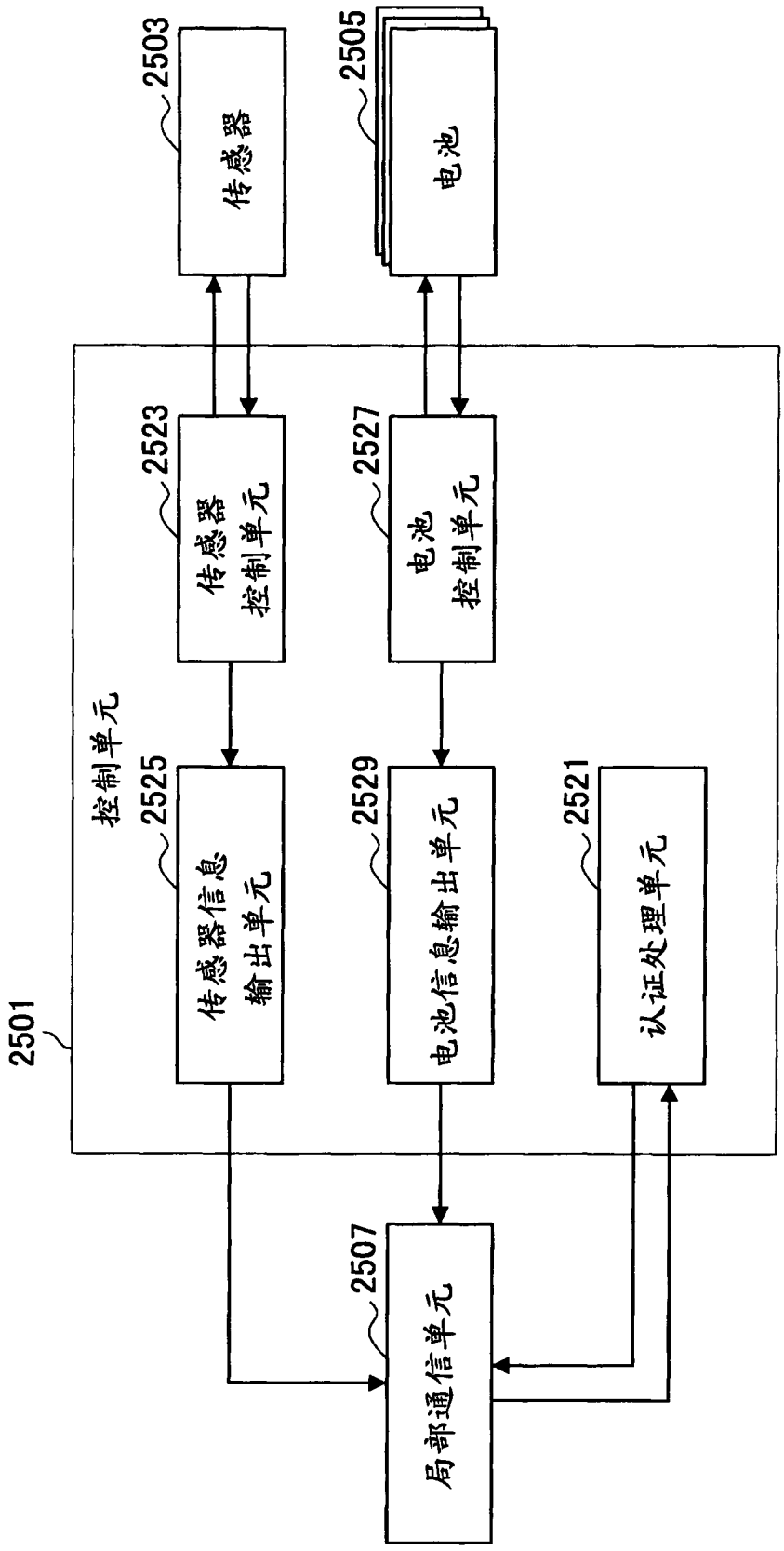

2503
传感器
2505
电池
2523
传感器控制单元
2527
电池控制单元
控制单元
2525
传感器信息输出单元
2529
电池信息输出单元
2521
认证处理单元
2501
2507
局部通信单元

图 31

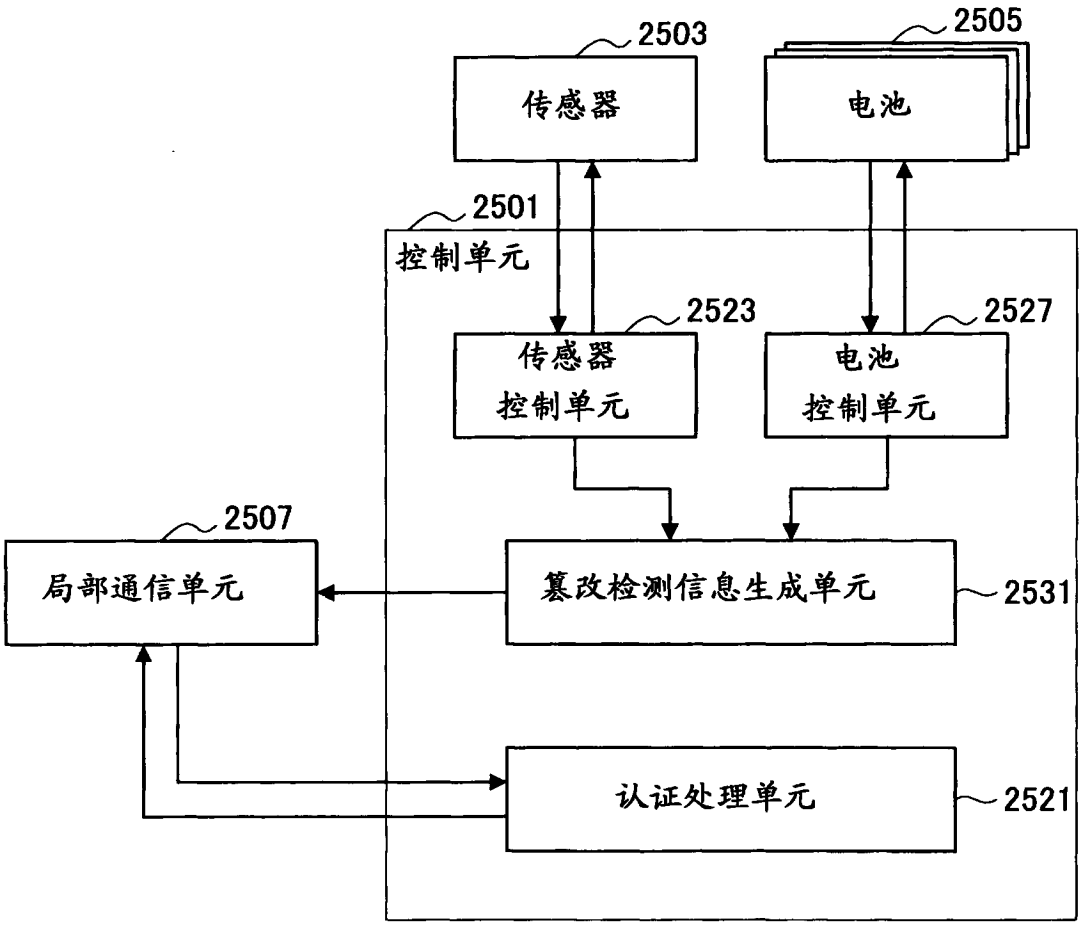

2503
传感器
2505
电池
2501
控制单元
2523
传感器
控制单元
2527
电池
控制单元
2507
局部通信单元
篡改检测信息生成单元
2531
认证处理单元
2521

图 32

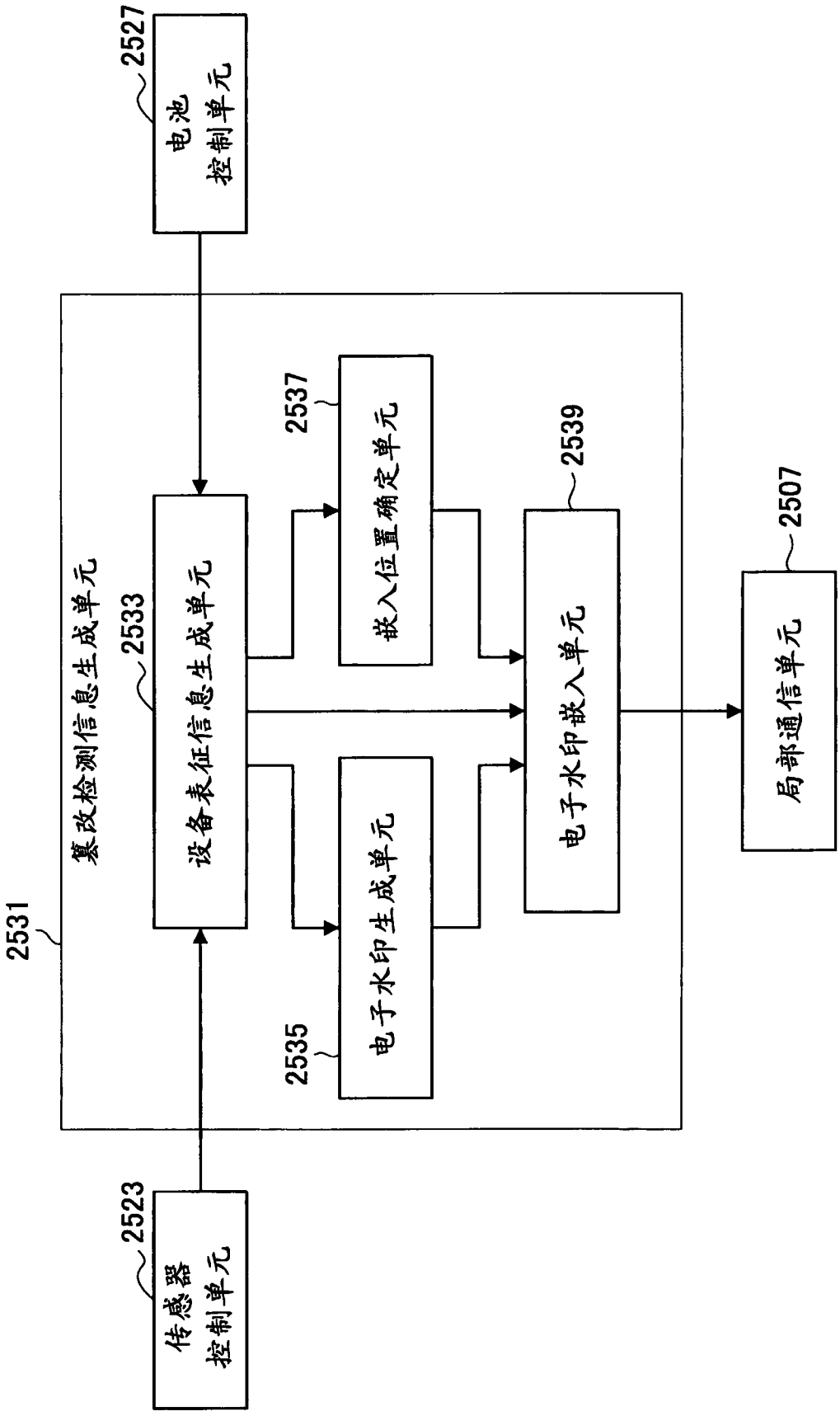

2527
电池
控制单元
2531
篡改检测信息生成单元
2533
设备表征信息生成单元
2537
嵌入位置确定单元
2539
电子水印嵌入单元
2507
局部通信单元
2535
电子水印生成单元
2523
传感器
控制单元

图 33

(电力管理装置的注册)

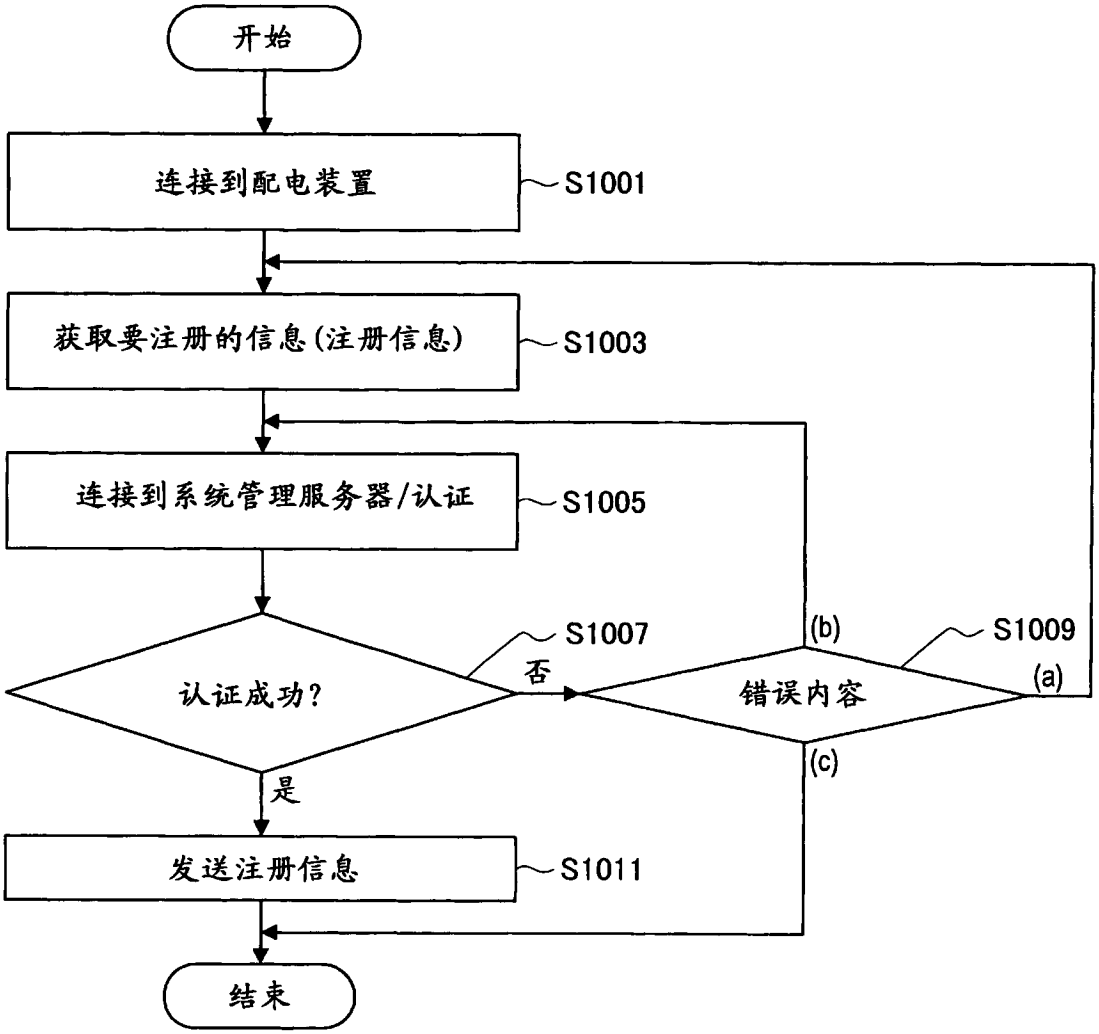


图 34

(通过系统管理服务器进行的处理的示例)

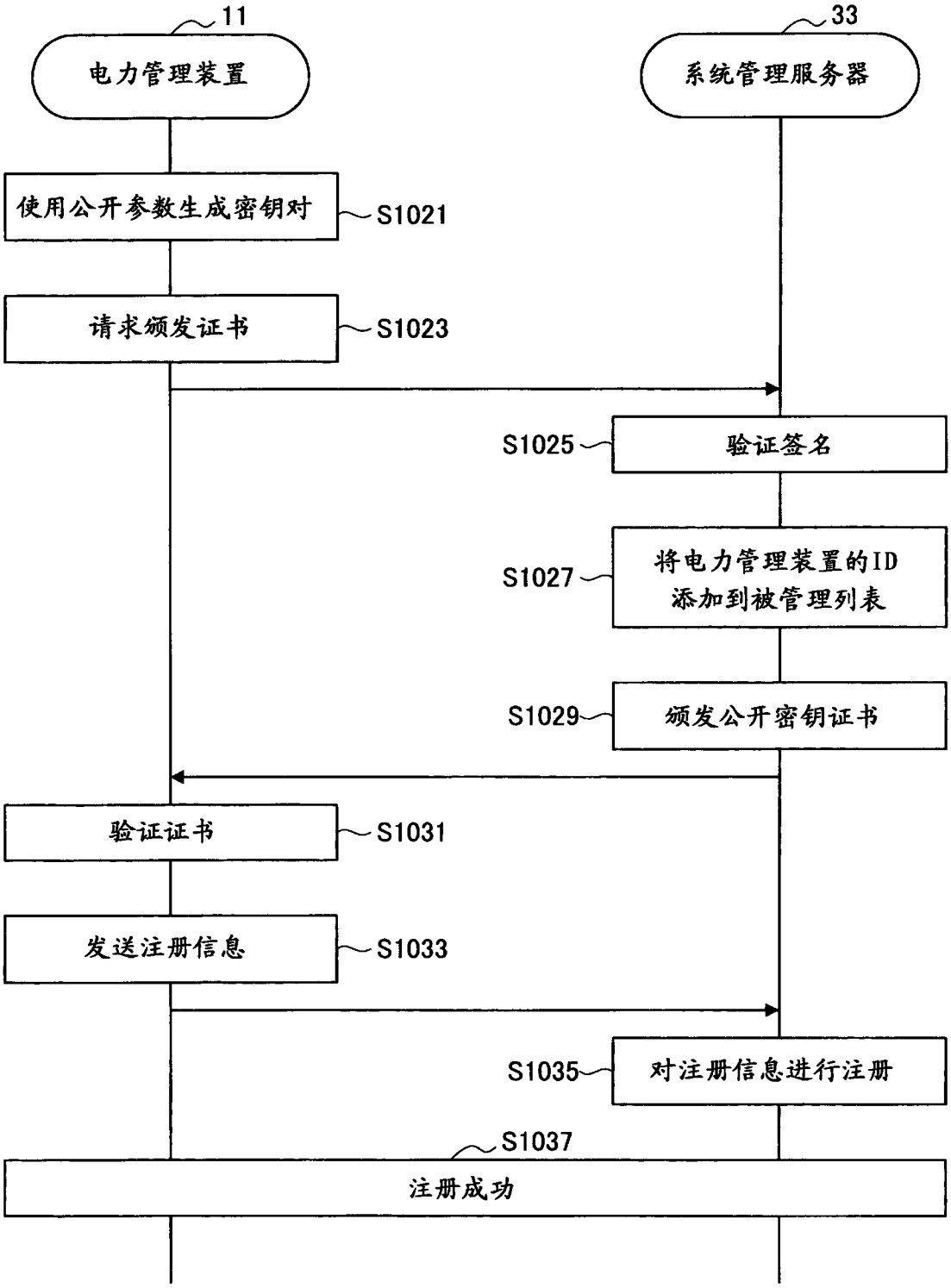


图 35

(可控制设备的注册)

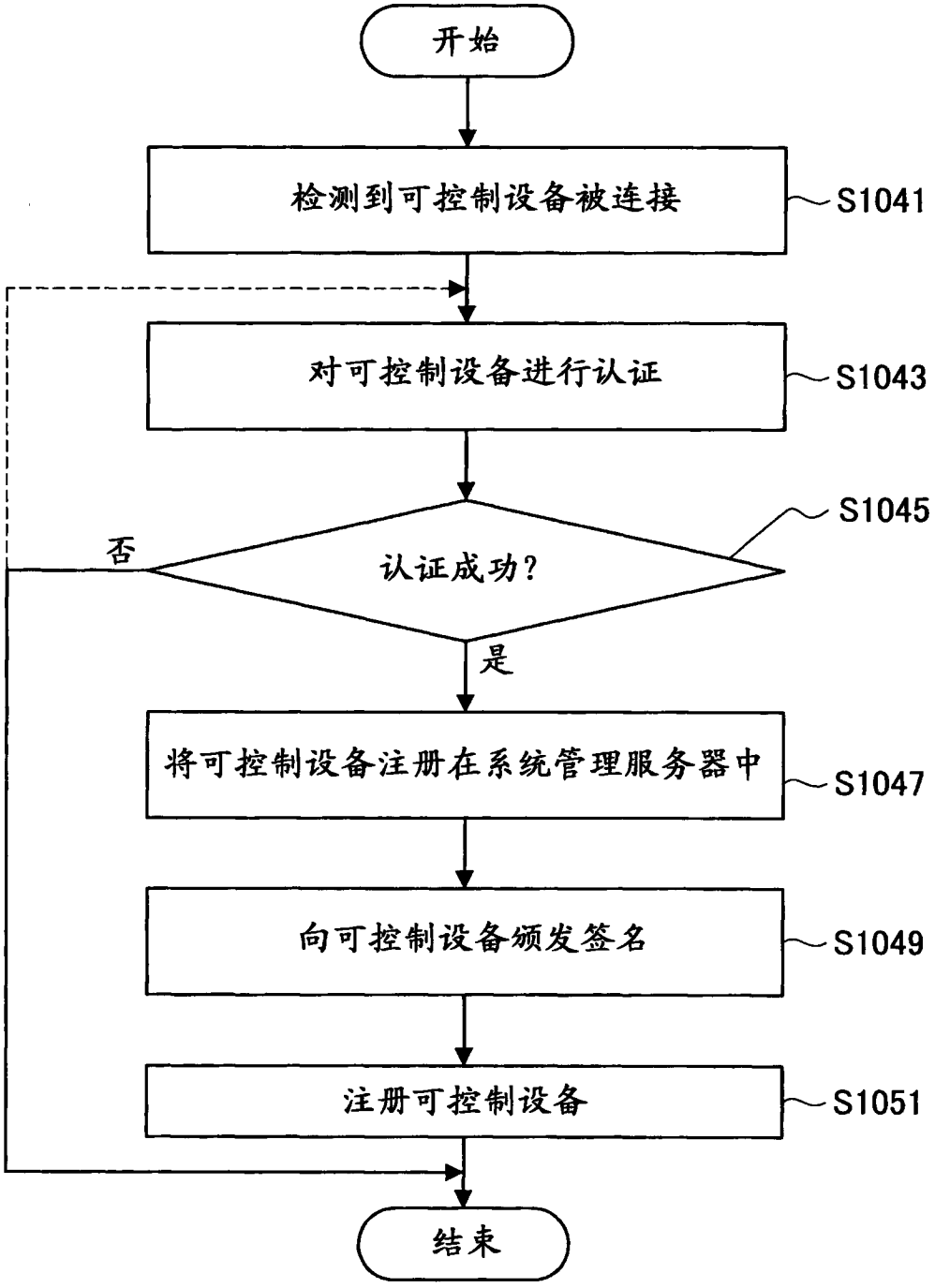


图 36

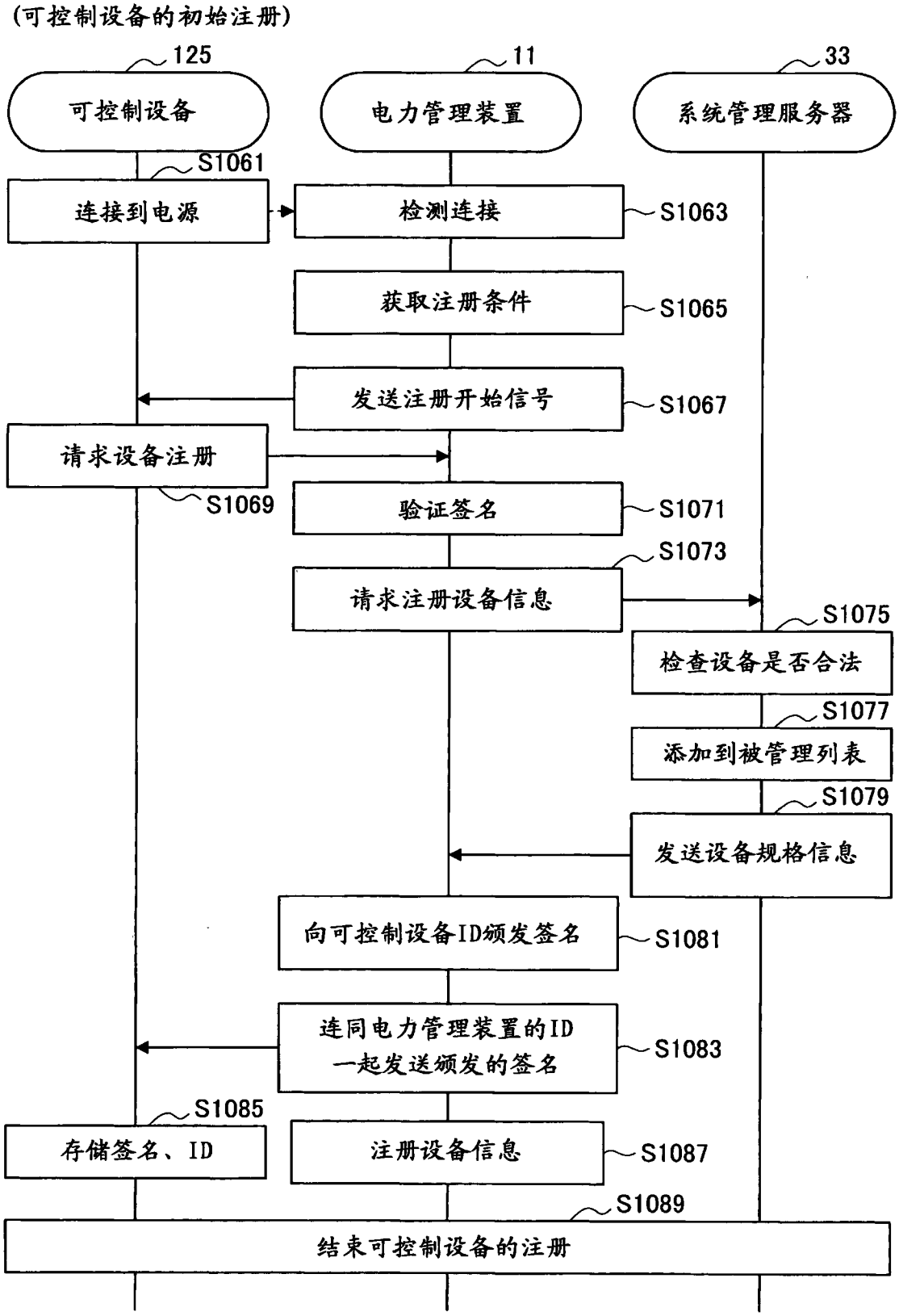

(可控制设备的初始注册)
125
11
33
可控制设备
电力管理装置
系统管理服务器
S1061
连接到电源
检测连接
S1063
获取注册条件
S1065
发送注册开始信号
S1067
请求设备注册
S1069
验证签名
S1071
S1073
请求注册设备信息
S1075
检查设备是否合法
S1077
添加到被管理列表
S1079
发送设备规格信息
向可控制设备ID颁发签名
S1081
连同电力管理装置的ID
一起发送颁发的签名
S1083
S1085
存储签名、ID
注册设备信息
S1087
S1089
结束可控制设备的注册

