(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 110959269 A
(43)申请公布日 2020.04.03

(21)申请号 201880048105.0

(22)申请日 2018.08.01

(30)优先权数据
2017-154765 2017.08.09 JP

(85)PCT国际申请进入国家阶段日
2020.01.19

(86)PCT国际申请的申请数据
PCT/JP2018/028827 2018.08.01

(87)PCT国际申请的公布数据
WO2019/031344 JA 2019.02.14

(71)申请人 欧姆龙健康医疗事业株式会社
地址 日本京都
申请人 欧姆龙株式会社

(72)发明人 久保诚雄 出野徹 近藤秀规

(74)专利代理机构 北京信慧永光知识产权代理有限责任公司 11290
代理人 鹿屹 李雪春

(51)Int.Cl.
H04L 9/08(2006.01)
G06F 21/60(2006.01)

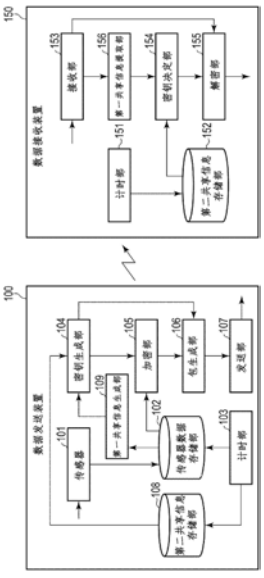
权利要求书2页 说明书18页 附图8页

(54)发明名称

数据发送装置、数据接收装置、方法和程序

(57)摘要

本发明提供数据发送装置、数据接收装置、方法和程序。利用单向通信而发送的数据不容易发生泄漏。数据发送装置包括：测定控制部，测定与生物的信息相关的量；密钥生成控制部，将根据能够与接收装置之间共享的第一共享信息和第二共享信息而算出的信息生成为密钥；加密控制部，使用第一共享信息和密钥对生物的信息进行加密来生成加密数据；包生成控制部，生成包含加密数据的单向发送用的包；以及发送部，发送包。



CN 110959269 A

1.一种数据发送装置,其特征在于,包括:

测定控制部,测定与生物的信息相关的量;

密钥生成控制部,将根据能够与接收装置之间共享的第一共享信息和第二共享信息而算出的信息生成为密钥;

加密控制部,使用所述密钥对所述生物的信息进行加密来生成加密数据;

包生成控制部,生成包含所述第一共享信息和所述加密数据的单向发送用的包;以及

发送部,发送所述包。

2.根据权利要求1所述的数据发送装置,其特征在于,所述第一共享信息、第二共享信息和算出的所述信息不包含所述生物的信息。

3.根据权利要求2所述的数据发送装置,其特征在于,所述密钥生成控制部使所述第一共享信息与日期和时间相对应,并且使所述第二共享信息与预先设定的日期和时间相对应。

4.根据权利要求3所述的数据发送装置,其特征在于,与所述第一共享信息相对应的日期和时间包含测定与所述生物的信息相关的量的日期和时间。

5.根据权利要求3或4所述的数据发送装置,其特征在于,根据所述第一共享信息和第二共享信息而算出的信息包含从由第二共享信息决定的日期和时间到与所述第一共享信息相对应的日期和时间的经过期间。

6.根据权利要求1至5中任意一项所述的数据发送装置,其特征在于,所述生物的信息包含血压值和脉搏中的至少一个。

7.一种数据接收装置,其特征在于,包括:

接收部,接收单向发送用的包,所述单向发送用的包中含有作为被加密的数据的加密数据和能够与发送装置之间共享的第一共享信息;

密钥决定控制部,将基于所述第一共享信息并根据与发送装置之间共享的第二共享信息而算出的信息决定为密钥;以及

解密控制部,使用所述密钥对所述包中所含的加密数据进行解密来生成解密数据,

所述解密数据包含由所述发送装置测定的生物的信息。

8.根据权利要求7所述的数据接收装置,其特征在于,所述第一共享信息、第二共享信息和算出的所述信息不包含所述生物的信息。

9.根据权利要求7或8所述的数据接收装置,其特征在于,

所述第一共享信息是由所述发送装置测定与所述生物的信息相关的量的日期和时间,

所述密钥决定控制部基于测定与所述生物的信息相关的量的日期和时间,并根据所述第二共享信息来决定所述密钥。

10.根据权利要求9所述的数据接收装置,其特征在于,根据所述第一共享信息和第二共享信息而算出的信息包含从由第二共享信息决定的日期和时间到与第一共享信息相对应的日期和时间的经过期间。