图 37

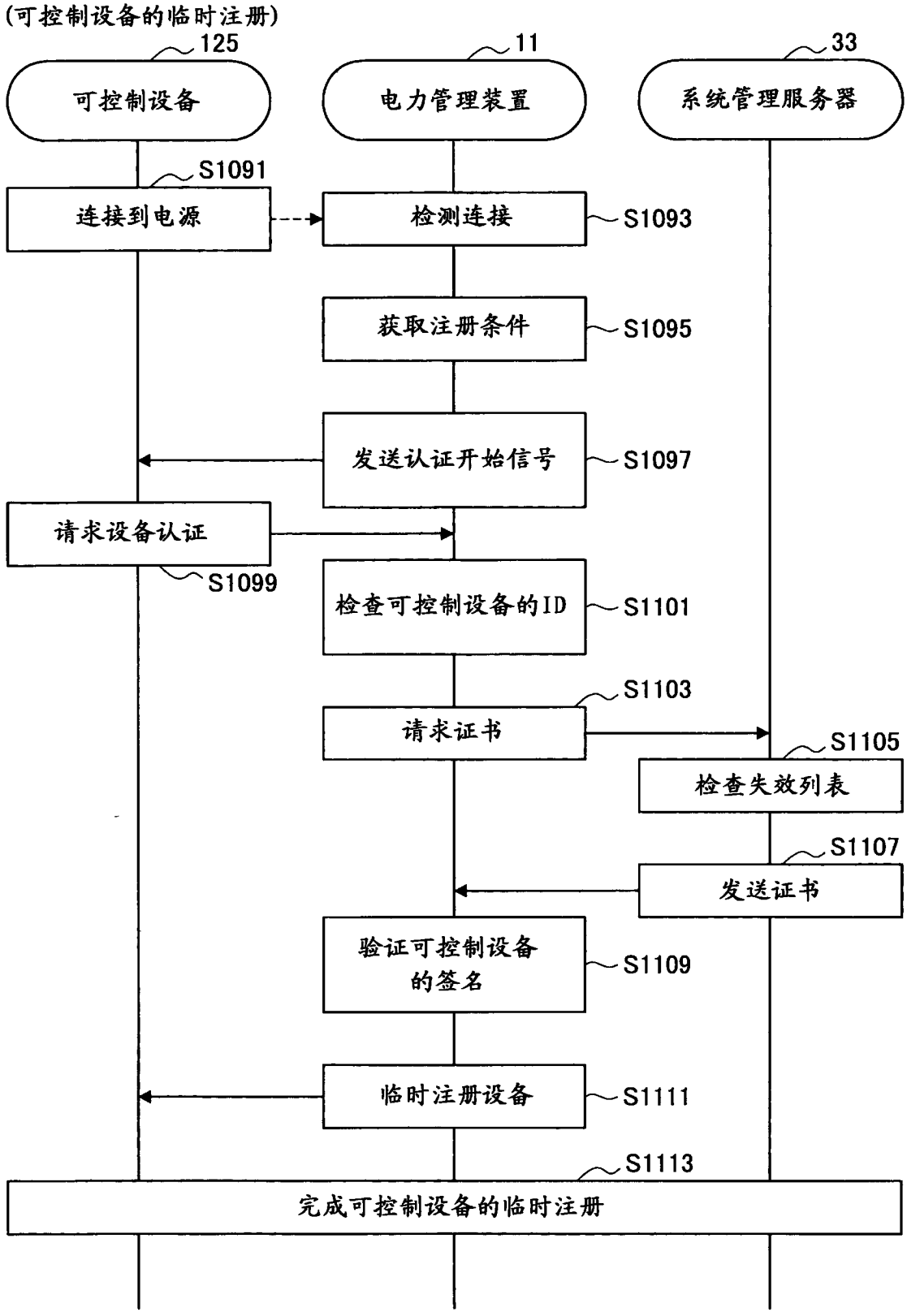

(可控制设备的临时注册)
125
可控制设备
11
电力管理装置
33
系统管理服务器
S1091
连接到电源
检测连接
S1093
获取注册条件
S1095
发送认证开始信号
S1097
请求设备认证
S1099
检查可控制设备的ID
S1101
S1103
请求证书
S1105
检查失效列表
S1107
发送证书
验证可控制设备的签名
S1109
临时注册设备
S1111
S1113
完成可控制设备的临时注册

图 38

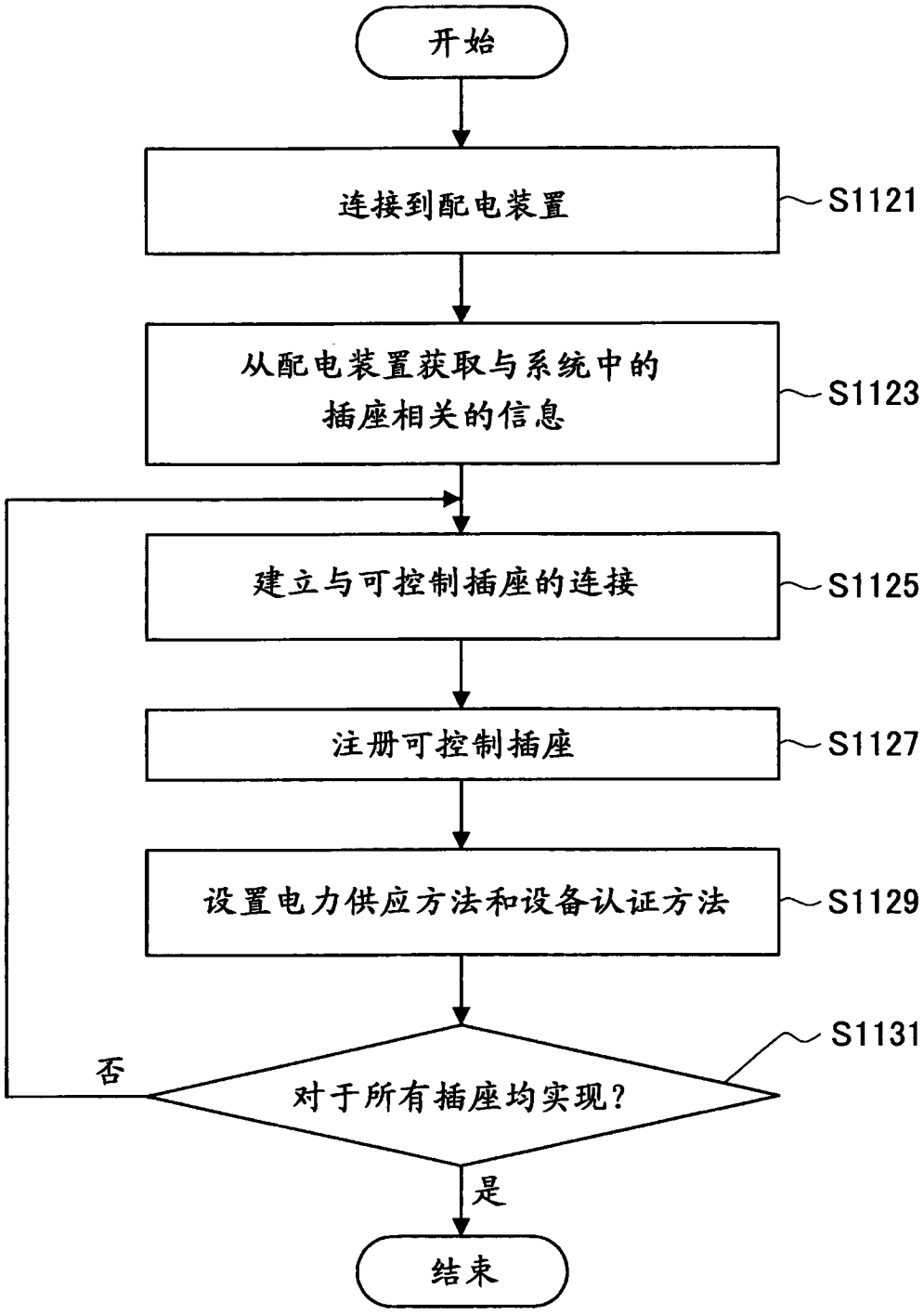

开始
连接到配电装置
S1121
从配电装置获取与系统中的
插座相关的信息
S1123
建立与可控制插座的连接
S1125
注册可控制插座
S1127
设置电力供应方法和设备认证方法
S1129
S1131
否
对于所有插座均实现?
是
结束

图 39

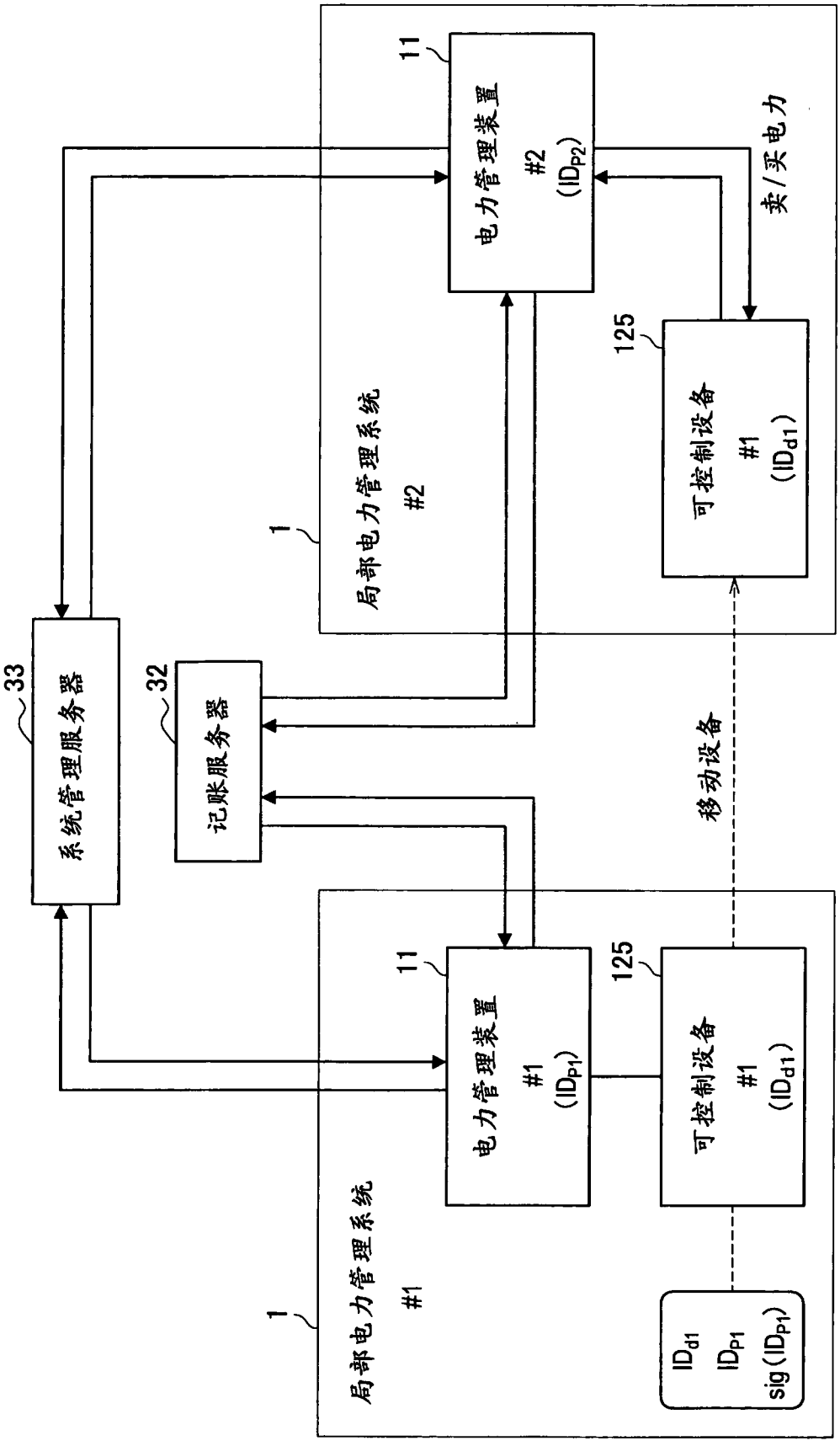

局部电力管理系统
#2
1
电力管理装置
#2
(ID_{P2})
11
可控制设备
#1
(ID_{d1})
125
卖/买电力
系统管理服务器
33
记账服务器
32
移动设备
局部电力管理系统
#1
1
电力管理装置
#1
(ID_{P1})
11
可控制设备
#1
(ID_{d1})
125
ID_{d1}
ID_{P1}
sig(ID_{P1})

图 40

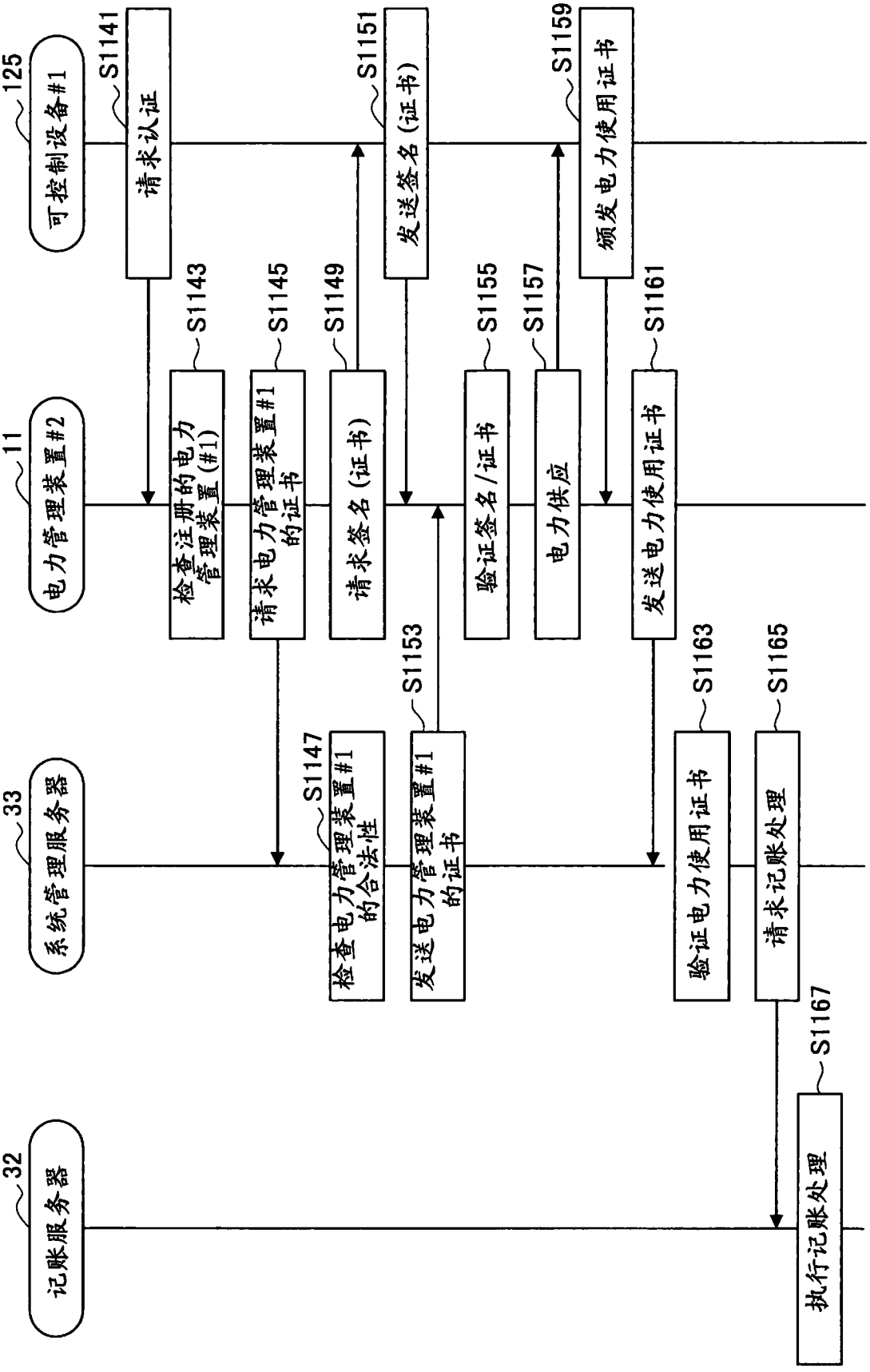

125
可控制设备#1
S1141
请求认证
S1151
发送签名(证书)
S1159
颁发电力使用证书
11
电力管理装置#2
S1143
检查注册的电力管理装置(#1)
S1145
请求电力管理装置#1的证书
S1149
请求签名(证书)
S1155
验证签名/证书
S1157
电力供应
S1161
发送电力使用证书
33
系统管理服务器
S1147
检查电力管理装置#1的合法性
S1153
发送电力管理装置#1的证书
S1163
验证电力使用证书
S1165
请求记账处理
S1167
执行记账处理
32
记账服务器

图 41

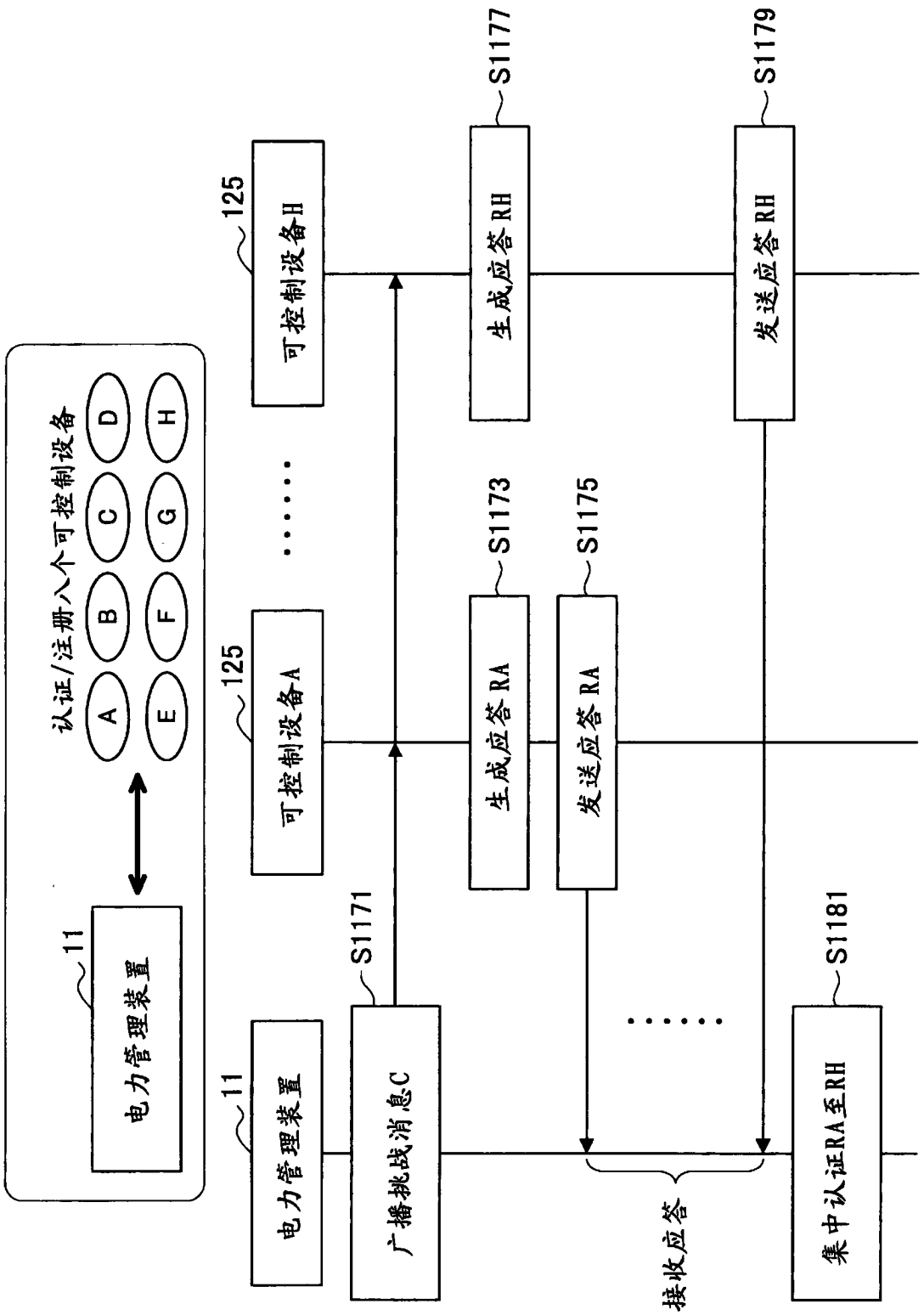

认证/注册八个可控制设备
A
B
C
D
E
F
G
H
11
电力管理装置
11
电力管理装置
S1171
广播挑战消息C
125
可控制设备A
S1173
生成应答 RA
S1175
发送应答 RA
125
可控制设备H
S1177
生成应答 RH
S1179
发送应答 RH
S1181
集中认证RA至RH
接收应答

图 42

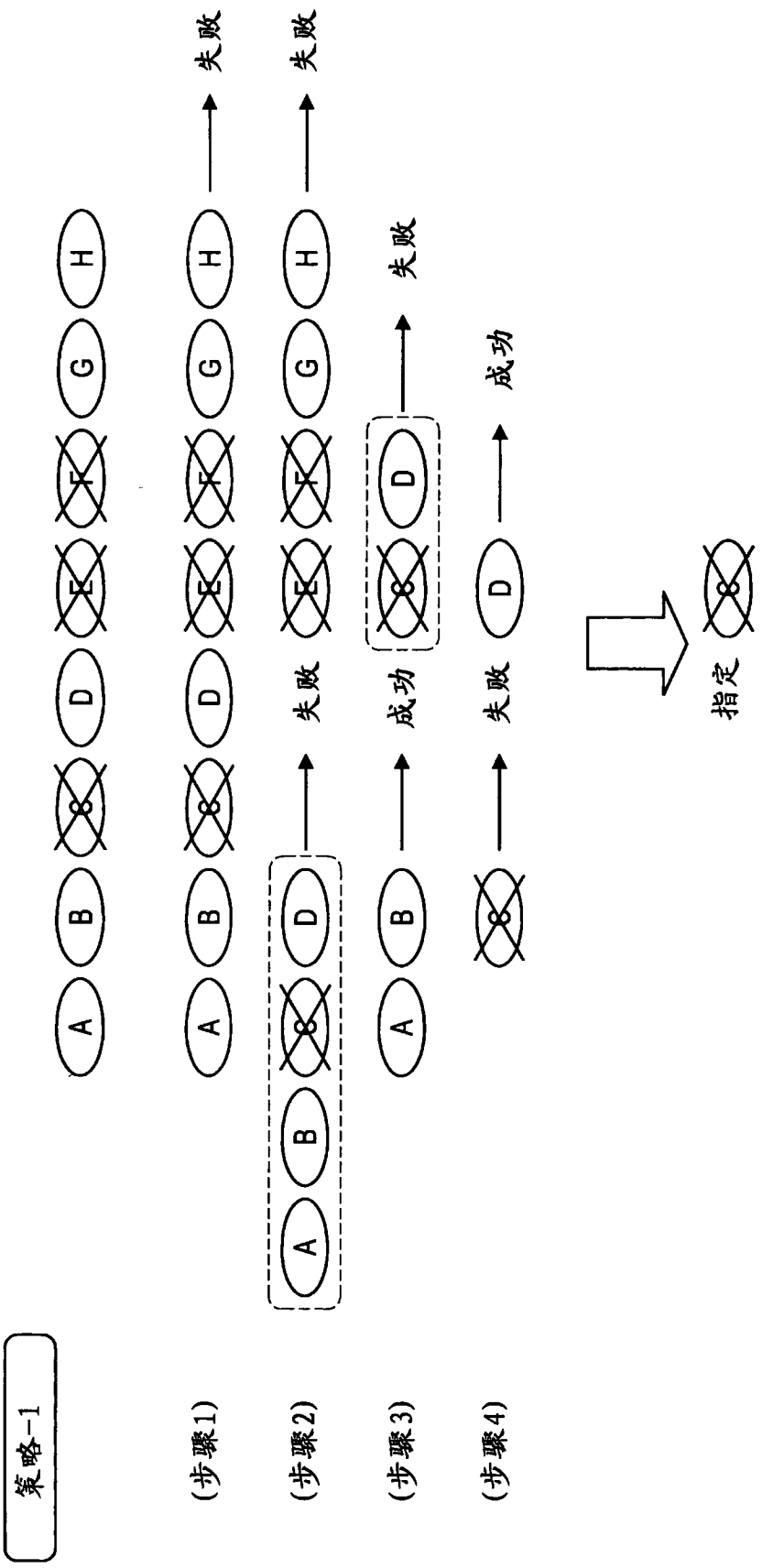


图 43

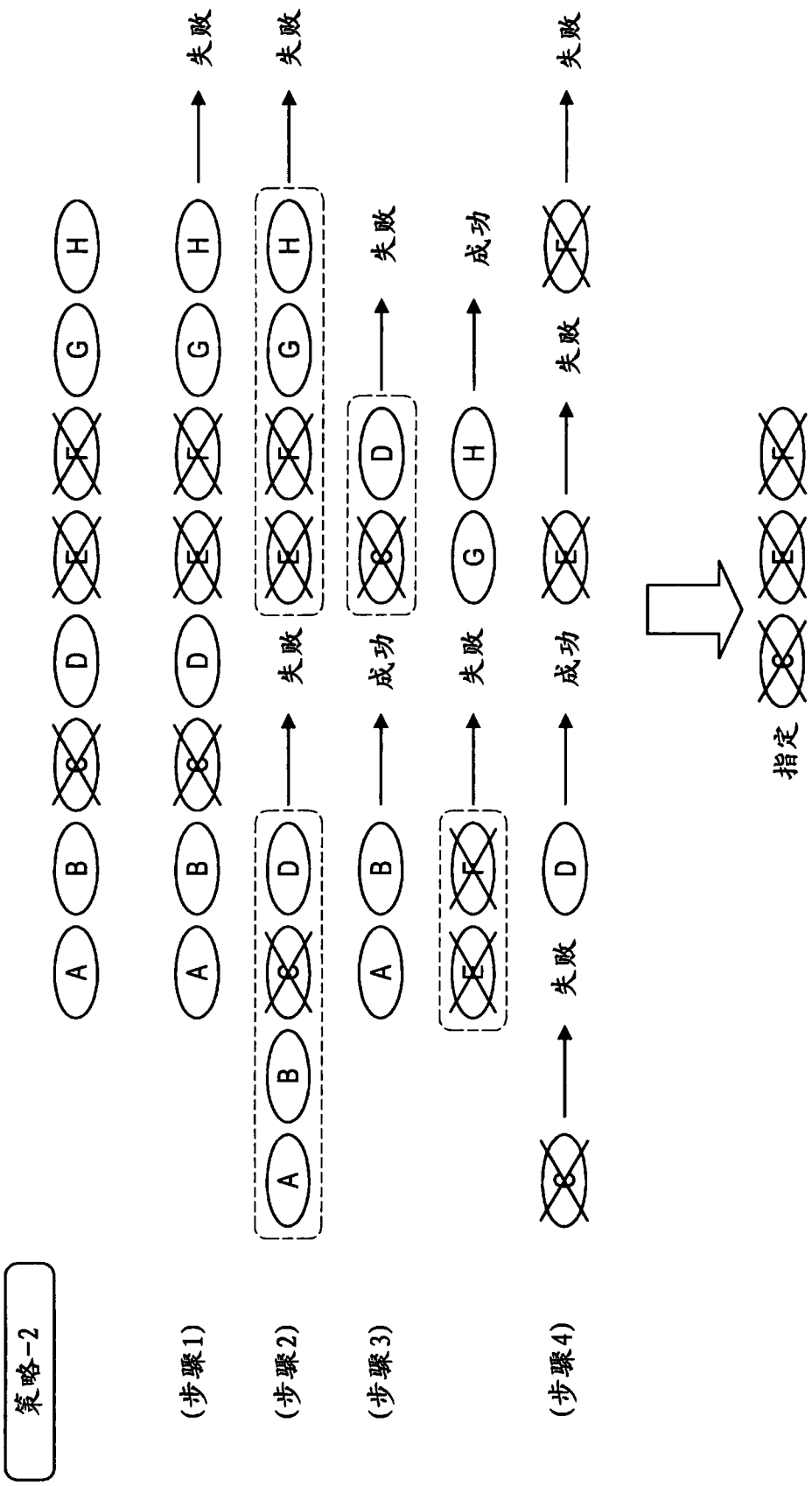


图 44

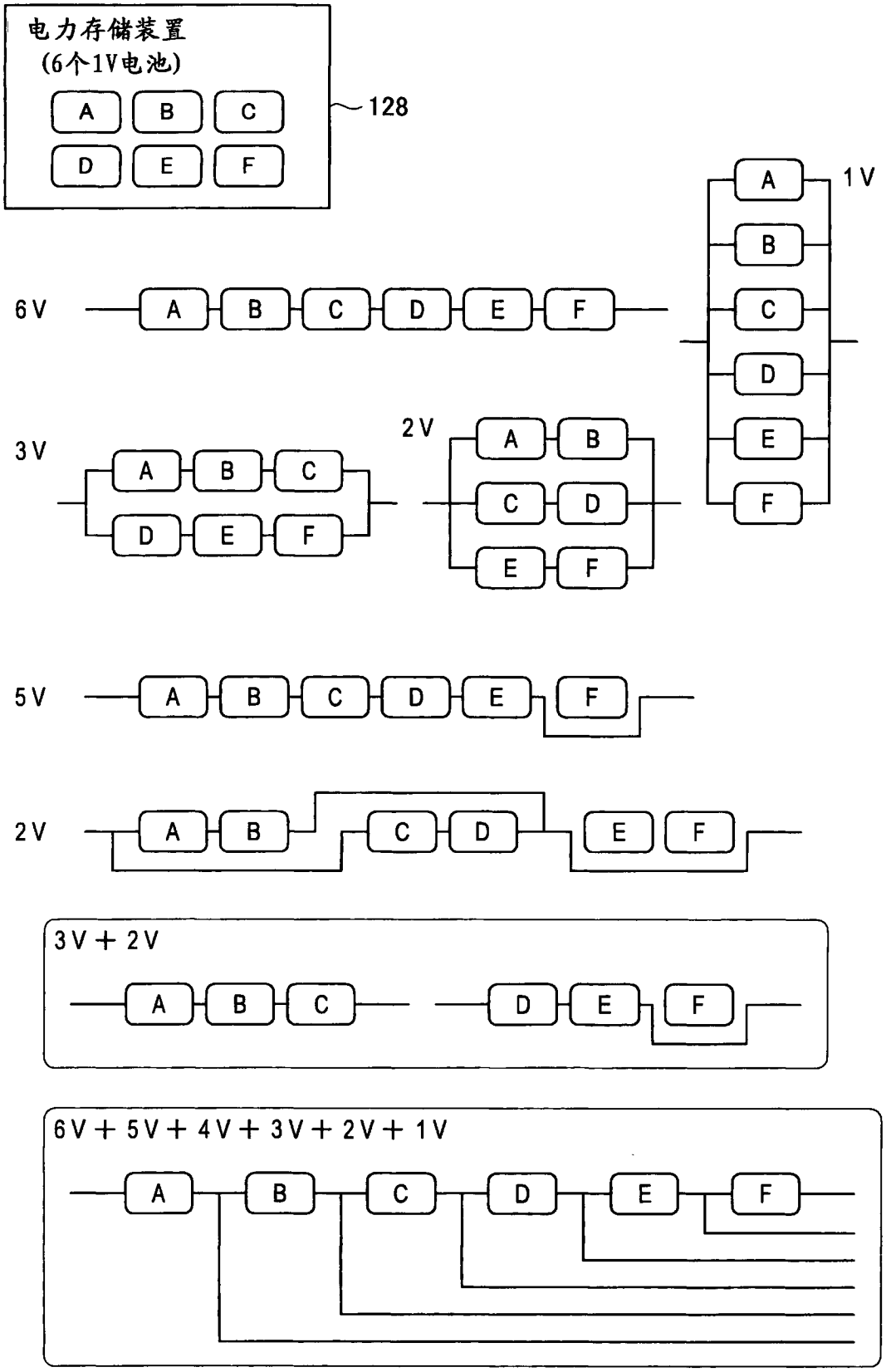


图 45

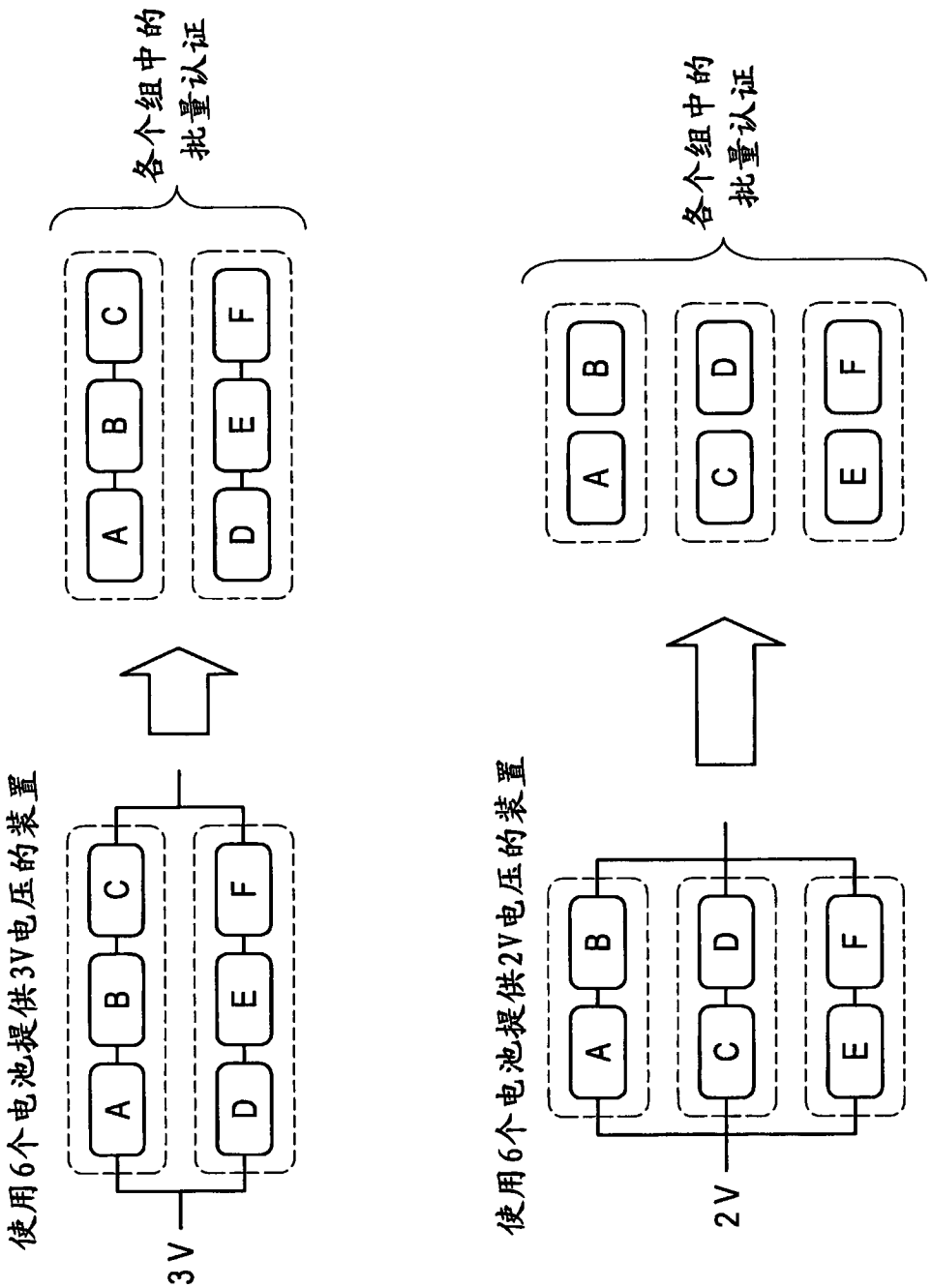

使用6个电池提供3V电压的装置
3V
A
B
C
D
E
F
各个组中的批量认证
使用6个电池提供2V电压的装置
2V
A
B
C
D
E
F
各个组中的批量认证

图 46

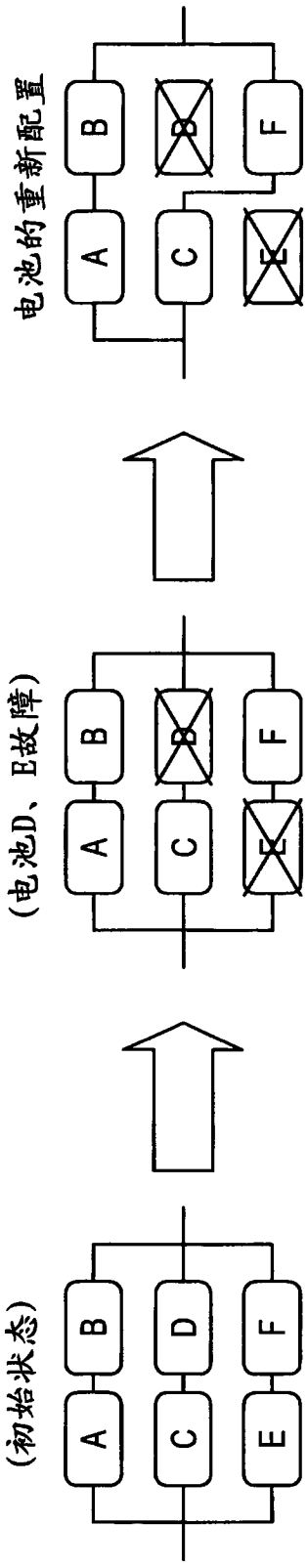


图 47

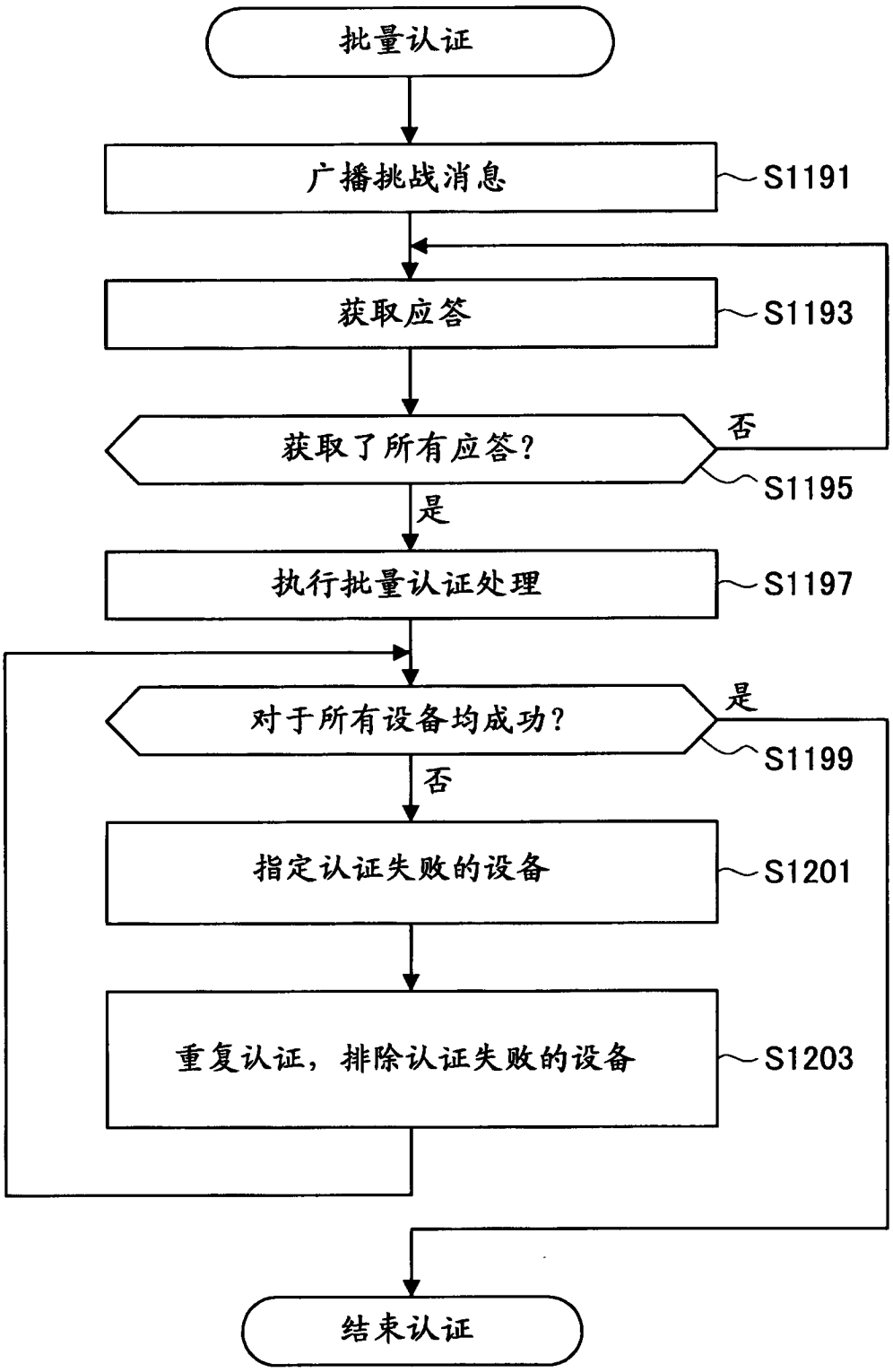

批量认证
广播挑战消息
S1191
获取应答
S1193
获取了所有应答?
否
S1195
是
执行批量认证处理
S1197
对于所有设备均成功?
是
S1199
否
指定认证失败的设备
S1201
重复认证，排除认证失败的设备
S1203
结束认证

图 48

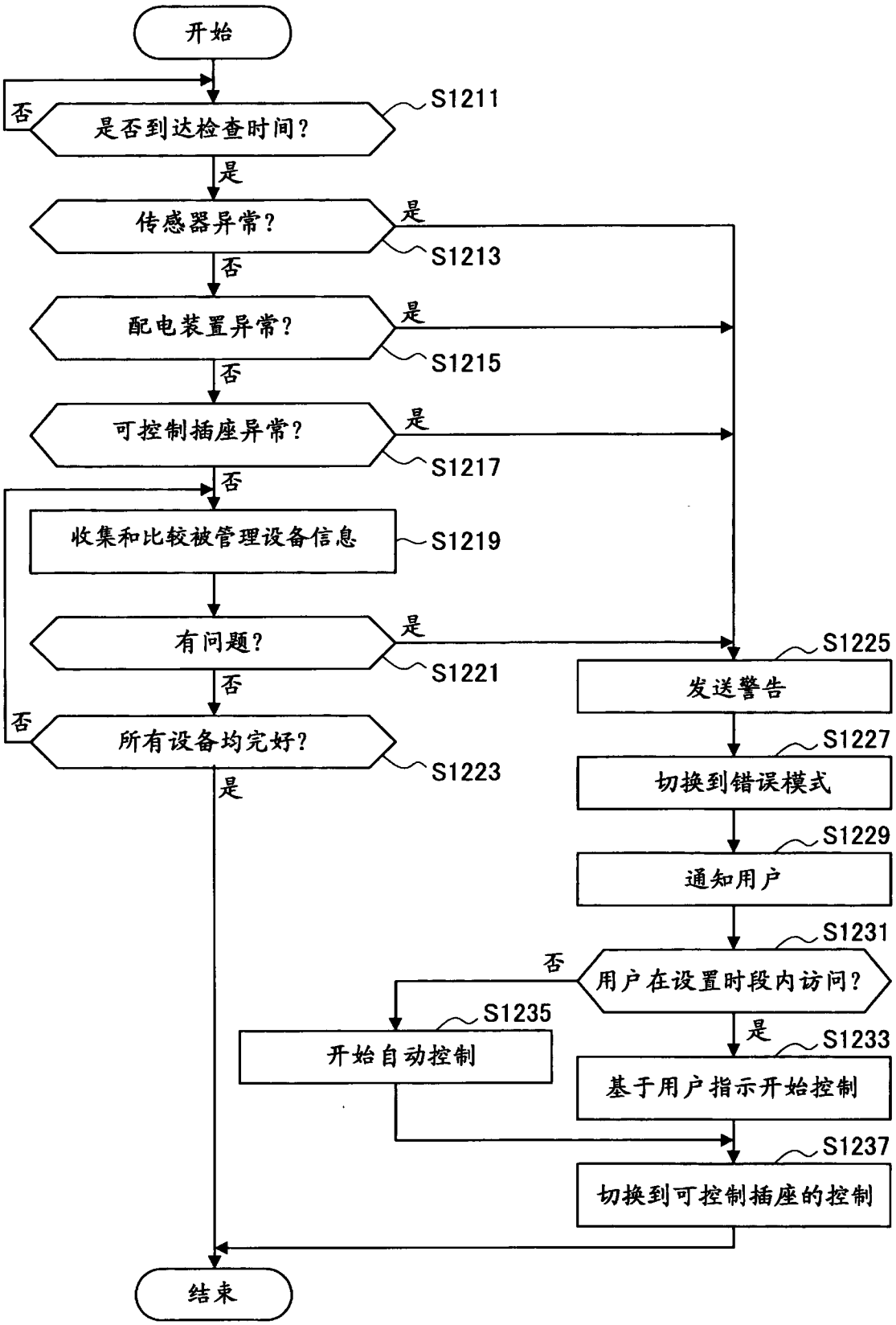

开始
是否到达检查时间？
S1211
否
是
传感器异常？
是
S1213
否
配电装置异常？
是
S1215
否
可控制插座异常？
是
S1217
否
收集和比较被管理设备信息
S1219
有问题？
是
S1221
否
所有设备均完好？
否
S1223
是
S1225
发送警告
S1227
切换到错误模式
S1229
通知用户
S1231
用户在设置时段内访问？
否
S1235
开始自动控制
是
S1233
基于用户指示开始控制
S1237
切换到可控制插座的控制
结束

图 49

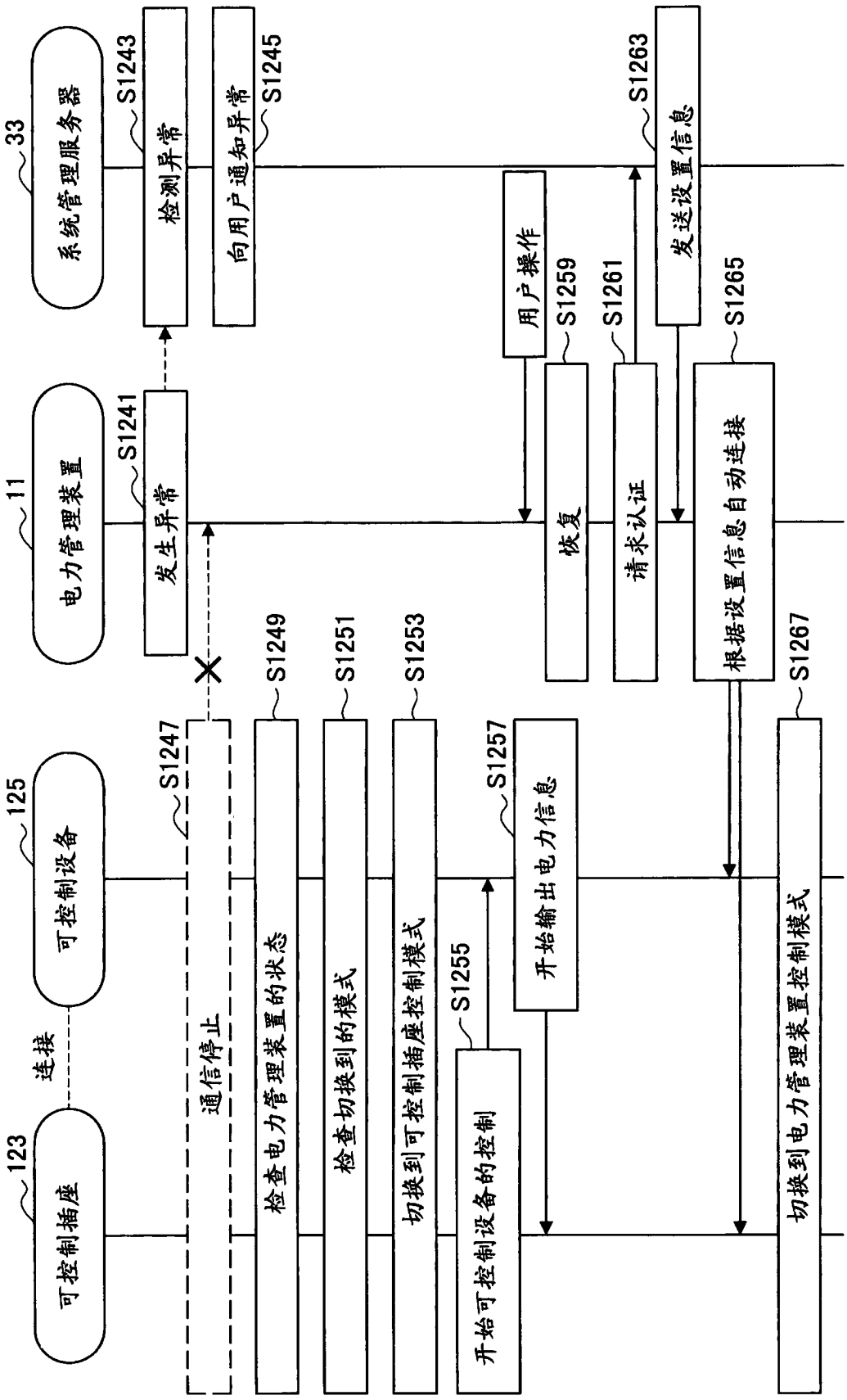

33
系统管理服务器
S1243
检测异常
S1245
向用户通知异常
S1263
发送设置信息
11
电力管理装置
S1241
发生异常
用户操作
S1259
S1261
请求认证
S1265
根据设置信息自动连接
恢复
125
可控制设备
S1247
通信停止
S1249
检查电力管理装置的状态
S1251
检查切换到的模式
S1253
切换到可控制插座控制模式
S1257
开始输出电力信息
S1267
切换到电力管理装置控制模式
连接
123
可控制插座
S1255
开始可控制设备的控制