11.根据权利要求7至9中任意一项所述的数据接收装置,其特征在于,所述生物的信息包含血压值和脉搏中的至少一个。

12.一种数据发送方法,其特征在于,包括:

测定与生物的信息相关的量;

将根据能够与接收装置之间共享的第一共享信息和第二共享信息而算出的信息生成为密钥；

使用所述密钥对所述生物的信息进行加密来生成加密数据；

生成包含所述第一共享信息和所述加密数据的单向发送用的包；以及

发送所述包。

13.一种数据接收方法，其特征在于，包括：

接收单向发送用的包，所述单向发送用的包中含有作为被加密的数据的加密数据和能够与发送装置之间共享的第一共享信息；

将基于所述第一共享信息并根据与发送装置之间共享的第二共享信息而算出的信息决定为密钥；以及

使用所述密钥对所述包中所含的加密数据进行解密来生成解密数据，

所述解密数据包含由所述发送装置测定的生物的信息。

14.一种程序，其特征在于，用于使计算机作为权利要求1至6中任意一项所述的数据发送装置所包括的各控制部发挥功能。

15.一种程序，其特征在于，用于使计算机作为权利要求7至11中任意一项所述的数据接收装置所包括的各控制部发挥功能。

数据发送装置、数据接收装置、方法和程序

技术领域

[0001] 本发明涉及利用单向通信的数据发送装置、数据接收装置、方法和程序。

背景技术

[0002] 具备将血压数据转送到用户的便携信息终端的功能的血压计已投入市场。便携信息终端例如使用智能手机、平板型终端、笔记本型个人计算机。如果利用上述功能，则用户能够在便携信息终端中一览各种状况下的自己的血压测定结果。此外，典型的例子中，血压数据的转送使用近距离无线通信技术、特别是Bluetooth(蓝牙;注册商标)技术。一般来说，Bluetooth的通信(连接)与WLAN(Wireless Local Area Network:无线局域网)通信相比，能够小规模且省电地实现。Bluetooth规格的版本4.0也被称为BLE(Bluetooth Low Energy:蓝牙低能耗)，与以往的规格相比能够进一步减少耗电。

[0003] 在BLE中能够进行被称为连接的双向通信。但是，连接存在如下问题:为了配对而由用户进行的操作繁琐;配对后的通信步骤繁琐;便携信息终端侧需要支持BLE;不仅便携信息终端需要高性能的硬件(处理器、存储器)，而且血压计也需要高性能的硬件(处理器、存储器);开发和/或评价成本高;以及通信的开销量大而不适合小容量的数据发送等。

[0004] 另一方面，在BLE中也能够进行被称为广播的单向通信。在日本专利公报第5852620号中公开了以下的技术:在广播包的数据字段的空余部分包含任意的数据进行发送。

[0005] 如果利用广播来发送血压数据，则不需要配对以及之后的繁琐的通信步骤，因此，上述问题被消除或减轻。但是，如果例如血压计仅安装有单向发送功能，则不能从便携信息终端向血压计发送控制数据并进行控制、或者不能相反地从血压计参照便携信息终端的状态(数据的接收状况等)。

[0006] 一般来说，从血压计无线发送的数据根据其电波的传播状况，也能够由用户的便携信息终端以外的数据接收装置接收。此时，假设血压数据未被加密地发送，则用户的血压数据有可能被他人看到。期望预防这样的示出用户的健康状态的信息的泄漏，来提高血压数据的转送功能的安全性。此外，如上所述，如果例如血压计仅安装有单向发送功能，则血压计不能参照便携信息终端中的数据的接收状况，因此有可能以必要以上的较大的功率发送包，以便不会发生便携信息终端中的数据缺失。在这种情况下，示出用户的健康状态的信息更容易泄漏。

发明内容

[0007] 本发明是着眼于上述情况而完成的，其目的在于提供利用单向通信而发送的数据不容易发生泄漏的数据发送装置、数据接收装置、方法和程序。

[0008] 为了解决上述课题，本发明采用以下构成。

[0009] 即，本发明的一方面的数据发送装置包括:测定控制部，测定与生物的信息相关的量;密钥生成控制部，将根据能够与接收装置之间共享的第一共享信息和第二共享信息而

算出的信息生成为密钥;加密控制部,使用所述密钥对所述生物的信息进行加密来生成加密数据;包生成控制部,生成包含所述第一共享信息和所述加密数据的单向发送用的包;以及发送部,发送所述包。

[0010] 在上述的构成中,将根据能够与接收装置之间共享的第一共享信息和第二共享信息而算出的信息作为密钥,对所希望的信息(例如生物的信息,以下也称为“生物信息”)进行加密。例如,在接收装置和发送装置中预先保存相同的第二共享信息(例如任意的相同数值(初始值)),并且在数据发送装置和数据接收装置之间共享第一共享信息(例如与可数值化的事件相关的数值(事件数值)),在上述情况下,将该第一共享信息和第二共享信息作为输入并实施运算而得到的输出值成为密钥。该运算例如只要是输入值与输出值对应的运算,则可以是任意的运算。理想的是,可以采用输入值与输出值一一对应的运算。在这种情况下,针对输入值唯一地决定输出值,此外,相反地针对输出值也唯一地决定输入值。但是,即使不是一对一的运算,只要针对输入值使输出值的分布适度地离散即可。即,即使输入值不同,输出值也可以是相同值(例如不完美的散列函数)。当然也可以将完美的散列函数用于运算来得到输出值。

[0011] 此外,虽然输入值根据第一共享信息和第二共享信息来决定,但是第一共享信息和第二共享信息也可以利用同样的运算来决定输入值。从安全的角度考虑,优选输出密钥的运算和输出输入值的运算不同。

[0012] 使用该密钥来生成加密数据,使单向发送用的包中含有加密数据和第一共享信息并单向发送包。即,包仅从数据发送装置发送,该装置不接收包。如上所述,使用将第一共享信息和第二共享信息作为输入而运算出的密钥,对所希望的信息进行加密并发送,因此可以提供能够实现隐匿性优异的发送的数据发送装置。另外,加密的方式采用共享密钥加密方式,但是具体的加密方式没有特别限定。

[0013] 在上述一个方面的数据发送装置中,所述第一共享信息、第二共享信息和算出的所述信息不包含所述生物的信息。

[0014] 在上述构成中,为了在数据发送装置和数据接收装置中根据第一共享信息、第二共享信息和算出的所述信息来生成通用的密钥,在各装置中不将传感器的生物信息用于生成密钥,因此生物不需要始终佩戴数据发送装置和数据接收装置,或者携带装置。因此,只要仅将数据发送装置佩戴于生物,就能够取得想要从数据发送装置发送的生物信息,并对该生物信息进行加密而发送到数据接收装置。

[0015] 在上述一个方面的数据发送装置中,所述密钥生成控制部使所述第一共享信息与日期和时间相对应,并且使所述第二共享信息与预先设定的日期和时间相对应。

[0016] 在上述构成中,使第一共享信息与日期和时间相对应,并且将其包含于包而发送到数据接收装置,因此能够在数据发送装置和数据接收装置中共享该第一共享信息。由此,能够将根据第二共享信息(例如在接收装置和发送装置中预先共享的任意的相同的日期和时间)和第一共享信息(例如测定与生物信息相关的量的日期和时间)而算出的信息(例如这些日期和时间的时间差(也称为经过时间或经过期间))作为密钥。另外,该日期和时间不仅可以是由数据发送装置测定生物信息的日期和时间,也可以是任意的时刻(可以是未来,也可以是过去)。此外,不仅仅限于时刻,也可以是包含年月日的日期和时间信息。另外,时刻被视为也包含与日期相关的信息,以与日期和时间信息相同的含义来使用。

[0017] 在上述一个方面的数据发送装置中，与所述第一共享信息相对应的日期和时间包含测定与所述生物的信息相关的量的日期和时间。

[0018] 在上述构成中，例如将在接收装置和发送装置中预先根据任意的相同时刻(第二共享信息)以及测定与生物信息相关的量的日期和时间(第一共享信息)而算出的信息作为共享信息，能够利用预定的运算来生成密钥。

[0019] 在上述一个方面的数据发送装置中，根据所述第一共享信息和第二共享信息而算出的信息包含从由第二共享信息决定的日期和时间到与所述第一共享信息相对应的日期和时间的经过期间。