图 50

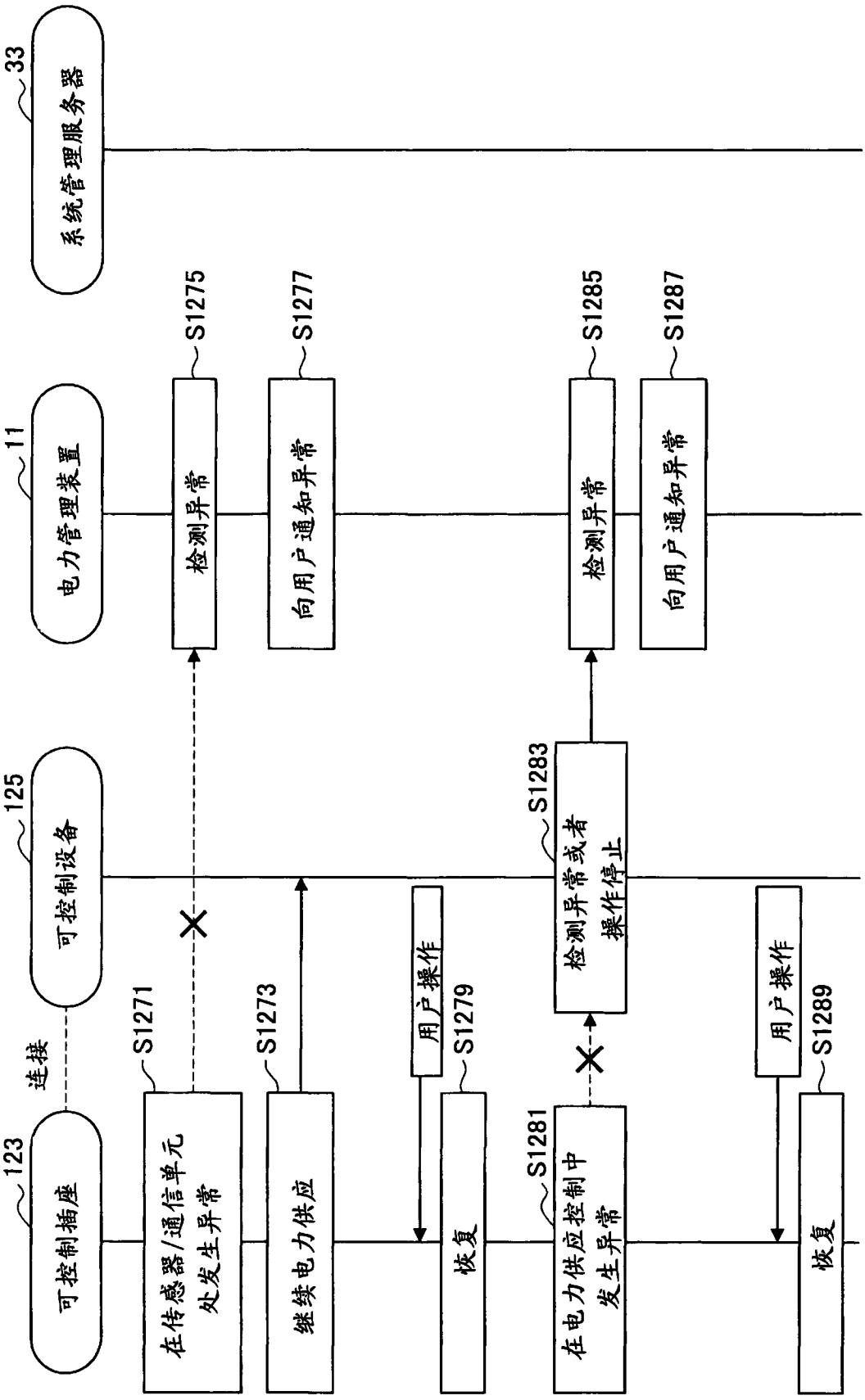

33
系统管理服务器
11
电力管理装置
125
可控制设备
123
可控制插座
连接
S1271
在传感器/通信单元处发生异常
S1273
继续电力供应
S1275
检测异常
S1277
向用户通知异常
用户操作
S1279
恢复
S1281
在电力供应控制中发生异常
S1283
检测异常或者操作停止
S1285
检测异常
S1287
向用户通知异常
用户操作
S1289
恢复

图 51

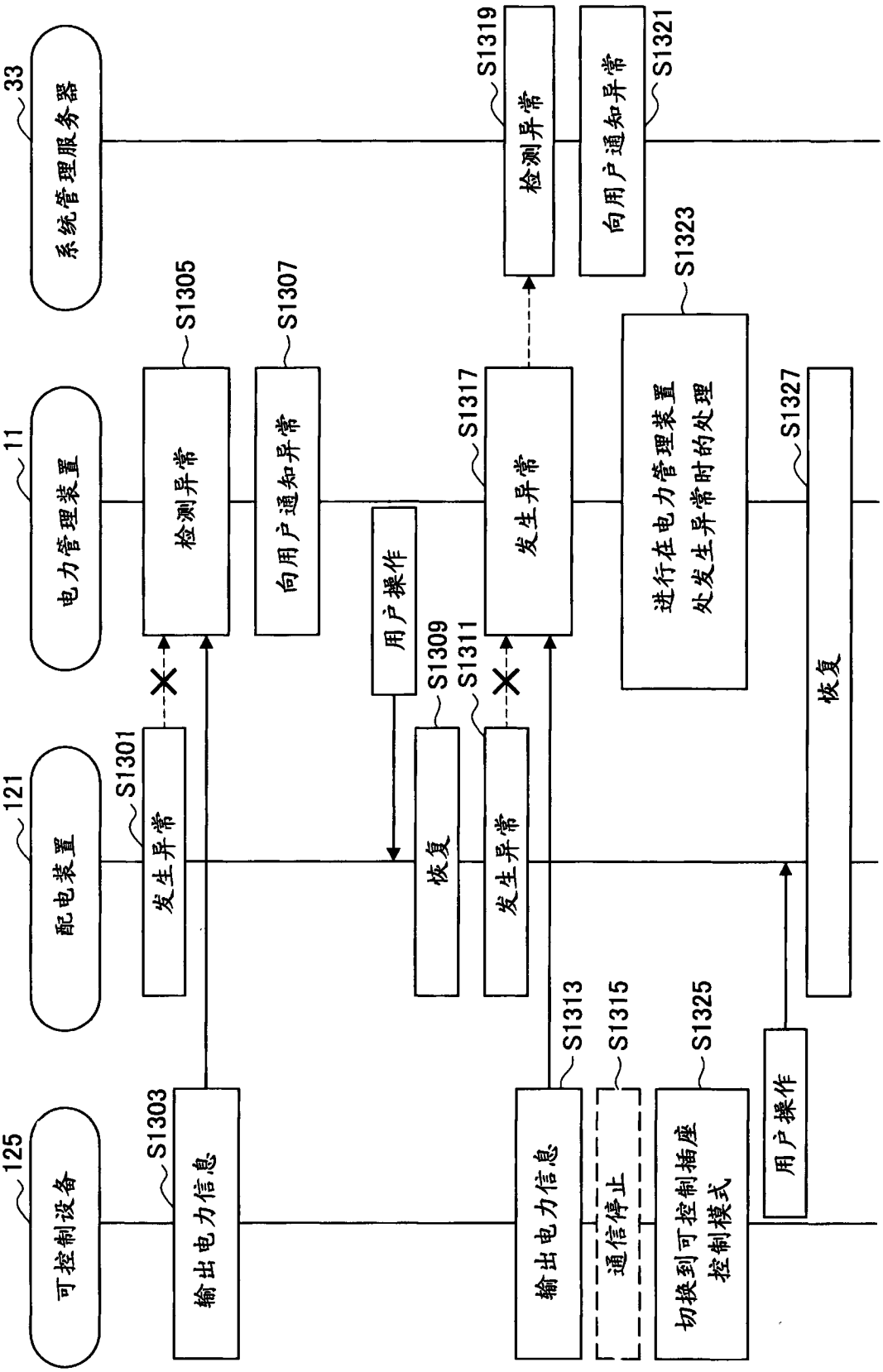

33
系统管理服务器
11
电力管理装置
121
配电装置
125
可控制设备
S1301
发生异常
S1303
输出电力信息
S1305
检测异常
S1307
向用户通知异常
S1309
恢复
S1311
发生异常
S1313
输出电力信息
S1315
通信停止
S1317
发生异常
S1319
检测异常
S1321
向用户通知异常
S1323
进行在电力管理装置处发生异常时的处理
S1325
切换到可控制插座控制模式
S1327
恢复
用户操作
用户操作

图 52

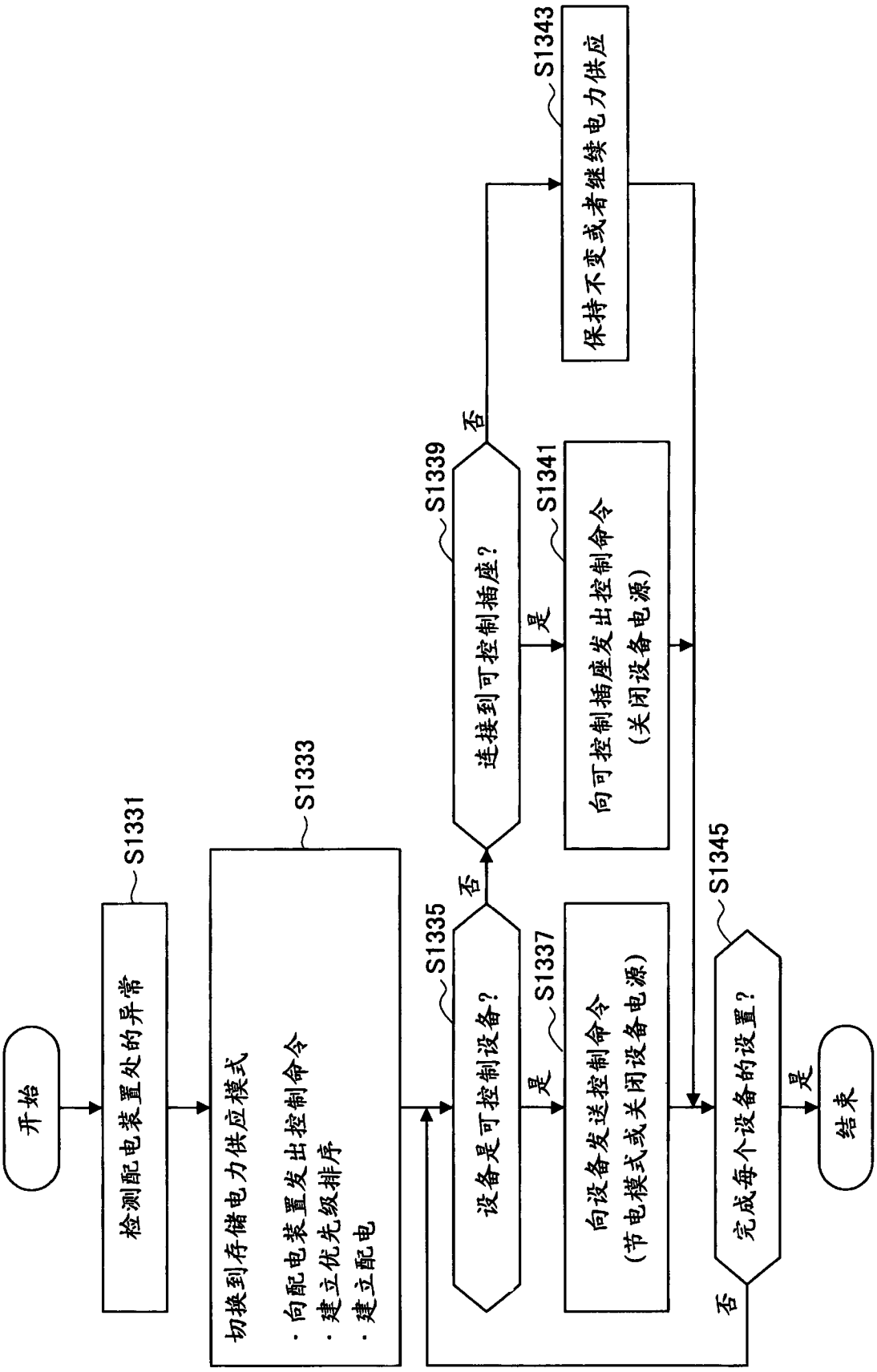

开始
检测配电装置处的异常
S1331
切换到存储电力供应模式
·向配电装置发出控制命令
·建立优先级排序
·建立配电
S1333
设备是可控制设备？
S1335
否
是
向设备发送控制命令
(节电模式或关闭设备电源)
S1337
连接到可控制插座？
S1339
否
是
向可控制插座发出控制命令
(关闭设备电源)
S1341
保持不变或者继续电力供应
S1343
完成每个设备的设置？
S1345
否
是
结束

图 53

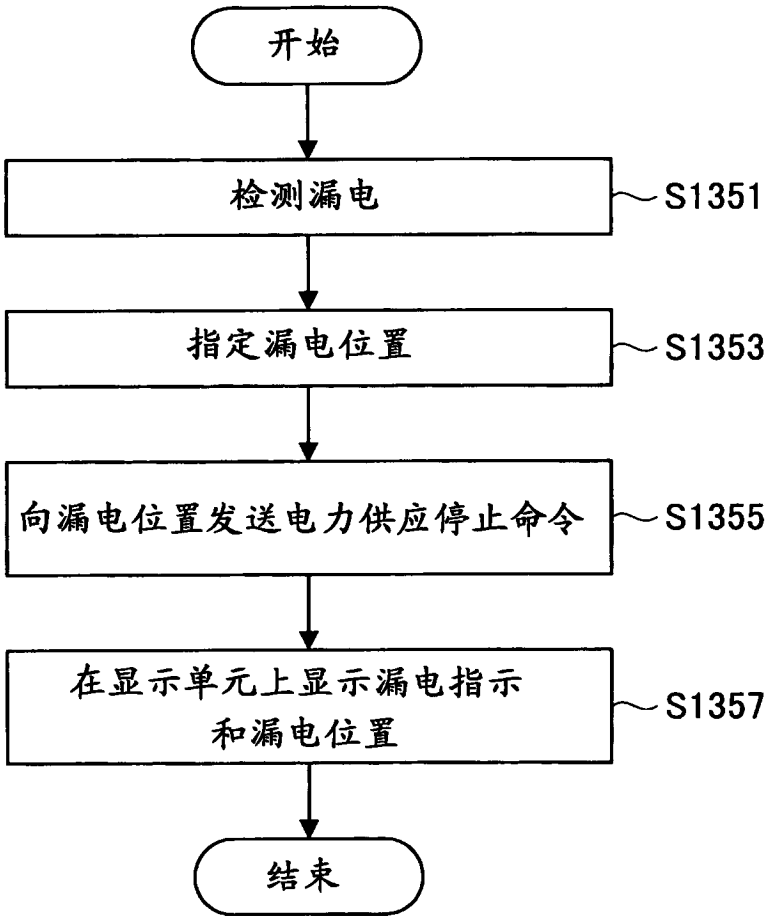

开始
检测漏电
S1351
指定漏电位置
S1353
向漏电位置发送电力供应停止命令
S1355
在显示单元上显示漏电指示
和漏电位置
S1357
结束

图 54

(可控制设备中的处理)

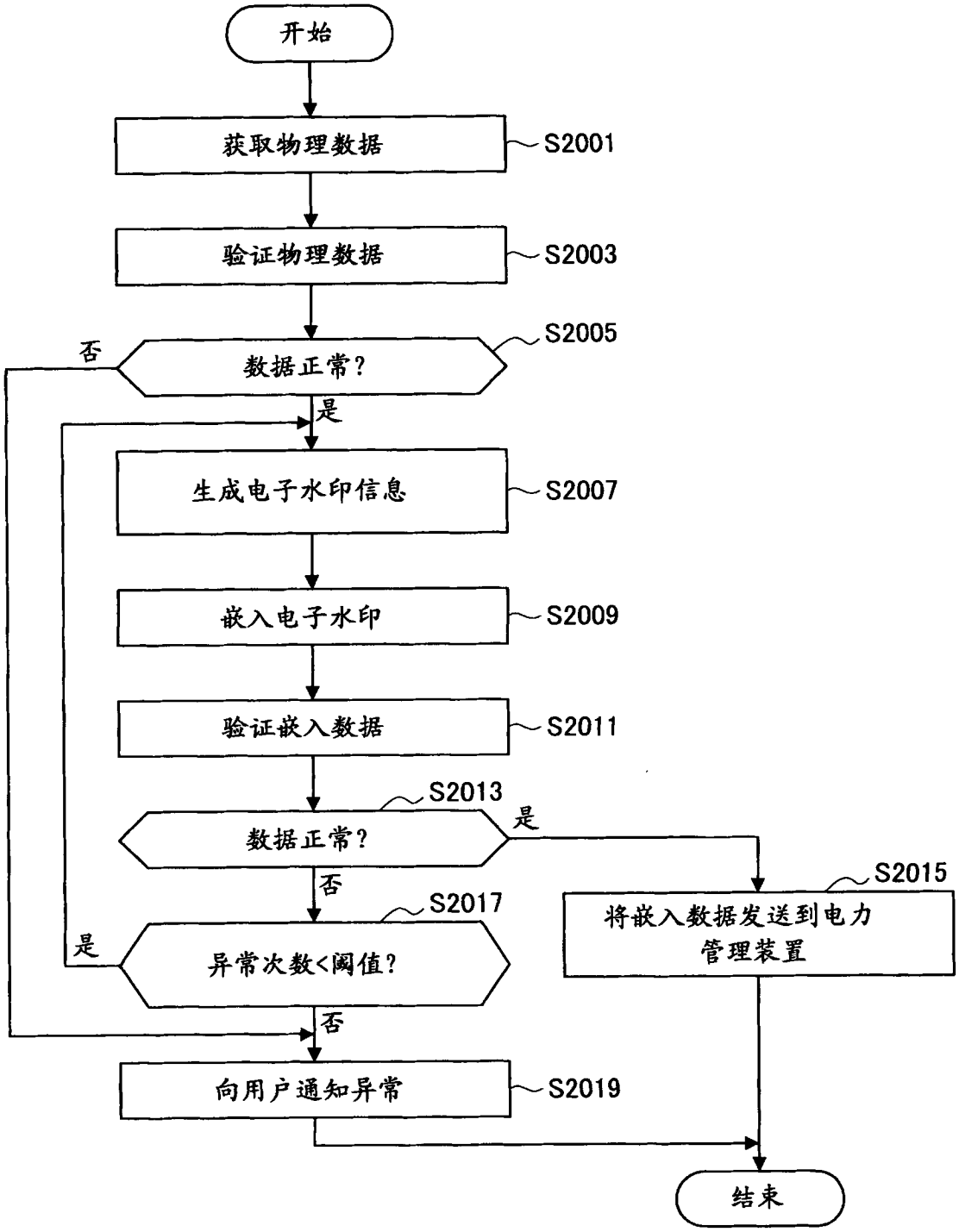
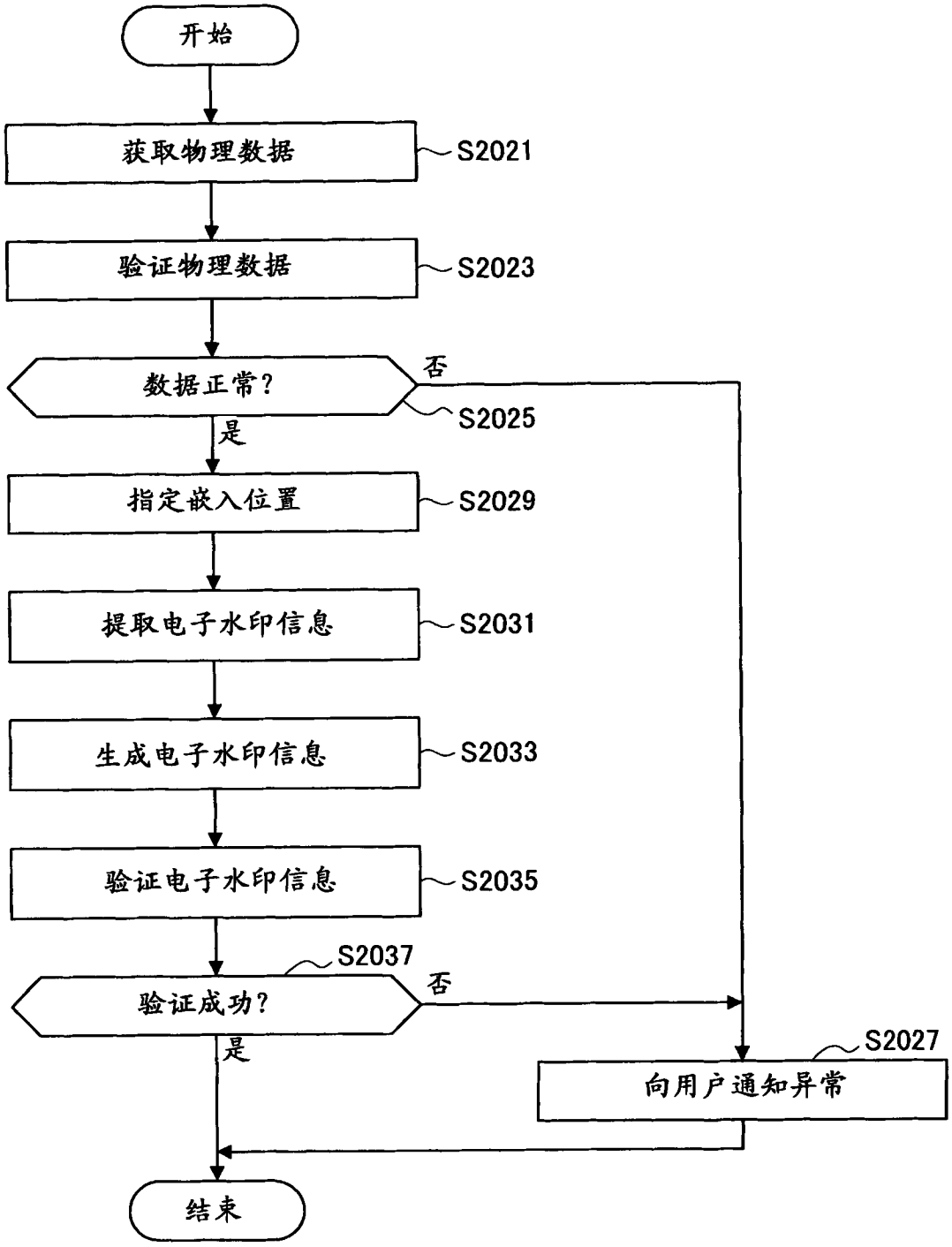


图 55

(分析服务器中的处理(*))



(*) 能够以电力管理装置中的相同方式进行验证

图 56

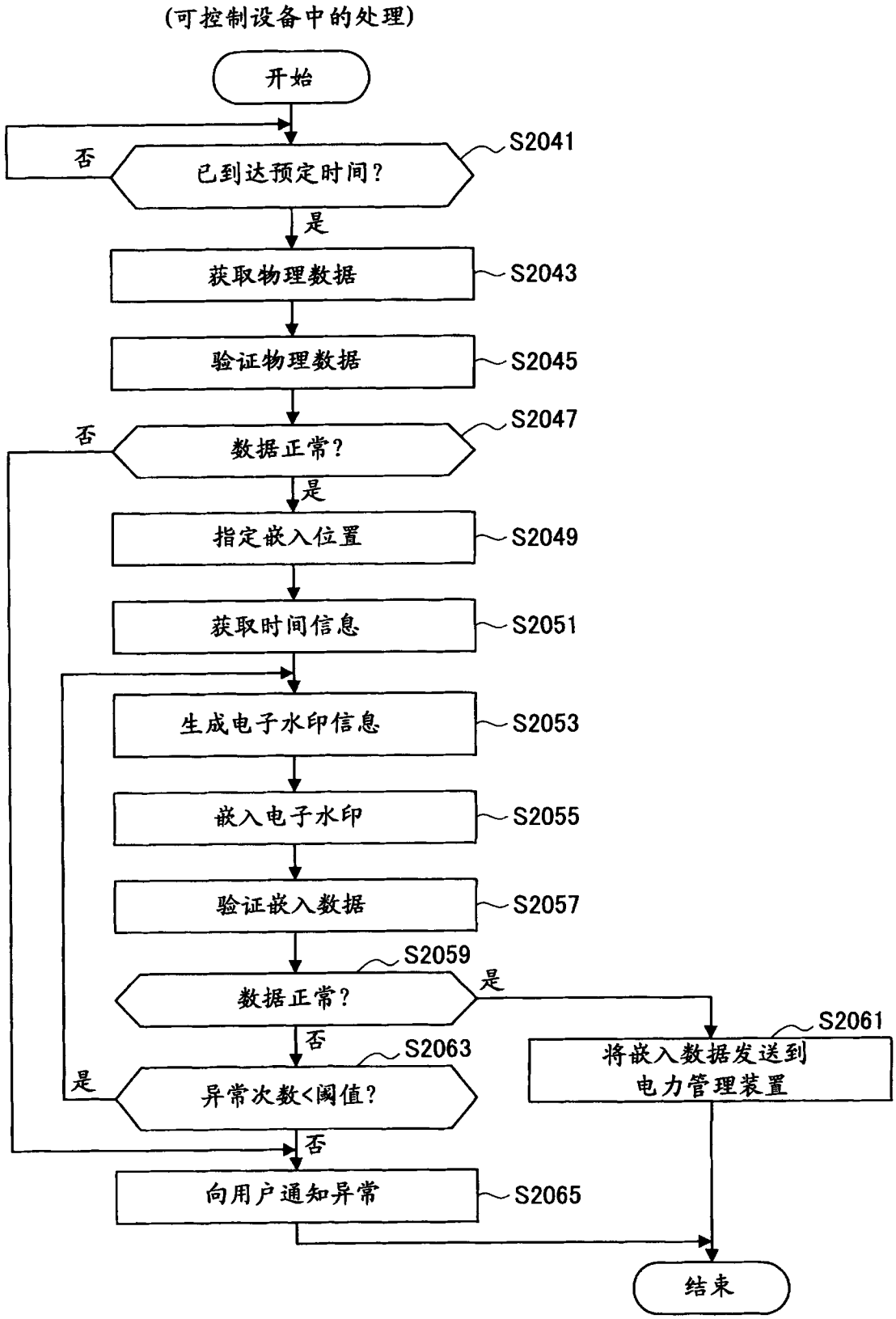

(可控制设备中的处理)
开始
S2041
否
已到达预定时间?
是
获取物理数据
S2043
验证物理数据
S2045
S2047
否
数据正常?
是
指定嵌入位置
S2049
获取时间信息
S2051
生成电子水印信息
S2053
嵌入电子水印
S2055
验证嵌入数据
S2057
S2059
数据正常?
是
S2061
将嵌入数据发送到
电力管理装置
否
S2063
是
异常次数<阈值?
否
向用户通知异常
S2065
结束

图 57

(分析服务器中的处理)