[0020] 在上述构成中，将经过期间作为密钥，该经过期间是根据在接收装置和发送装置中预先根据任意的相同的日期和时间(第二共享信息)以及测定与生物信息相关的量的日期和时间(第一共享信息)而算出的这些日期和时间的时间差。因此，可以使用仅在数据发送装置和数据接收装置之间通用的密钥而对任意的数据(例如生物信息)进行加密。

[0021] 在上述一个方面的数据发送装置中，所述生物的信息包含血压值和脉搏中的至少一个。

[0022] 在上述构成中，数据发送装置能够基于第一共享信息和第二共享信息而使用密钥来发送生物信息。在此，生物信息通常是包含取得日期和时间的血压值和/或脉搏亦即时间序列数据。因此，可以提供能够安全地发送所希望的生物信息的数据发送装置。

[0023] 上述一个方面的数据接收装置包括：接收部，接收单向发送用的包，所述单向发送用的包中含有作为被加密的数据的加密数据和能够与发送装置之间共享的第一共享信息；密钥决定控制部，将基于所述第一共享信息并根据与发送装置之间共享的第二共享信息而算出的信息决定为密钥；以及解密控制部，使用所述密钥对所述包中所含的加密数据进行解密来生成解密数据，所述解密数据包含由所述发送装置测定的生物的信息。

[0024] 在上述构成中，将根据能够与数据发送装置之间共享的第一共享信息和第二共享信息而算出的信息作为密钥，对所希望的信息(例如生物信息)进行加密。例如，第一共享信息和第二共享信息是数值，在接收装置和发送装置中预先存储任意的相同初始值(第二共享信息)，并且发送与可数值化的事件相关的事件数值(第一共享信息)，由此能够在数据发送装置和数据接收装置之间共享第一共享信息和第二共享信息。无论是数据发送装置还是数据接收装置都利用根据第一共享信息和第二共享信息决定的运算来生成密钥，由此数据接收装置能够利用该密钥安全地进行接收，能够对加密数据进行解密而得到所希望的生物信息。

[0025] 在上述一个方面的数据接收装置中，所述第一共享信息、第二共享信息和算出的所述信息不包含所述生物的信息。

[0026] 在上述构成中，为了生成与数据发送装置之间通用的密钥，在各装置中不将传感器的生物信息用于生成密钥。因此，由于数据接收装置不需要采用使用了生物信息的密钥，所以数据接收装置的使用形态多种多样。例如，不需要将数据接收装置始终佩戴于生物或携带装置。其结果，数据接收装置保持设置在自己家中等状态下也能够进行加密数据的收发。

[0027] 在上述一个方面的数据接收装置中，所述第一共享信息是由所述发送装置测定与所述生物的信息相关的量的日期和时间，所述密钥决定控制部基于测定与所述生物的信息

相关的量的日期和时间，并根据所述第二共享信息来决定所述密钥。

[0028] 在上述构成中，使由发送装置测定与所述生物信息相关的量的日期和时间包含于包并由数据接收装置接收，因此能够在数据发送装置和数据接收装置中共享该日期和时间。例如，能够将在接收装置和发送装置中预先根据任意的相同的日期和时间(第二共享信息)以及测定与生物信息相关的量的日期和时间(第一共享信息)而算出的信息(例如这些日期和时间的时间差亦即经过期间)作为密钥。另外，该日期和时间不仅可以是数据发送装置测定与生物信息相关的量的日期和时间，也可以是任意的时刻(可以是未来，也可以是过去)。此外，不仅仅限于时刻，也可以是包含年月日的日期和时间信息。另外，时刻被视为也包含与日期相关的信息，以与日期和时间信息相同的含义来使用。

[0029] 在上述一个方面的数据接收装置中，根据所述第一共享信息和第二共享信息而算出的信息包含从由第二共享信息决定的日期和时间到与第一共享信息相对应的日期和时间的经过期间。

[0030] 在上述构成中，将从接收装置和发送装置预先共享的日期和时间(第二共享信息)到测定与生物信息相关的量的日期和时间(第一共享信息)的经过期间作为密钥。由于该经过期间只能在数据接收装置和数据发送装置之间得知，所以可以提供能够安全地交接生物信息的数据接收装置。

[0031] 在上述一个方面的数据接收装置中，所述生物的信息包含血压值和脉搏中的至少一个。

[0032] 在上述构成中，解密数据是数据发送装置的传感器取得的生物信息，例如是血压值和/或脉搏。数据接收装置能够将基于第一共享信息和第二共享信息生成的信息用作密钥而对生物信息进行解密。在此，生物信息通常是包含取得日期和时间的血压值和/或脉搏亦即时间序列数据。因此，可以提供能够安全地对所希望的生物信息进行解密的数据接收装置。