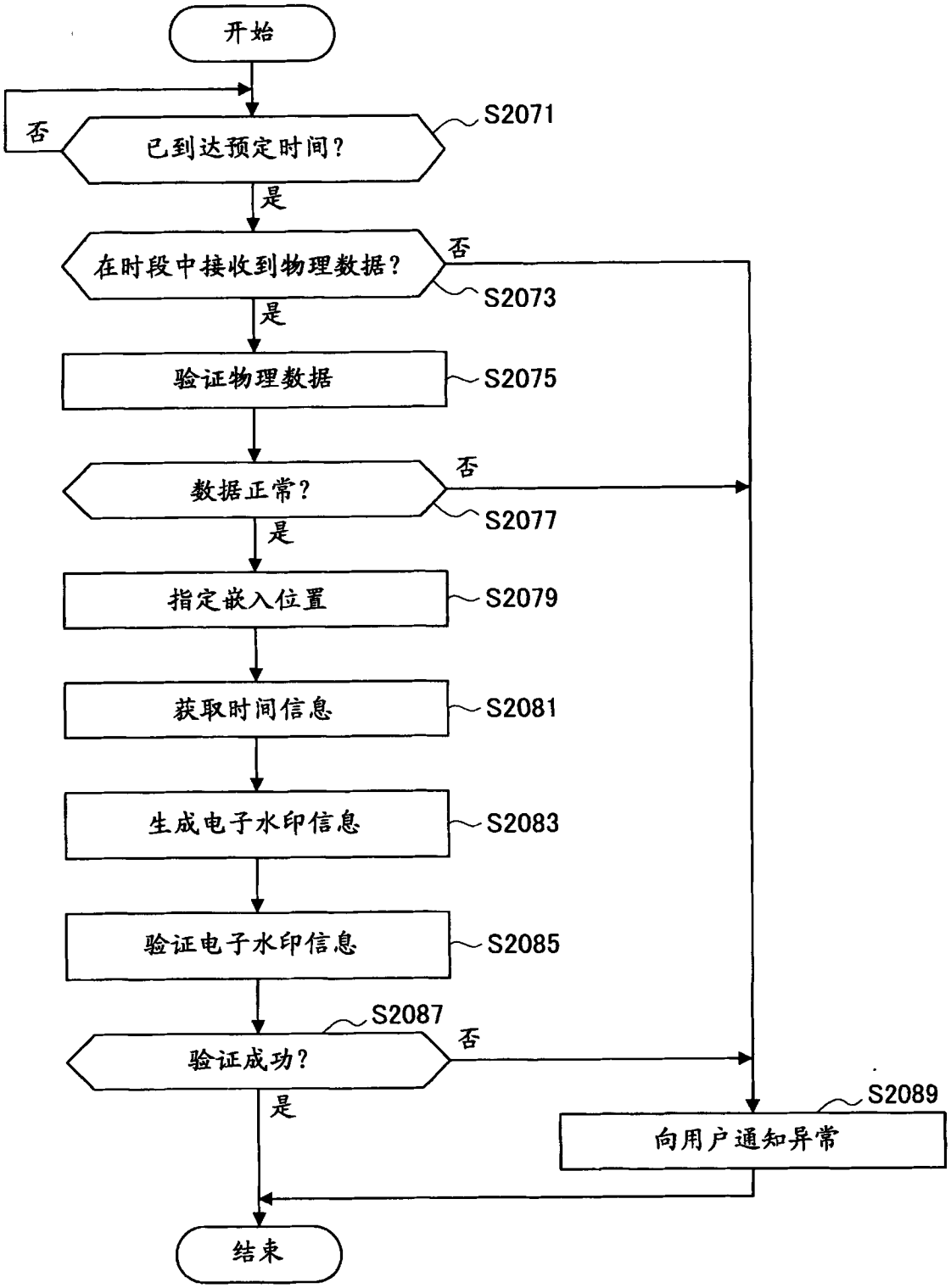


图 58

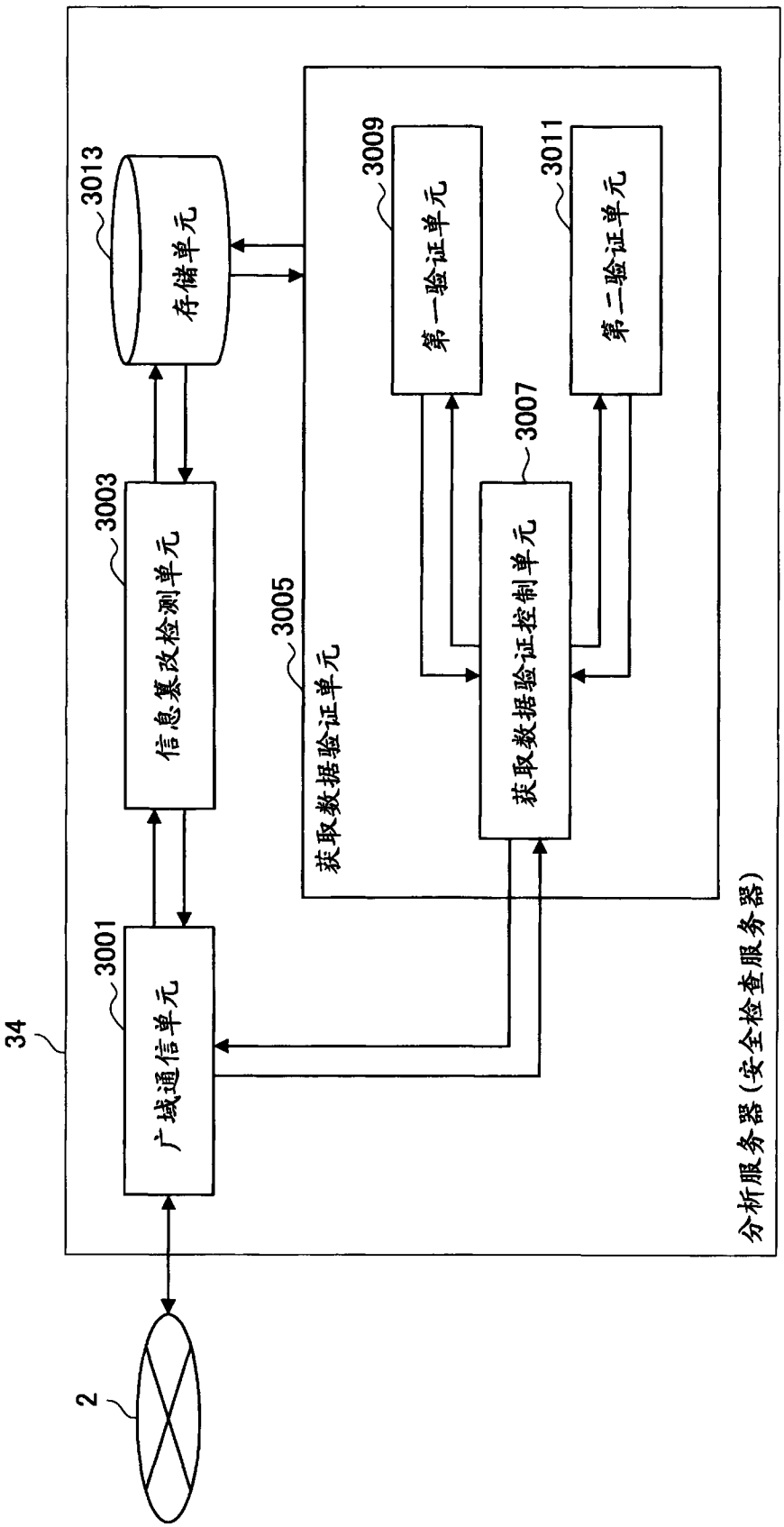

34
2
3001
广域通信单元
3003
信息篡改检测单元
3005
获取数据验证单元
3007
获取数据验证控制单元
3009
第一验证单元
3011
第二验证单元
3013
存储单元
分析服务器(安全检查服务器)

图 59

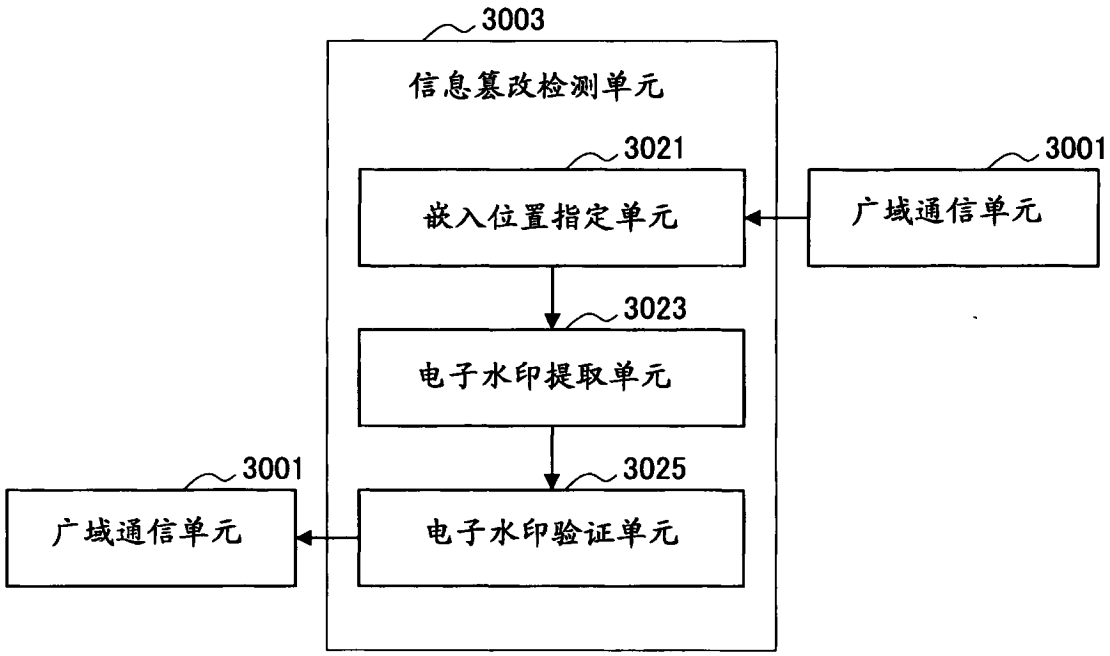

3003
信息篡改检测单元
3021
嵌入位置指定单元
3001
广域通信单元
3023
电子水印提取单元
3001
广域通信单元
3025
电子水印验证单元

图 60

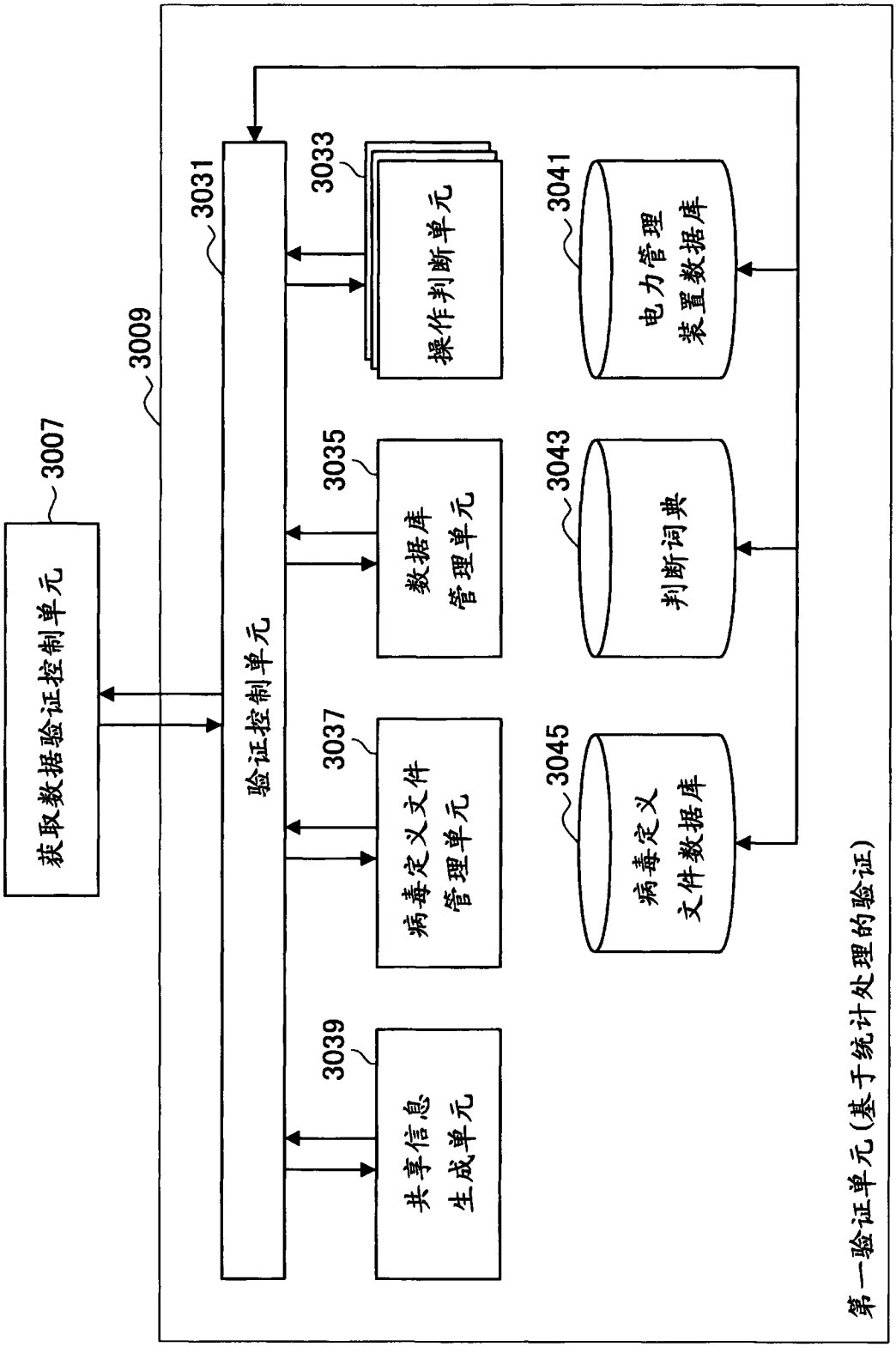

第一验证单元(基于统计处理的验证)
3009
3007
获取数据验证控制单元
验证控制单元
3031
3033
操作判断单元
3035
数据库
管理单元
3037
病毒定义文件
管理单元
3039
共享信息
生成单元
3041
电力管理
装置数据库
3043
判断词典
3045
病毒定义
文件数据库

图 61

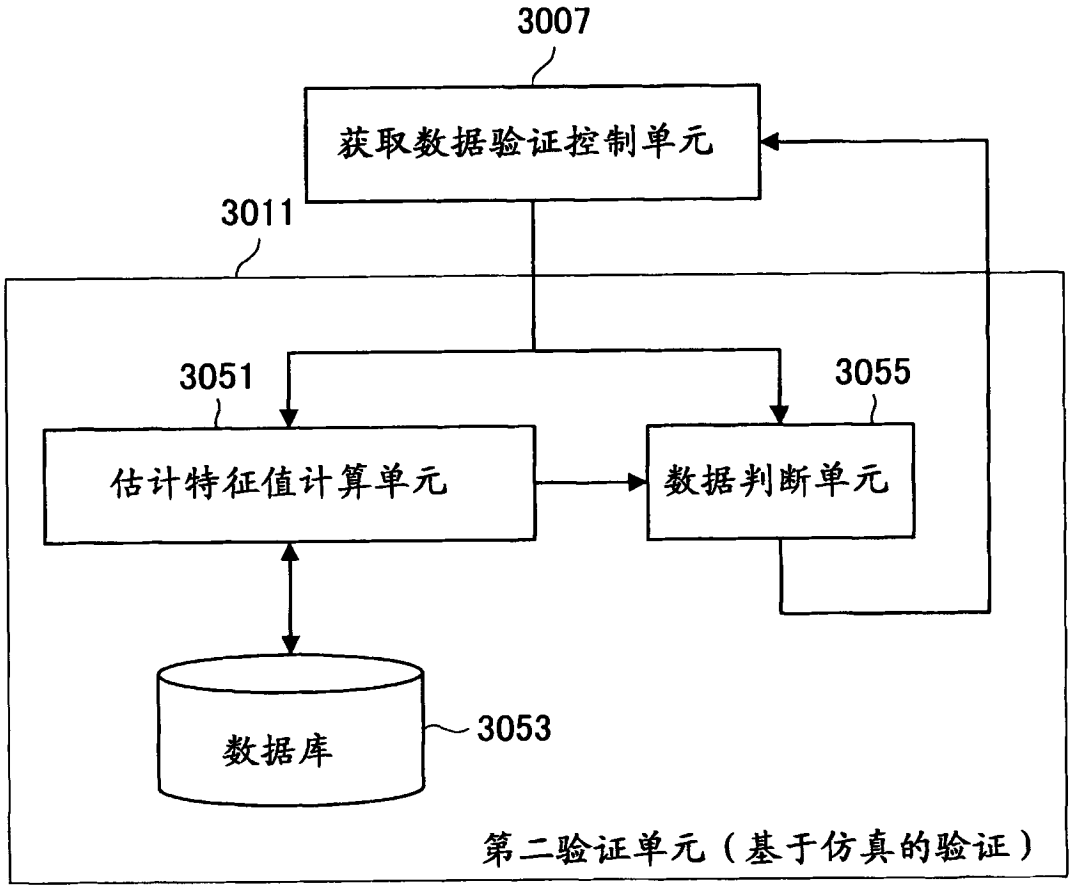

3007
获取数据验证控制单元
3011
3051
3055
估计特征值计算单元
数据判断单元
数据库
3053
第二验证单元（基于仿真的验证）

图 62

情况	电池	包括认证芯片的电路板	状态	电池特征/设备信息
1	合法产品	合法产品	正常	没有关于电池特征的问题，输出正确的设备信息 (*)
2			劣化	没有关于电池特征的问题，输出正确的设备信息
3				与估计的电池特征或者设备信息有差异
4	假冒产品	任一情况	正常	没有关于电池特征的问题，输出正确的设备信息
5		合法产品	部分缺陷	与估计的电池特征有差异但是输出正确设备信息
6		假冒认证芯片		与估计的电池特征有差异但是输出正确设备信息
7			缺陷	与估计的电池特征有差异并且也有设备信息的差异

(*) 与电池电压相关的信息、与剩余电量相关的信息等

图 63

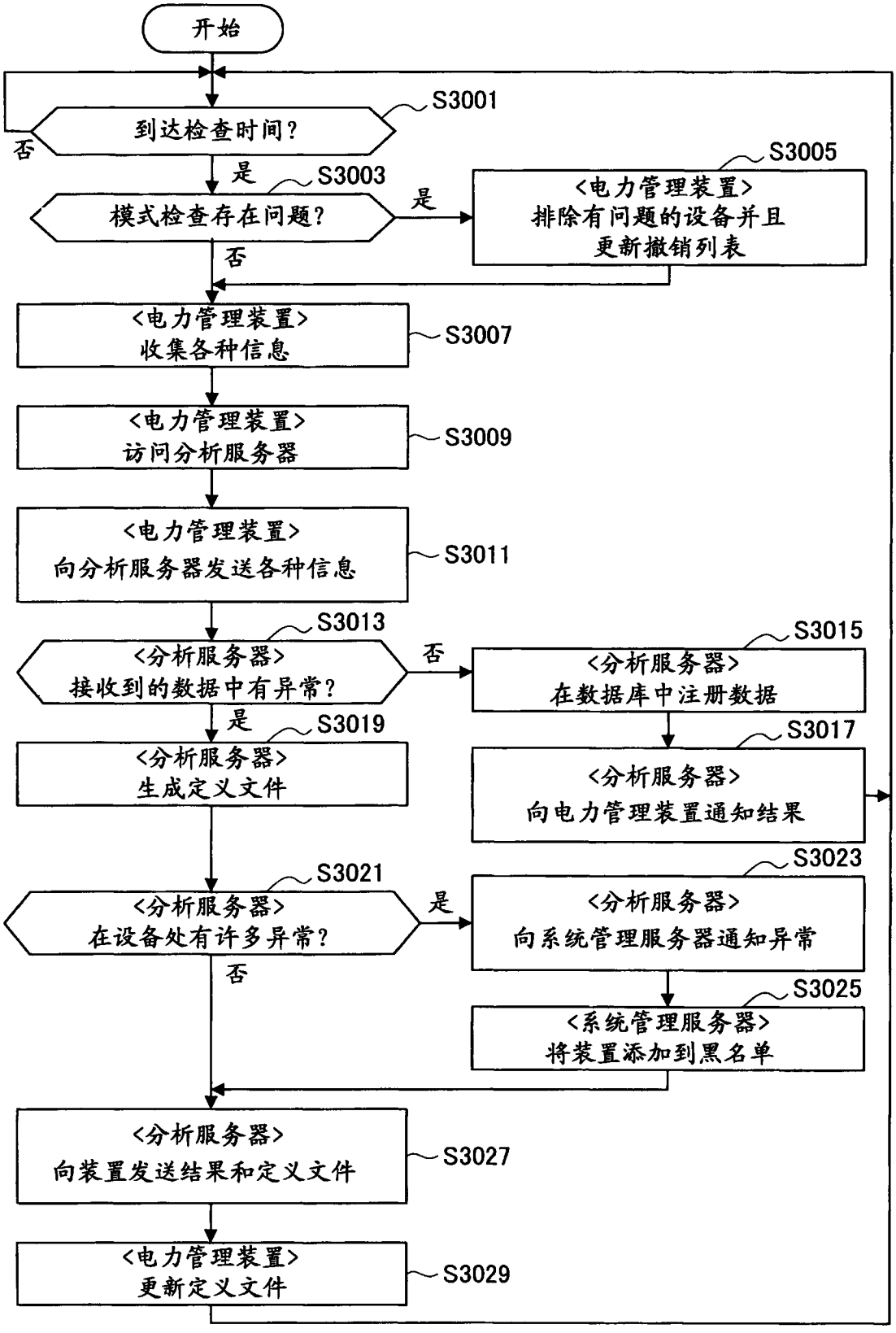

开始
S3001
到达检查时间？
否
是
S3003
模式检查存在问题？
是
S3005
<电力管理装置>
排除有问题的设备并且
更新撤销列表
否
<电力管理装置>
收集各种信息
S3007
<电力管理装置>
访问分析服务器
S3009
<电力管理装置>
向分析服务器发送各种信息
S3011
S3013
<分析服务器>
接收到的数据中有异常？
否
S3015
<分析服务器>
在数据库中注册数据
是
S3019
<分析服务器>
生成定义文件
S3017
<分析服务器>
向电力管理装置通知结果
S3021
<分析服务器>
在设备处有许多异常？
是
S3023
<分析服务器>
向系统管理服务器通知异常
否
S3025
<系统管理服务器>
将装置添加到黑名单
<分析服务器>
向装置发送结果和定义文件
S3027
<电力管理装置>
更新定义文件
S3029

图 64

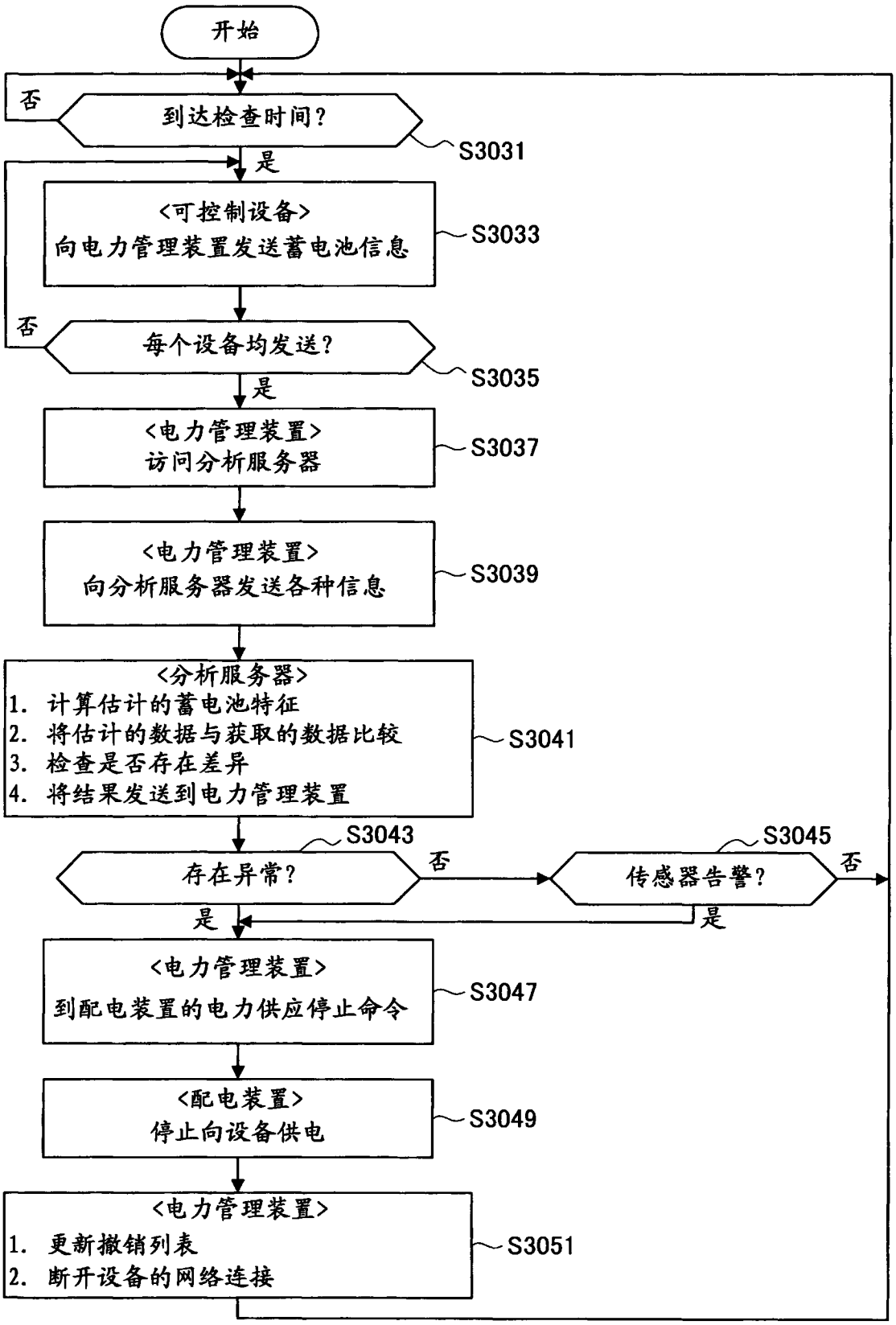

开始
否
到达检查时间？
S3031
是
<可控制设备>
向电力管理装置发送蓄电池信息
S3033
否
每个设备均发送？
S3035
是
<电力管理装置>
访问分析服务器
S3037
<电力管理装置>
向分析服务器发送各种信息
S3039
<分析服务器>
1. 计算估计的蓄电池特征
2. 将估计的数据与获取的数据比较
3. 检查是否存在差异
4. 将结果发送到电力管理装置
S3041
S3043
存在异常？
否
S3045
传感器告警？
否
是
是
<电力管理装置>
到配电装置的电力供应停止命令
S3047
<配电装置>
停止向设备供电
S3049
<电力管理装置>
1. 更新撤销列表
2. 断开设备的网络连接
S3051

图 65

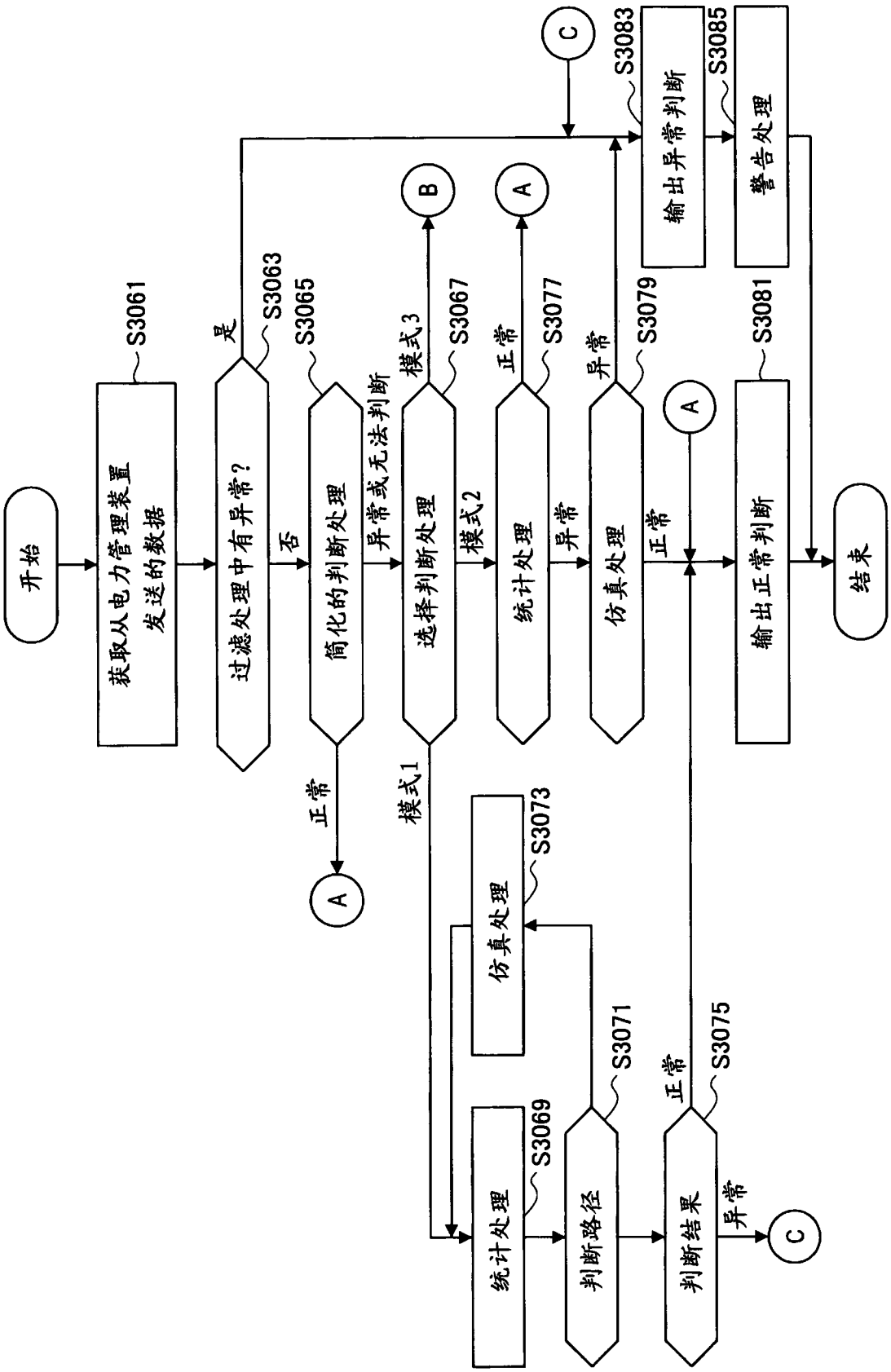

开始
获取从电力管理装置发送的数据
S3061
过滤处理中有异常?
是
否
S3063
简化的判断处理
正常
异常或无法判断
S3065
选择判断处理
模式1
模式2
模式3
S3067
统计处理
正常
异常
S3077
仿真处理
正常
异常
S3079
输出正常判断
S3081
输出异常判断
S3083
警告处理
S3085
结束
A
B
C
仿真处理
S3073
统计处理
S3069
判断路径
S3071
判断结果
正常
异常
S3075

图 66A

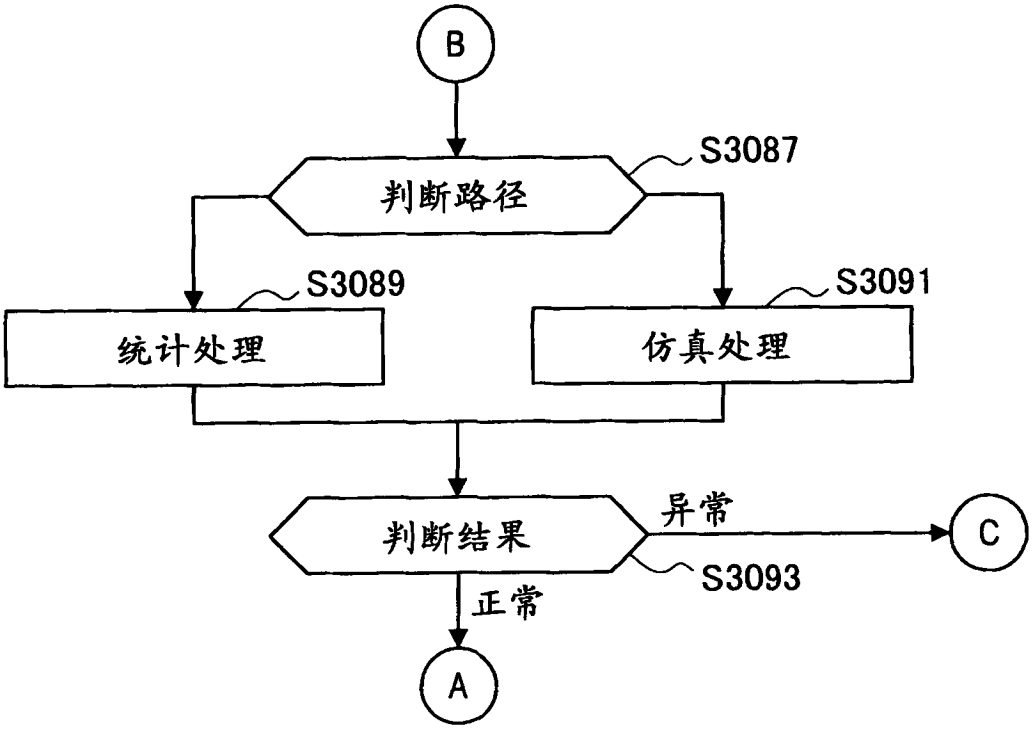


图 66B

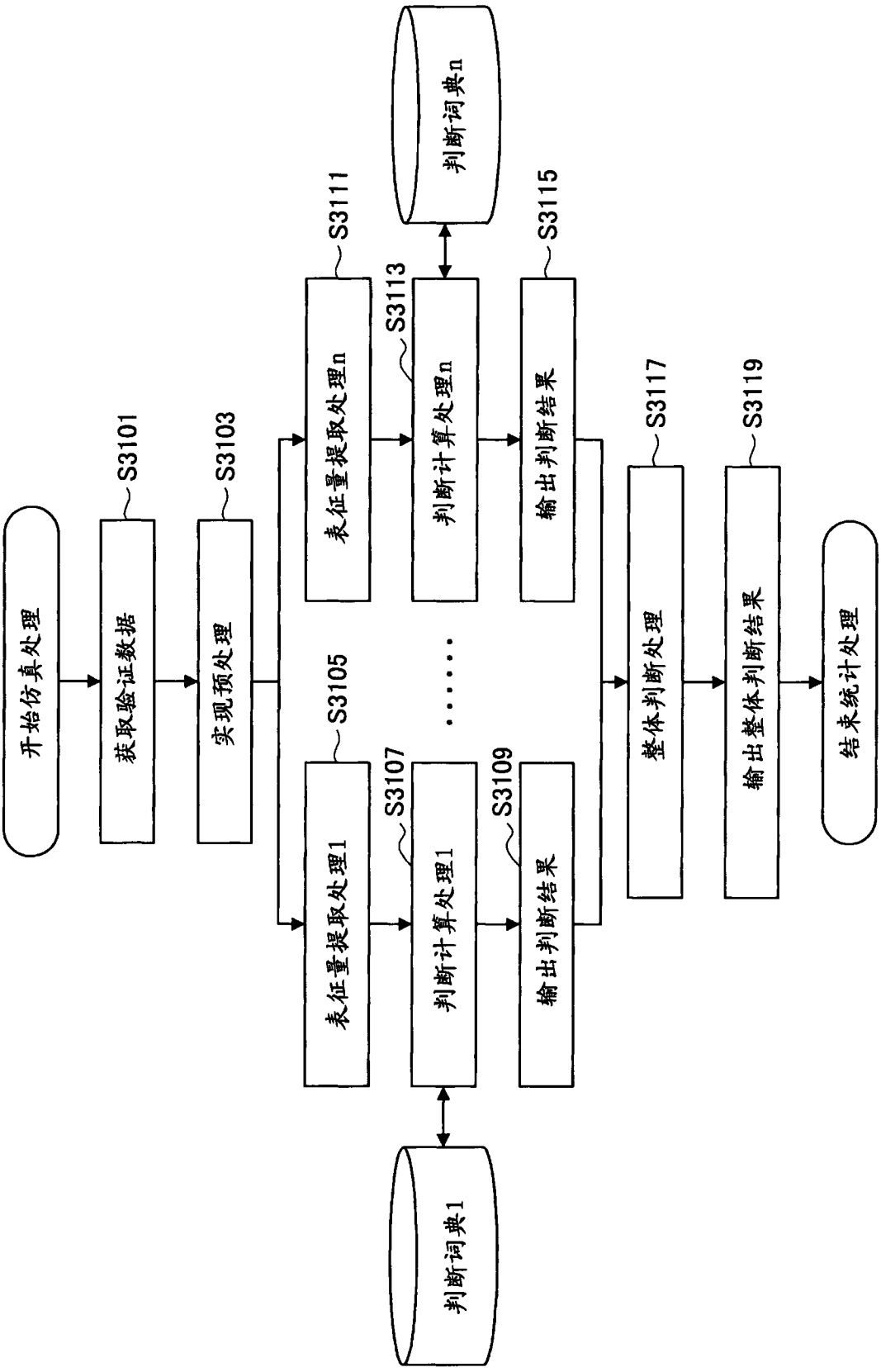

开始仿真处理
S3101
获取验证数据
S3103
实现预处理
S3105
表征量提取处理1
S3107
判断计算处理1
S3109
输出判断结果
判断词典1
S3111
表征量提取处理n
S3113
判断计算处理n
S3115
输出判断结果
判断词典n
S3117
整体判断处理
S3119
输出整体判断结果
结束统计处理

图 67

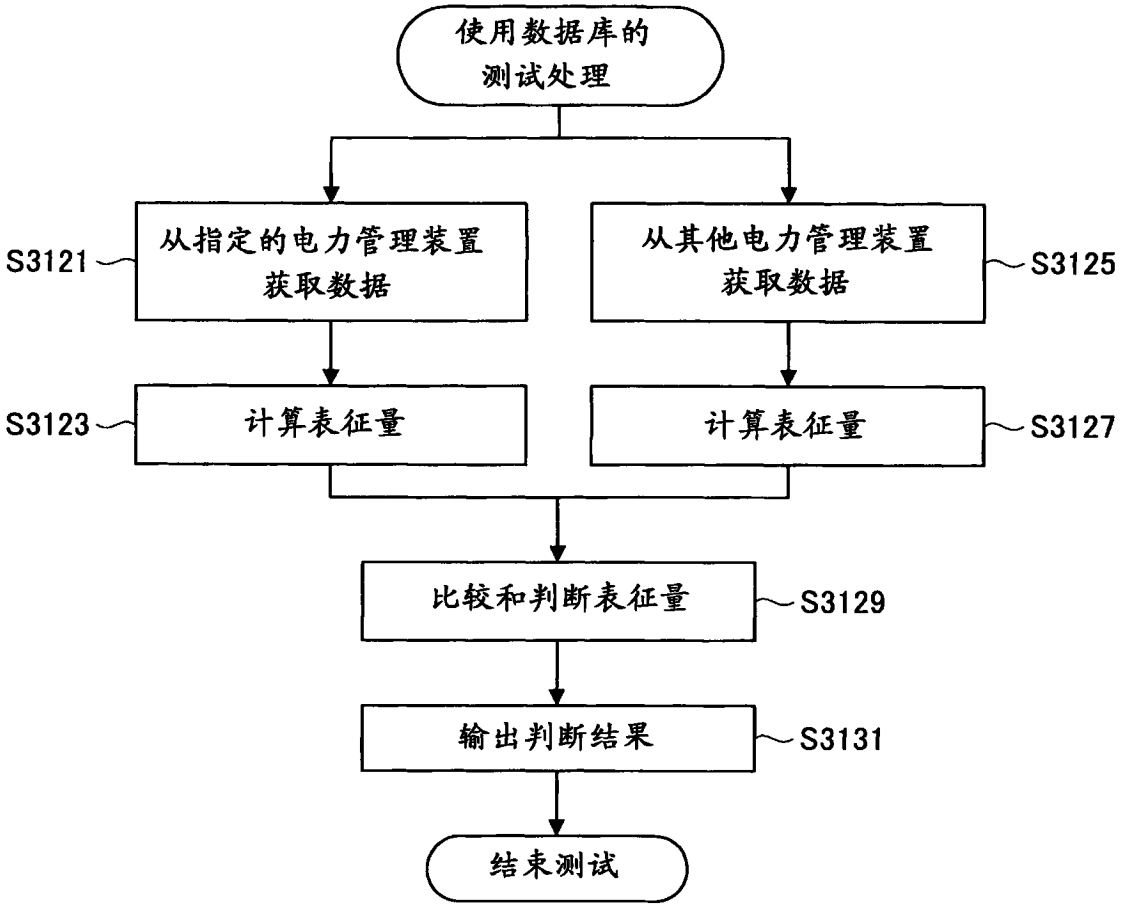

使用数据库的
测试处理
从指定的电力管理装置
获取数据
S3121
从其他电力管理装置
获取数据
S3125
计算表征量
S3123
计算表征量
S3127
比较和判断表征量
S3129
输出判断结果
S3131
结束测试

图 68

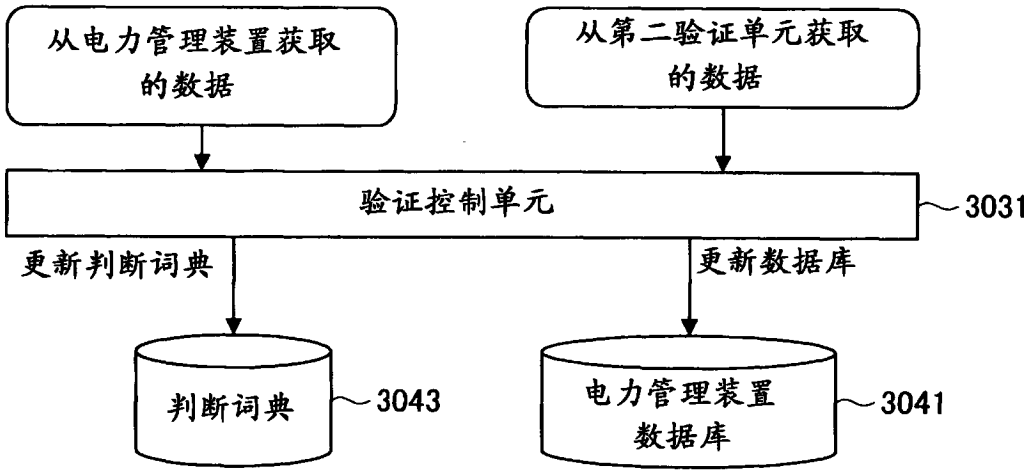

从电力管理装置获取
的数据
从第二验证单元获取
的数据
验证控制单元
3031
更新判断词典
更新数据库
判断词典
3043
电力管理装置
数据库
3041

图 69

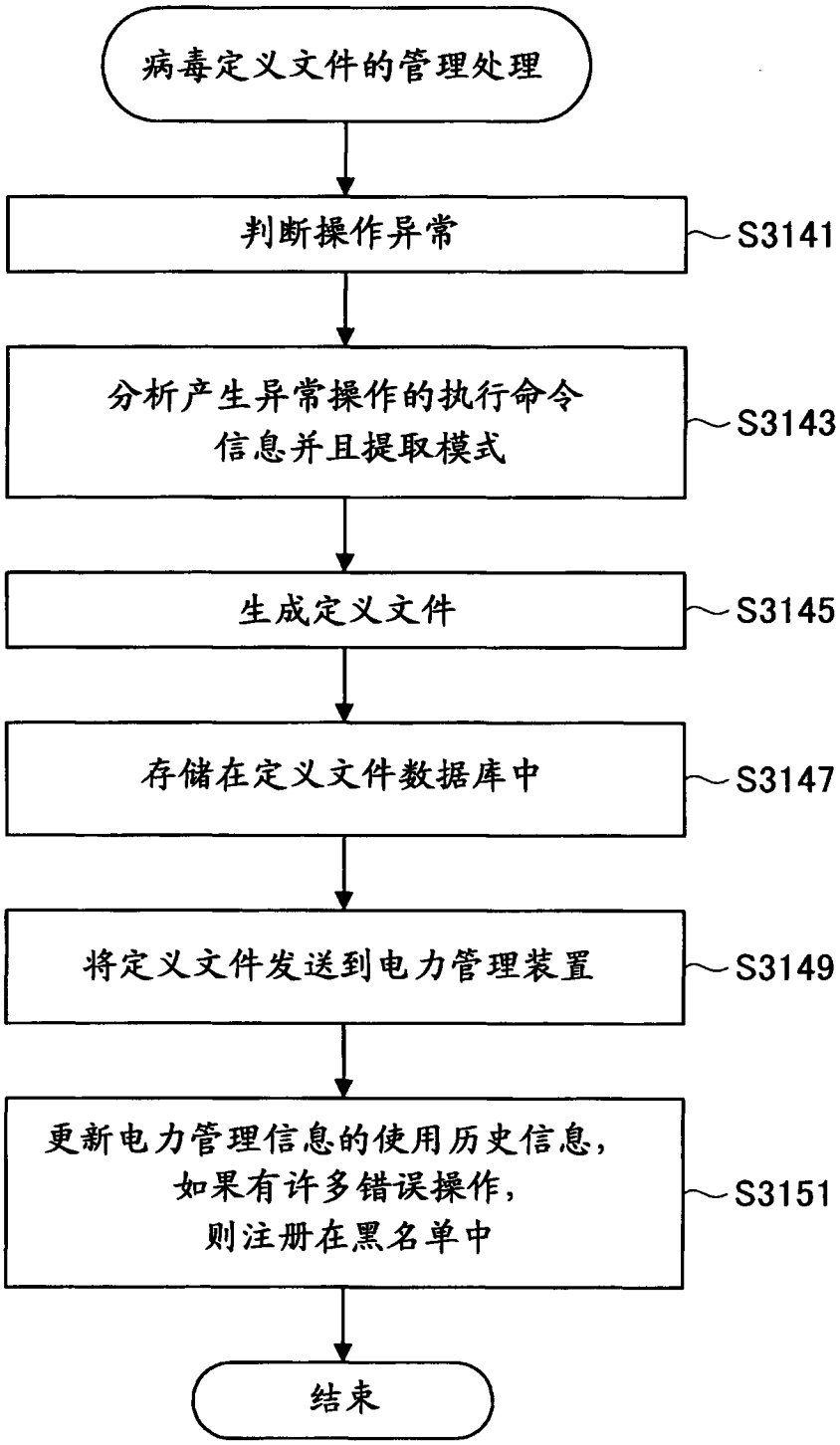

病毒定义文件的管理处理
判断操作异常
S3141
分析产生异常操作的执行命令
信息并且提取模式
S3143
生成定义文件
S3145
存储在定义文件数据库中
S3147
将定义文件发送到电力管理装置
S3149
更新电力管理信息的使用历史信息，
如果有许多错误操作，
则注册在黑名单中
S3151
结束

图 70

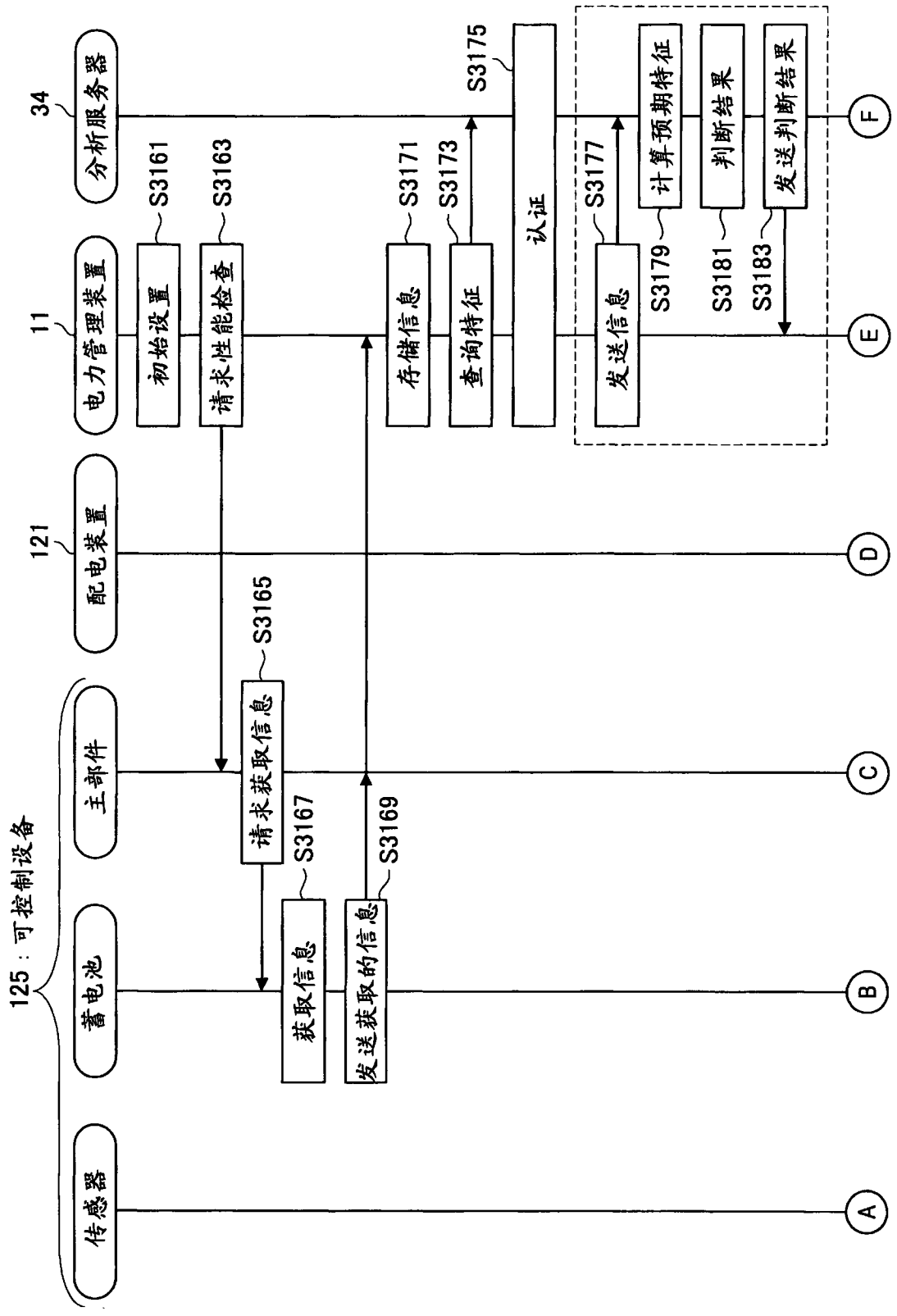

125：可控制设备
传感器
蓄电池
主部件
121
配电装置
11
电力管理装置
34
分析服务器
初始设置
S3161
请求性能检查
S3163
请求获取信息
S3165
获取信息
S3167
发送获取的信息
S3169
存储信息
S3171
查询特征
S3173
S3175
认证
发送信息
S3177
S3179
计算预期特征
判断结果
S3181
发送判断结果
S3183
A
B
C
D
E
F

图 71A

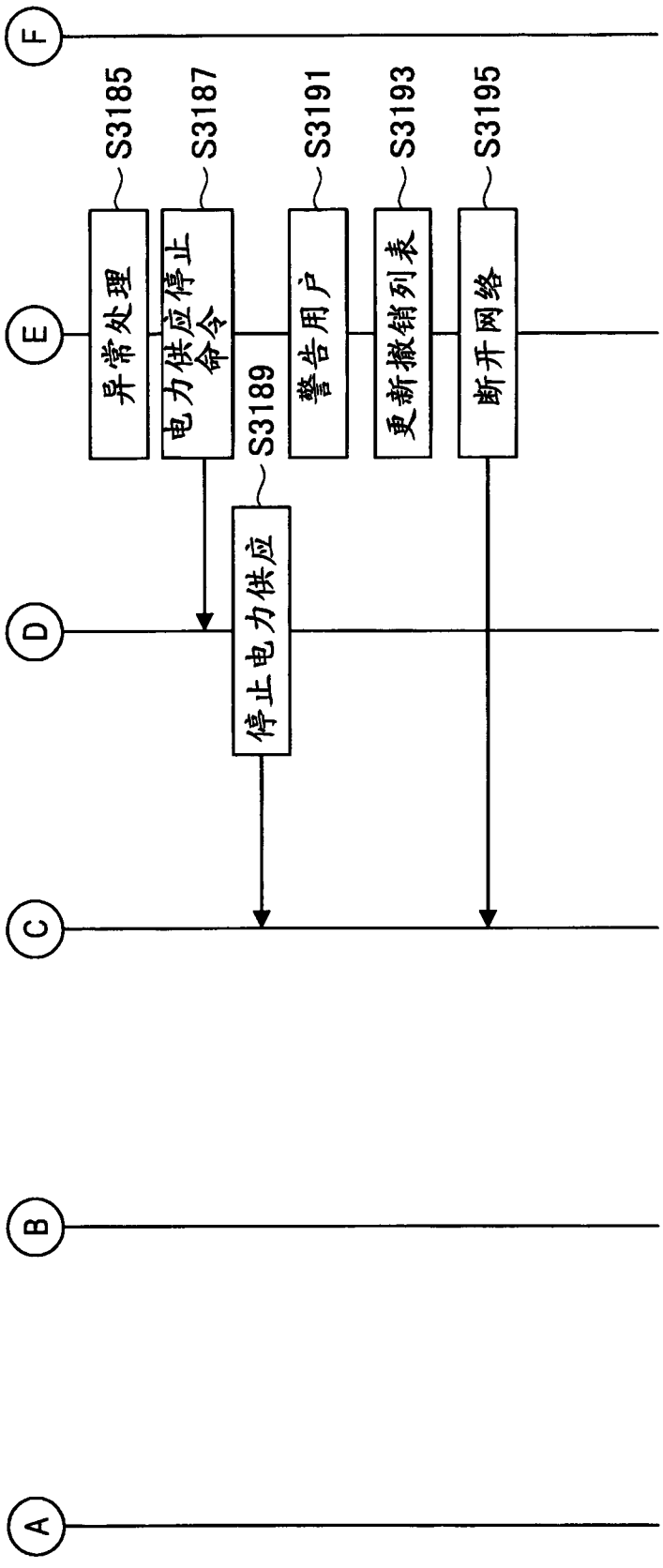

F
S3185
S3187
S3191
S3193
S3195
异常处理
电力供应停止命令
警告用户
更新撤销列表
断开网络
E
S3189
停止电力供应
D
C
B
A

图 71B

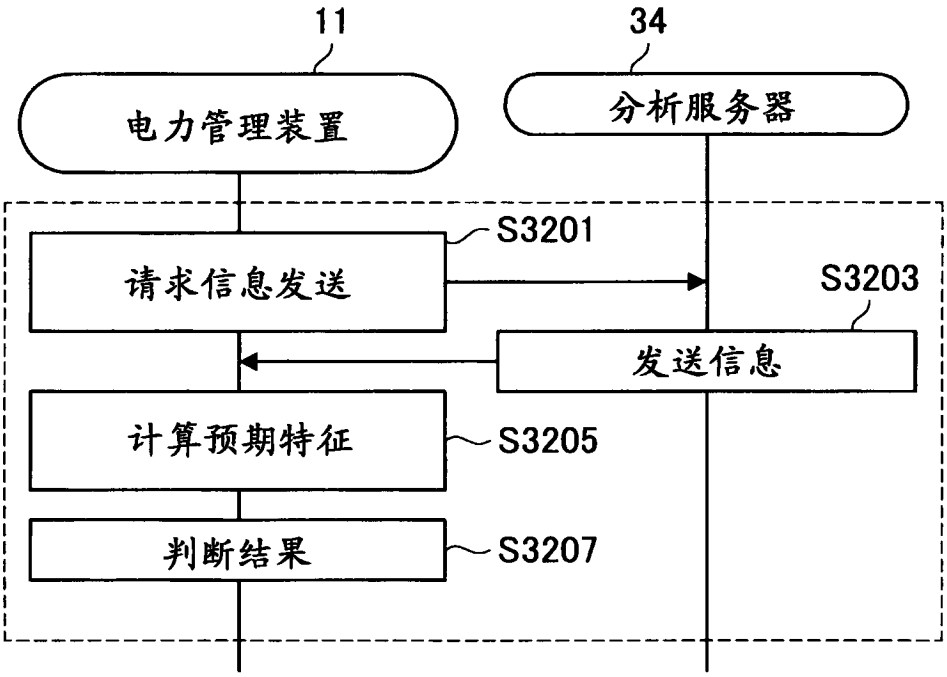

11
34
电力管理装置
分析服务器
S3201
请求信息发送
S3203
发送信息
计算预期特征
S3205
判断结果
S3207

图 71C

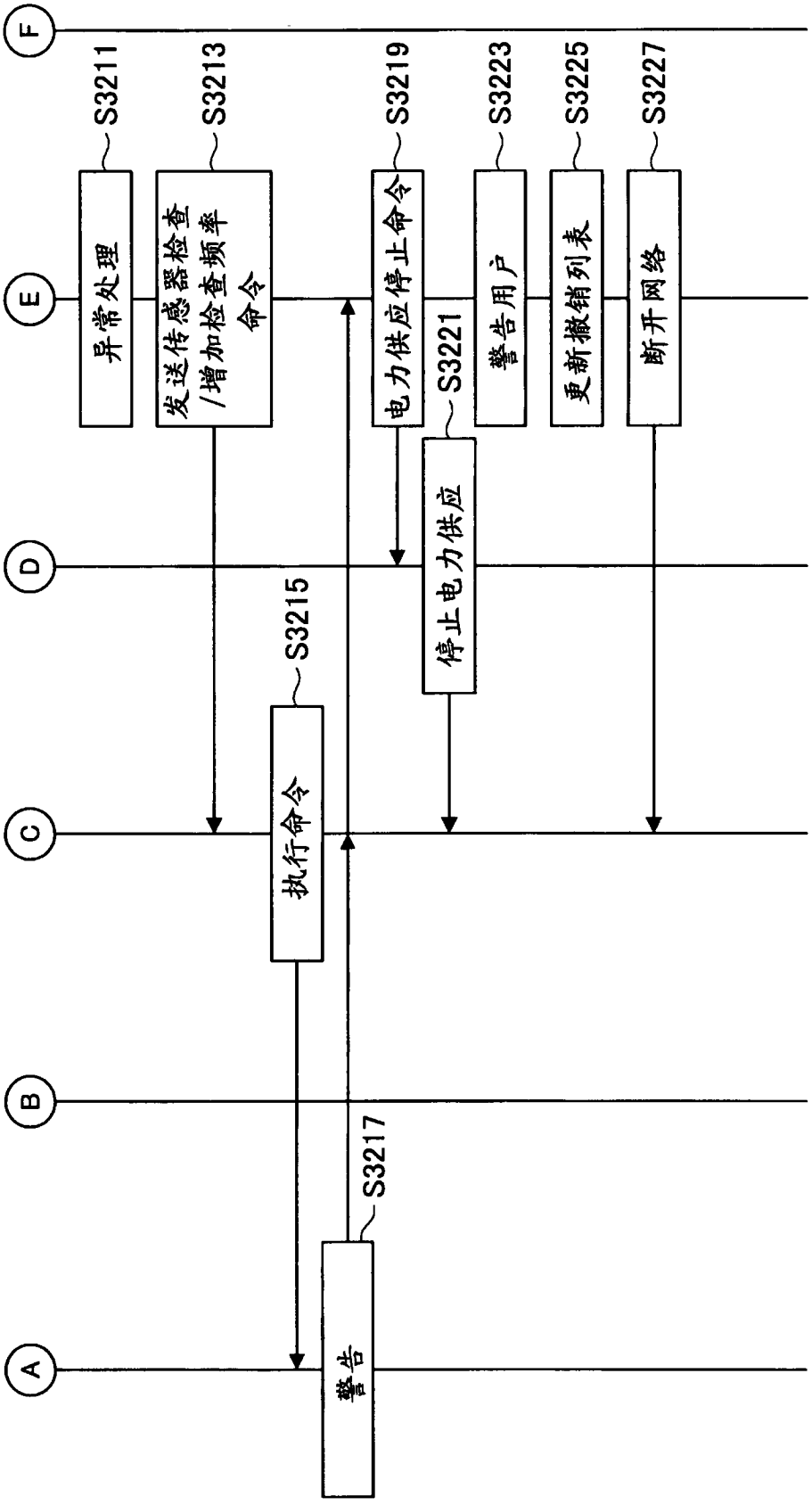

F
E
D
C
B
A
S3211
异常处理
S3213
发送传感器检查/增加检查频率命令
S3219
电力供应停止命令
S3223
警告用户
S3225
更新撤销列表
S3227
断开网络
S3221
停止电力供应
S3215
执行命令
S3217
警告

图 72

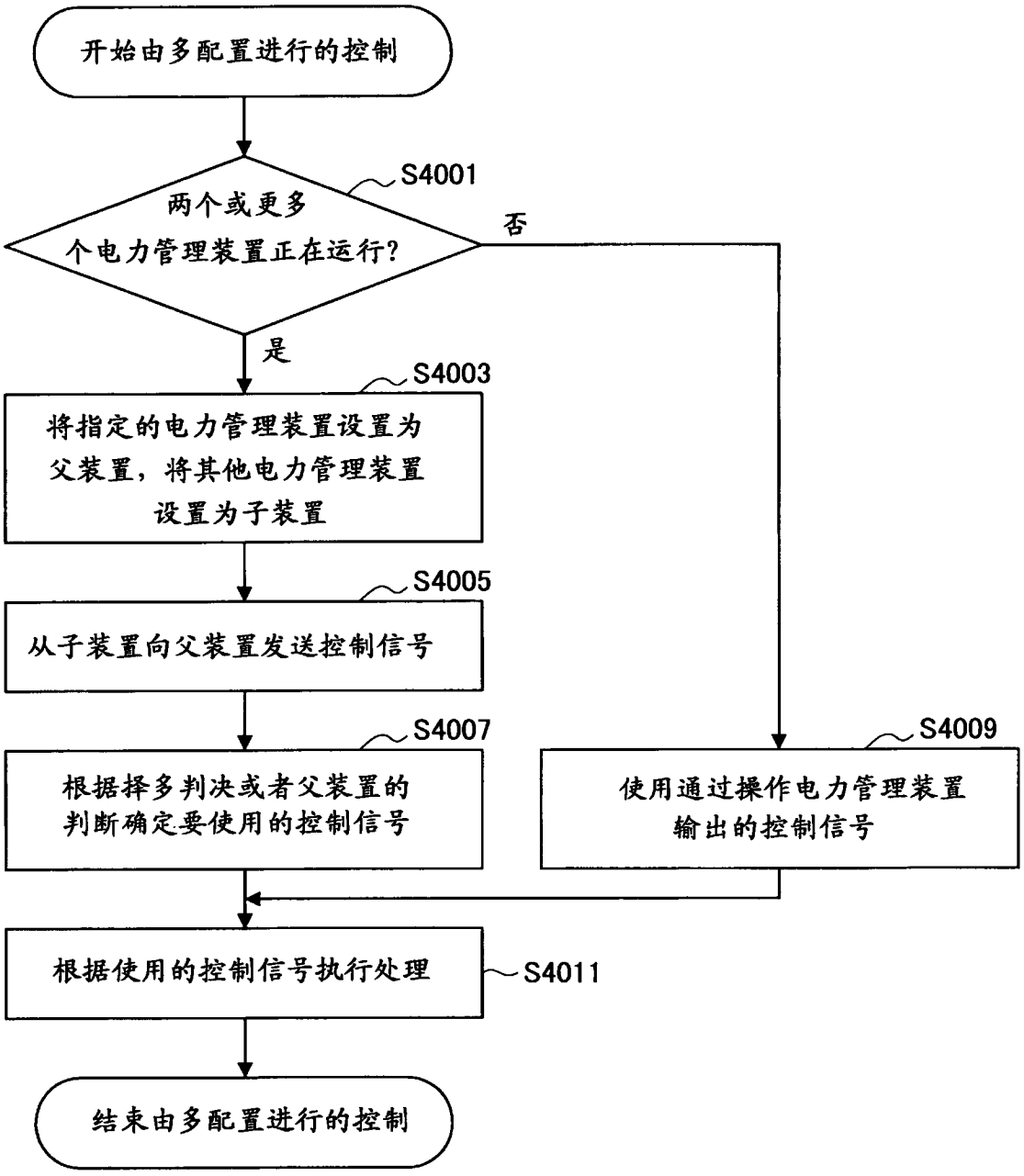

开始由多配置进行的控制
S4001
两个或更多
个电力管理装置正在运行?
否
是
S4003
将指定的电力管理装置设置为
父装置，将其他电力管理装置
设置为子装置
S4005
从子装置向父装置发送控制信号
S4007
根据择多判决或者父装置的
判断确定要使用的控制信号
S4009
使用通过操作电力管理装置
输出的控制信号
根据使用的控制信号执行处理
S4011
结束由多配置进行的控制

图 73

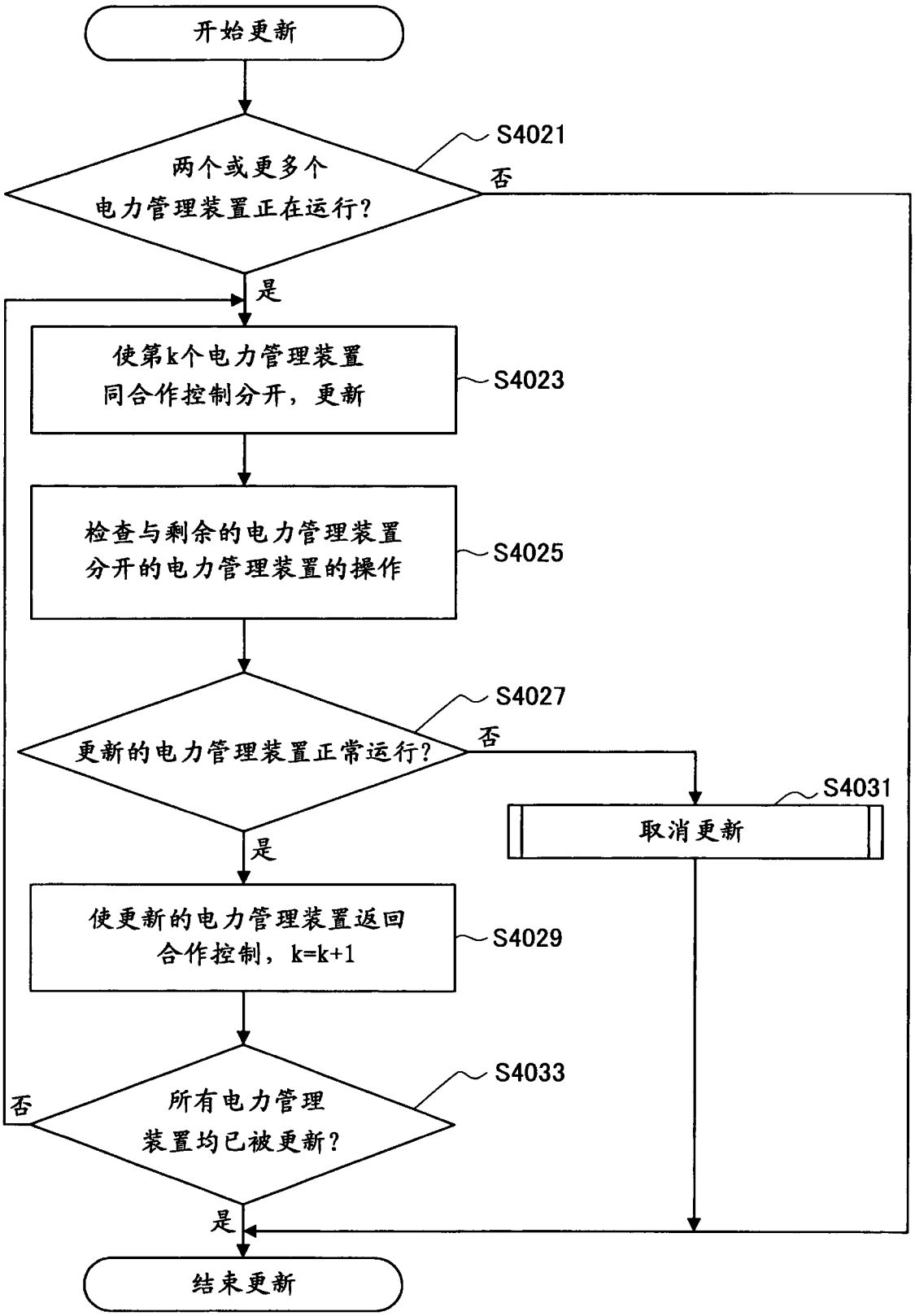

开始更新
两个或更多个
电力管理装置正在运行?
S4021
否
是
使第k个电力管理装置
同合作控制分开，更新
S4023
检查与剩余的电力管理装置
分开的电力管理装置的操作
S4025
更新的电力管理装置正常运行?
S4027
否
S4031
取消更新
是
使更新的电力管理装置返回
合作控制，k=k+1
S4029
所有电力管理
装置均已被更新?
S4033
否
是
结束更新

图 74

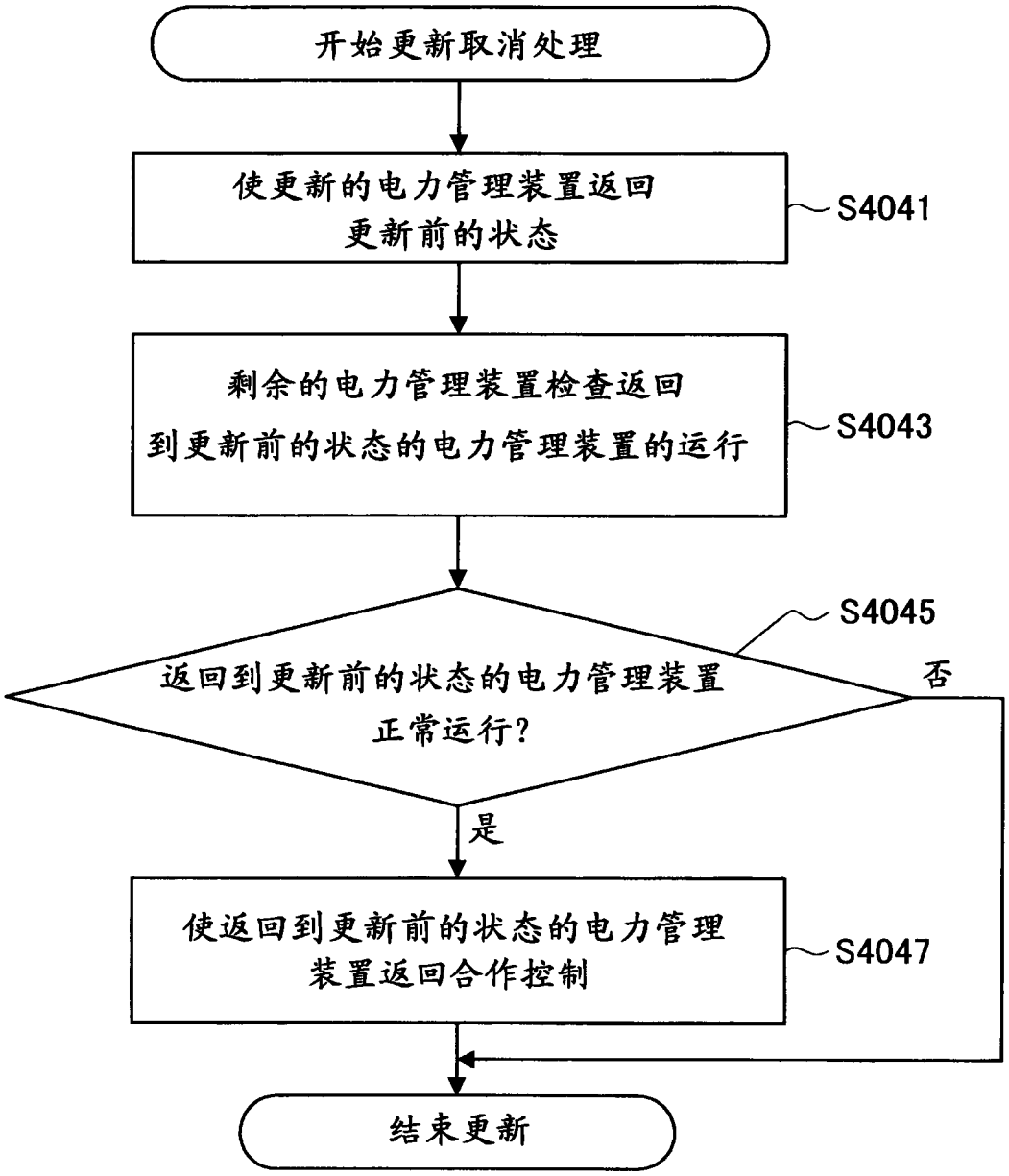

开始更新取消处理
使更新的电力管理装置返回
更新前的状态
S4041
剩余的电力管理装置检查返回
到更新前的状态的电力管理装置的运行
S4043
返回到更新前的状态的电力管理装置
正常运行?
S4045
否
是
使返回到更新前的状态的电力管理
装置返回合作控制
S4047
结束更新

图 75

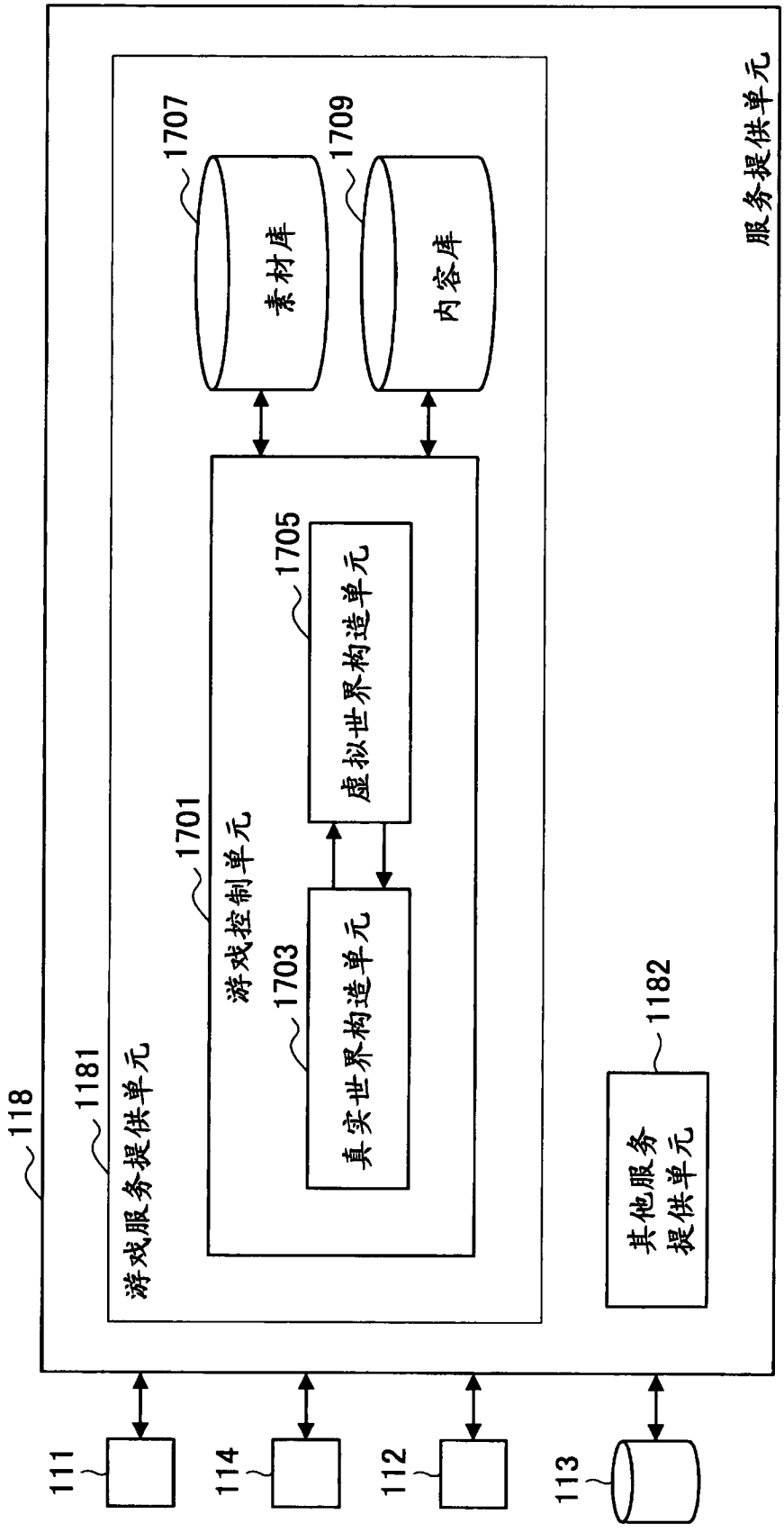

118
服务提供单元
1181
游戏服务提供单元
1701
游戏控制单元
1703
真实世界构造单元
1705
虚拟世界构造单元
1707
素材库
1709
内容库
1182
其他服务提供单元
111
114
112
113

图 76

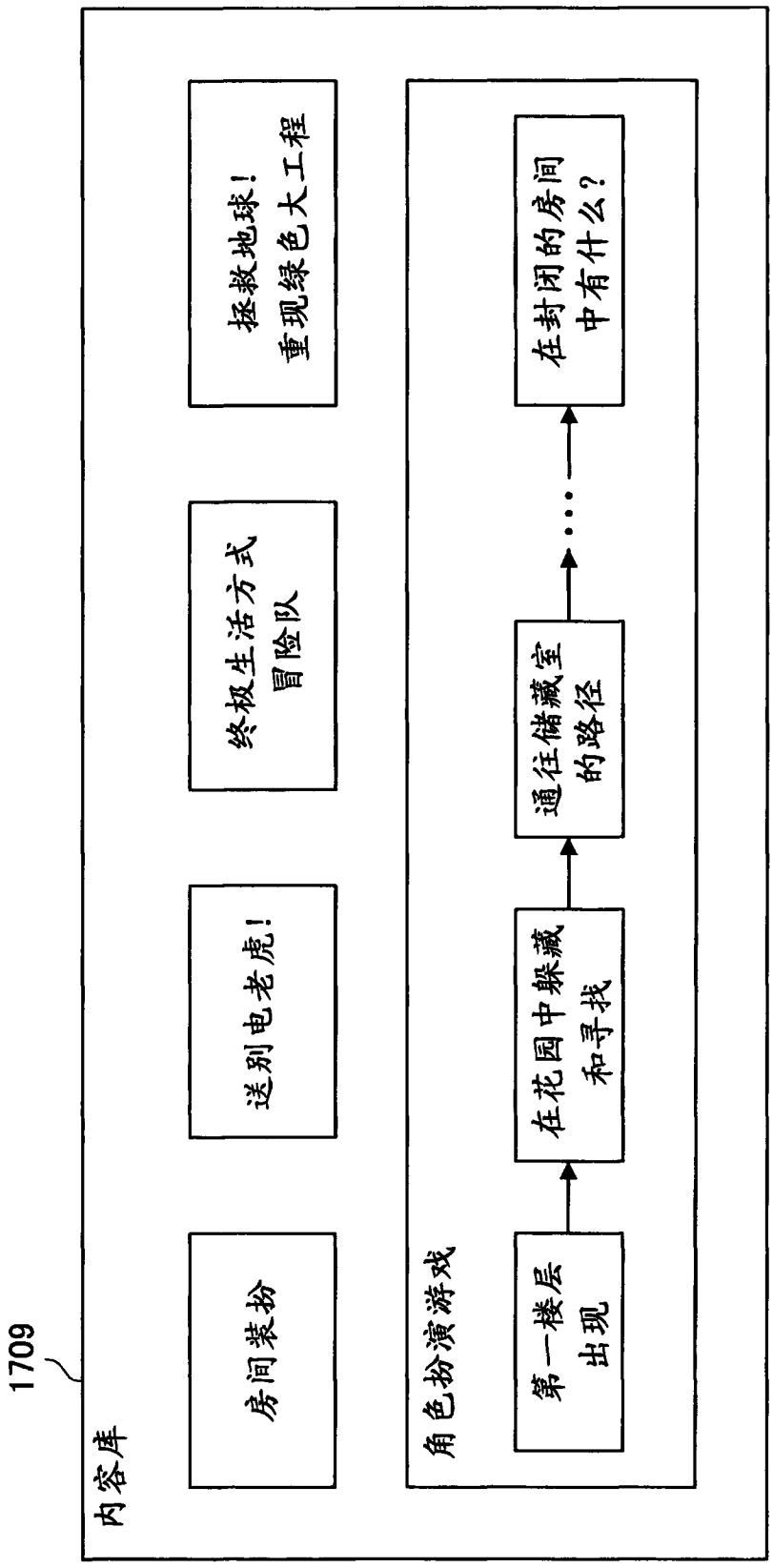

1709
内容库
房间装扮
送别电老虎!
终极生活方式
冒险队
拯救地球!
重现绿色大工程
角色扮演游戏
第一楼层
出现
在花园中躲藏
和寻找
通往储藏室
的路径
在封闭的房间
中有什么?

图 77

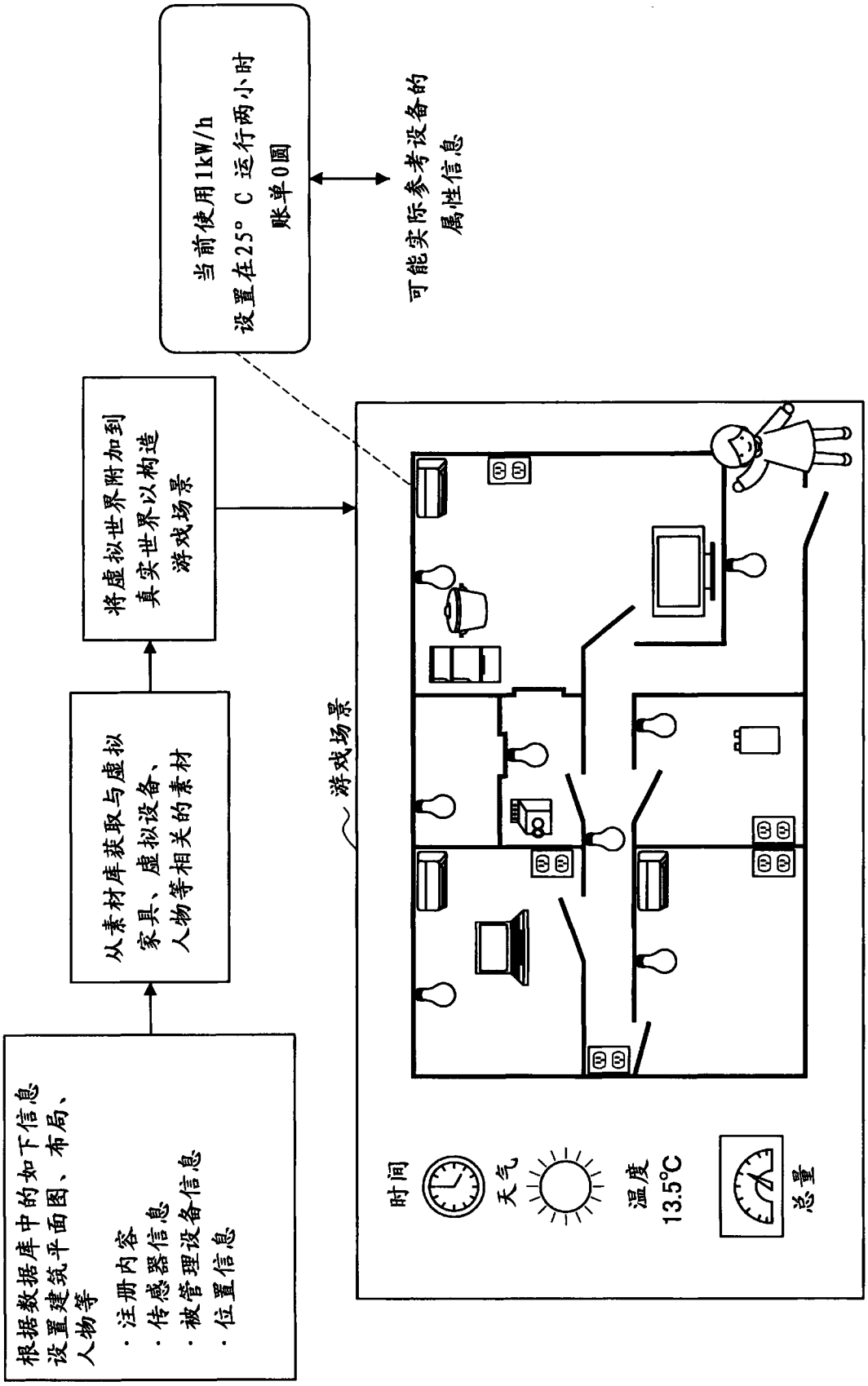

根据数据库中的如下信息
设置建筑平面图、布局、
人物等
·注册内容
·传感器信息
·被管理设备信息
·位置信息
从素材库获取与虚拟
家具、虚拟设备、
人物等相关的素材
将虚拟世界附加到
真实世界以构造
游戏场景
游戏场景
当前使用1kW/h
设置在25° C 运行两小时
账单0圆
可能实际参考设备的
属性信息
时间
天气
温度
13.5°C
总量

图 78

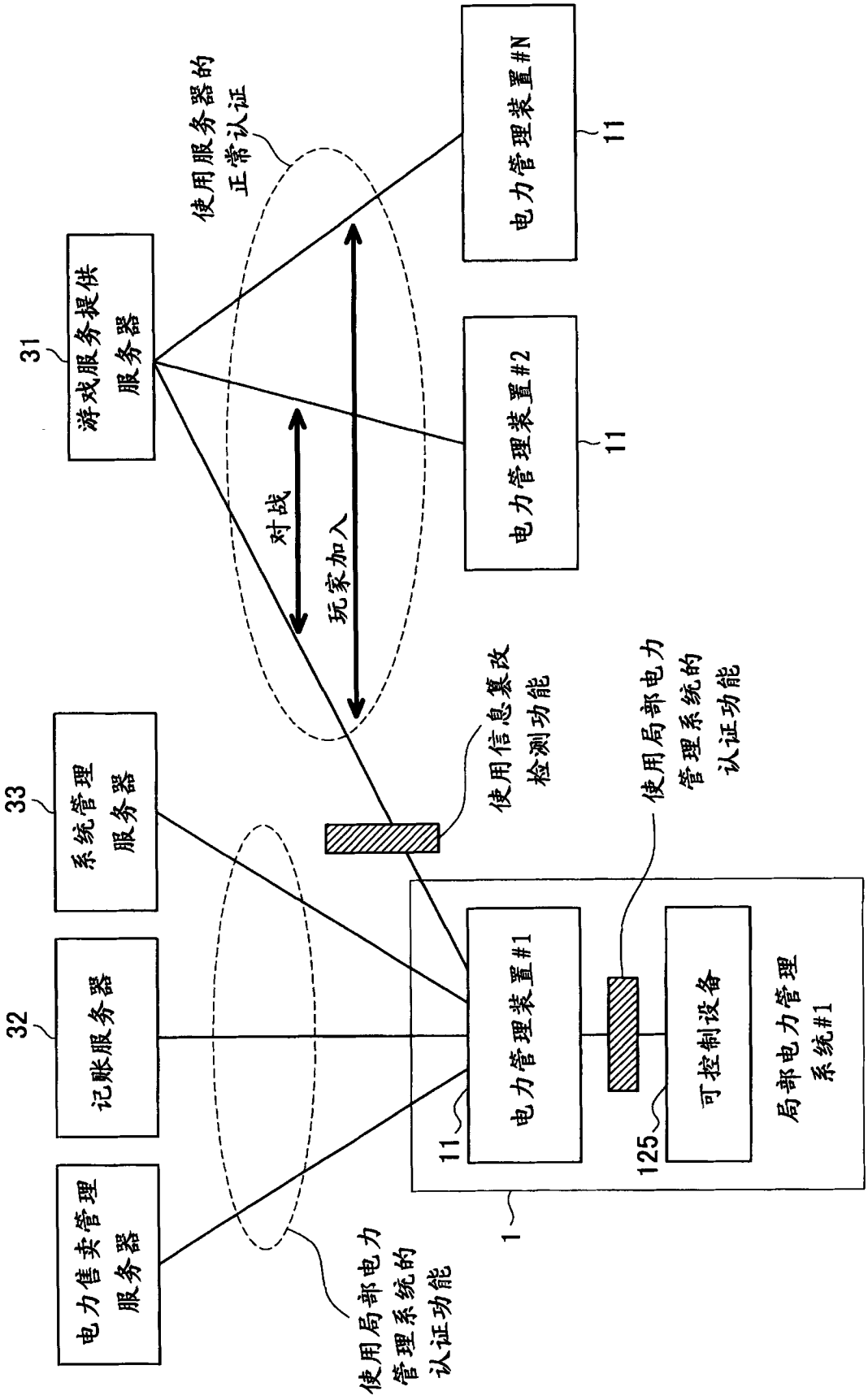

游戏服务提供服务器
31
使用服务器的正常认证
电力管理装置#N
11
电力管理装置#2
11
对战
玩家加入
使用信息篡改检测功能
使用局部电力管理系统的认证功能
系统管理服务器
33
记账服务器
32
电力售卖管理服务器
使用局部电力管理系统的认证功能
电力管理装置#1
11
可控制设备
125
局部电力管理系统#1
1

图 79

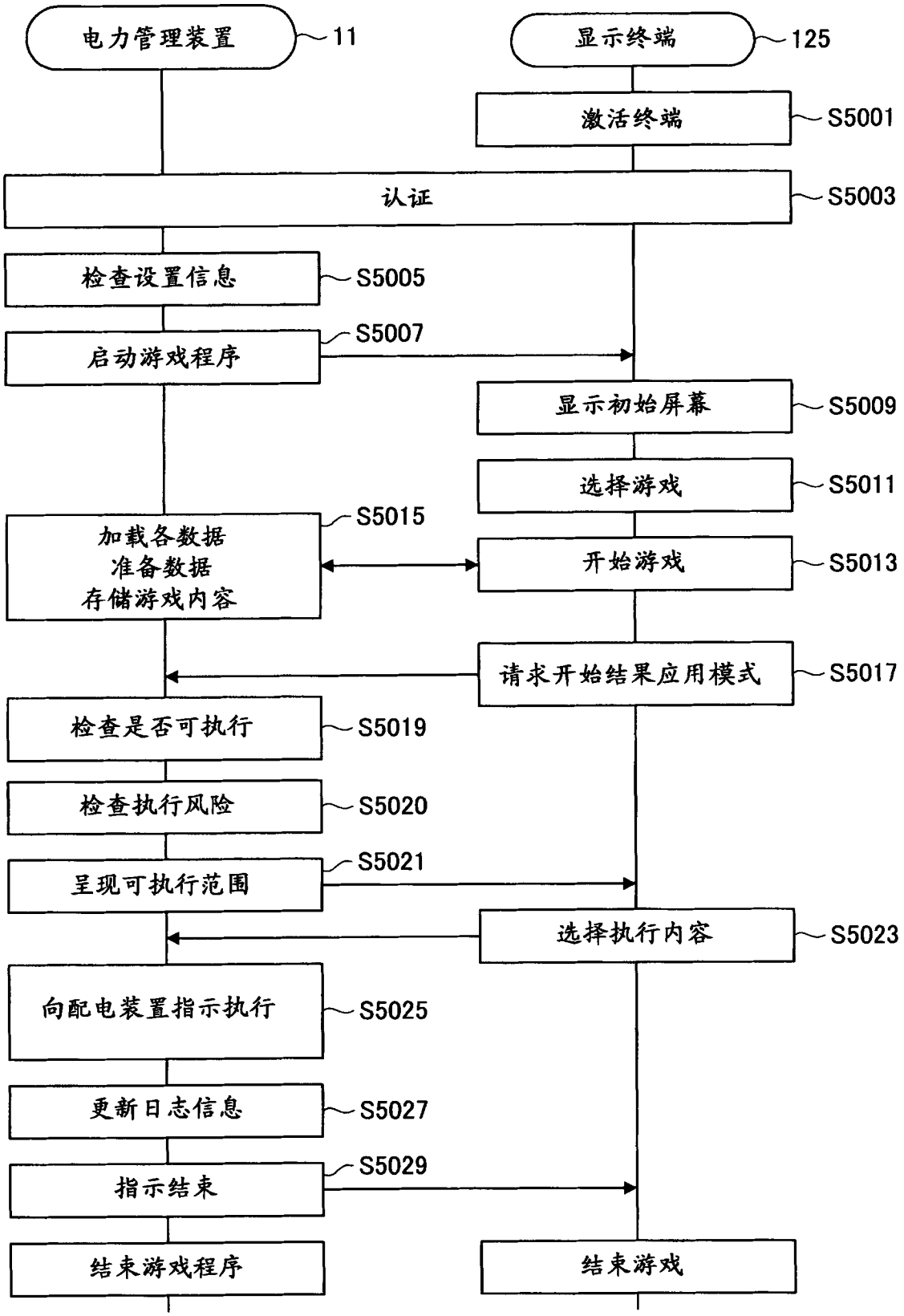

电力管理装置
11
显示终端
125
激活终端
S5001
认证
S5003
检查设置信息
S5005
启动游戏程序
S5007
显示初始屏幕
S5009
选择游戏
S5011
加载各数据
准备数据
存储游戏内容
S5015
开始游戏
S5013
请求开始结果应用模式
S5017
检查是否可执行
S5019
检查执行风险
S5020
呈现可执行范围
S5021
选择执行内容
S5023
向配电装置指示执行
S5025
更新日志信息
S5027
指示结束
S5029
结束游戏程序
结束游戏

图 80

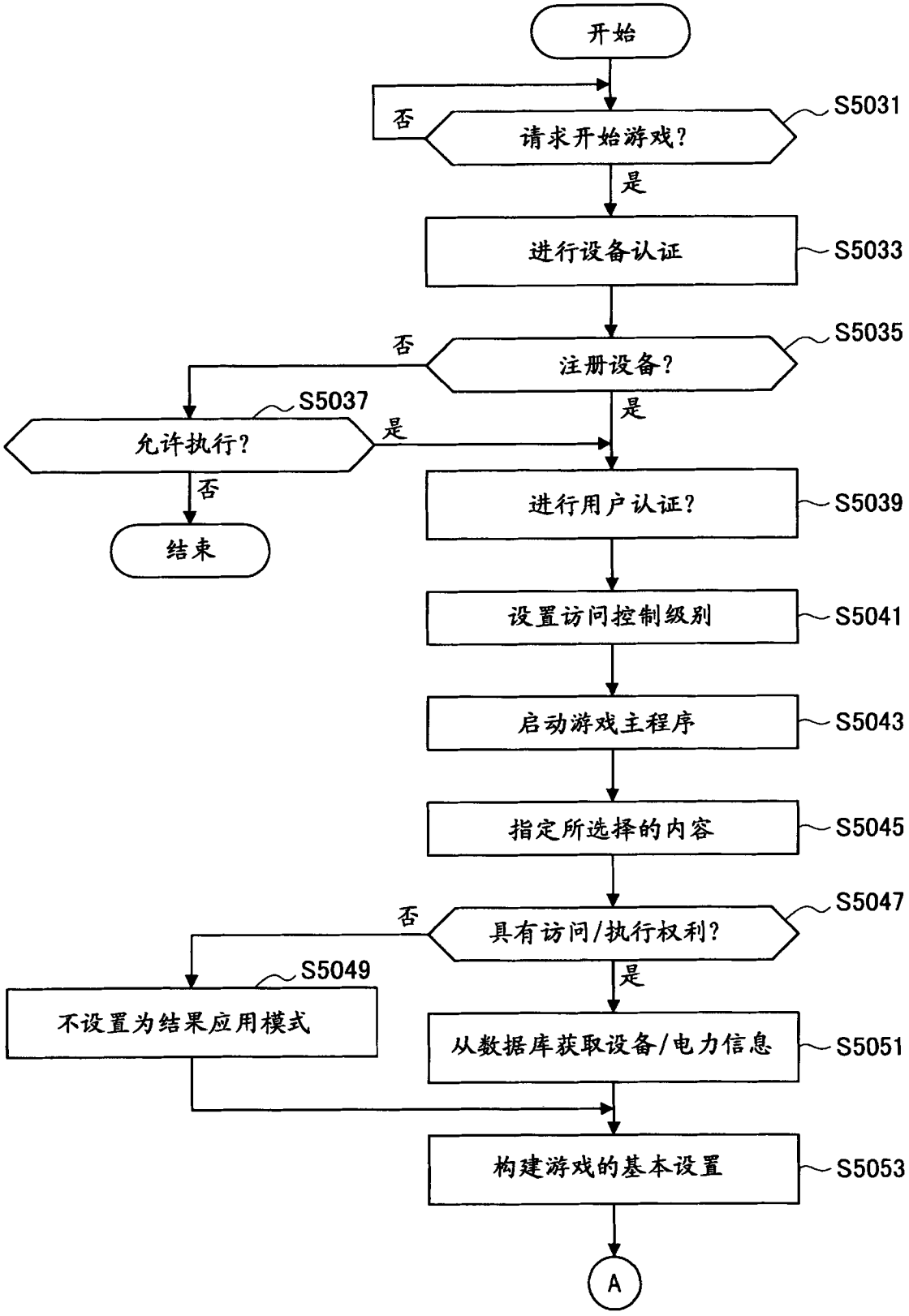

开始
否
请求开始游戏?
S5031
是
进行设备认证
S5033
否
注册设备?
S5035
是
S5037
允许执行?
是
否
结束
进行用户认证?
S5039
设置访问控制级别
S5041
启动游戏主程序
S5043
指定所选择的内容
S5045
否
具有访问/执行权利?
S5047
是
S5049
不设置为结果应用模式
从数据库获取设备/电力信息
S5051
构建游戏的基本设置
S5053
A

图 81A

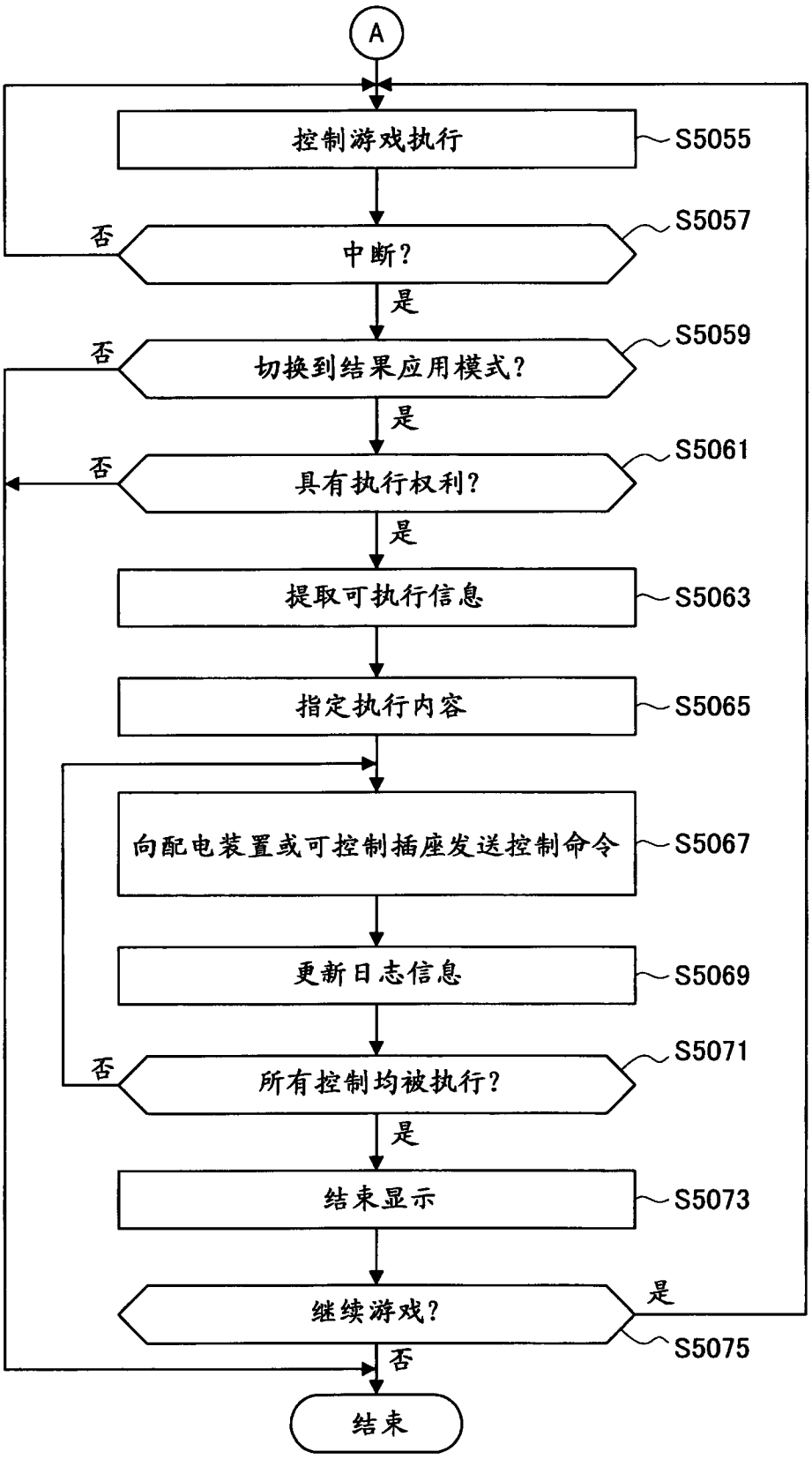

A
控制游戏执行
S5055
中断?
S5057
否
是
切换到结果应用模式?
S5059
否
是
具有执行权利?
S5061
否
是
提取可执行信息
S5063
指定执行内容
S5065
向配电装置或可控制插座发送控制命令
S5067
更新日志信息
S5069
所有控制均被执行?
S5071
否
是
结束显示
S5073
继续游戏?
S5075
是
否
结束

图 81B

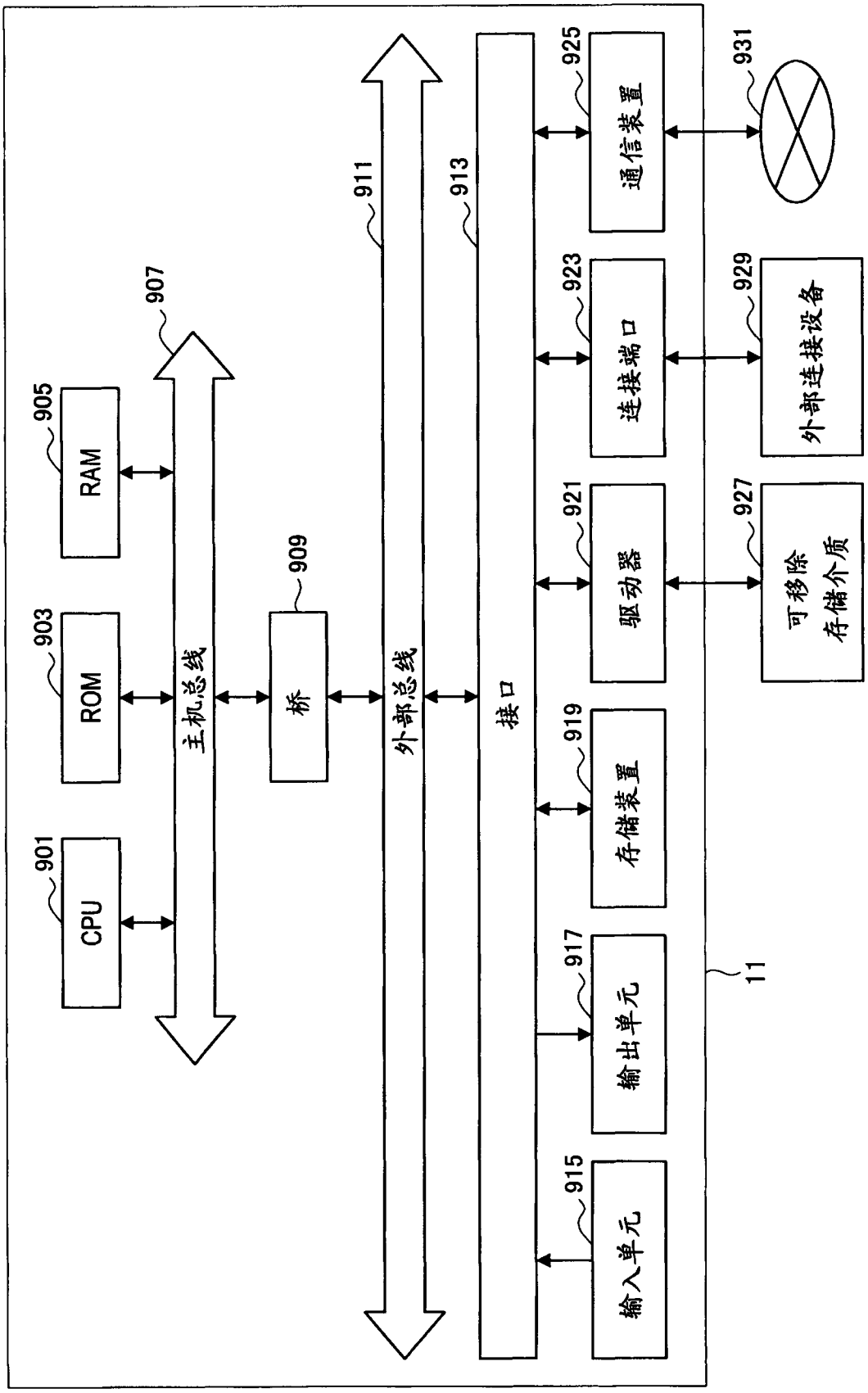

CPU
901
ROM
903
RAM
905
主机总线
907
桥
909
外部总线
911
接口
913
输入单元
915
输出单元
917
存储装置
919
驱动器
921
连接端口
923
通信装置
925
可移除存储介质
927
外部连接设备
929
931
11

图 82