[0033] 上述一个方面的所述数据发送装置是血压计或脉搏计，所述数据接收装置是便携信息终端。

[0034] 在上述构成中，发送由血压计或脉搏计测定的生物信息，并且便携信息终端能够安全地接收该生物信息。

[0035] 上述一个方面的数据发送装置中生成的包采用近距离无线通信方式发送。

[0036] 在上述构成中，从数据发送装置朝向数据接收装置的发送按照近距离无线通信方式(例如BLE)，由此与其他无线通信方式相比，能够利用低耗电且廉价的设备实现发送。

[0037] 按照本发明，可以提供一种利用单向通信发送的数据能够不容易发生泄漏的数据发送装置、数据接收装置、方法和程序。

附图说明

[0038] 图1是示意性例示实施方式的数据发送装置和数据接收装置的应用场景的一例的图。

[0039] 图2是示意性例示实施方式的数据发送装置的硬件构成的一例的图。

[0040] 图3是示意性例示实施方式的数据接收装置的硬件构成的一例的图。

[0041] 图4是示意性例示实施方式的数据发送装置的软件构成的一例的图。

[0042] 图5是示意性例示实施方式的数据接收装置的软件构成的一例的图。

[0043] 图6是例示实施方式的数据发送装置的处理步骤的一例的图。

[0044] 图7是例示实施方式的数据接收装置的处理步骤的一例的图。

[0045] 图8是在BLE中进行的广播的说明图。

[0046] 图9是例示在BLE中收发的包的数据结构的图。

[0047] 图10是例示广播包的PDU字段的数据结构的图。

[0048] 图11是表示在实施方式的数据发送装置发送的包的PDU字段的净荷中储存的数据结构的一例的图。

[0049] 图12是例示包含实施方式的数据发送装置和数据接收装置的数据传送系统的一例的图。

具体实施方式

[0050] 下面，基于附图对本发明的一个方面的实施方式(以下也记载为“本实施方式”)进行说明。另外，在以下的实施方式中，标注了相同的附图标记的部分进行相同的动作，省略重复的说明。

[0051] [应用示例]

[0052] 首先，利用图1对应用本发明的场景的一例进行说明。图1示意性例示本实施方式的数据发送装置100和数据接收装置150的应用场景的一例。本实施方式的数据发送装置100将时间序列的传感器数据存储于传感器数据存储部102，该时间序列的传感器数据将由传感器101从生物取得的传感器数据与计时部103的时刻相对应。第一共享信息生成部109从传感器数据存储部102生成第一共享信息，密钥生成部104从第二共享信息存储部108取得第二共享信息。并且，密钥生成部104基于数据发送装置100和数据接收装置150的第一共享信息和第二共享信息来生成密钥，加密部105利用该密钥对从传感器数据存储部102取得的想要发送的所希望的数据(例如生物信息)进行加密。接着，包生成部106生成包含第一共享信息和加密数据的包，并且发送部107发送所生成的单向发送用的包(例如使用BLE的广播)。另外，密钥生成部104相当于本发明的“密钥生成控制部”，加密部105相当于本发明的“加密控制部”。第一共享信息例如是由传感器取得(或检测)传感器数据的日期和时间，第二共享信息例如是预先在数据发送装置与数据接收装置之间共享的日期和时间。更准确地说，由传感器取得(或测定、检测)传感器数据的日期和时间是由传感器取得(或测定、检测)成为传感器数据源的生物信息的日期和时间，但是为了便于说明，在以下的说明和权利要求书中以相同的意思使用。优选的是，用户能够任意地设定第二共享信息。其结果，即使具有多个数据发送装置和数据接收装置，也降低了生成相同的密钥的可能性。因此，即使不应当进行解密的任意的数据接收装置接收到第一共享信息，也降低了数据接收装置能够对加密数据进行解密的可能性。

[0053] 在本实施方式的数据接收装置150中，接收部153接收单向发送用的包，密钥决定部154基于由第一共享信息提取部156从包中提取的第一共享信息(例如由传感器取得传感器数据的日期和时间数据)和包含于第二共享信息存储部152的信息，生成并决定密钥。在第二共享信息存储部152中存储有数据接收装置和数据发送装置的第二共享信息(例如预先存储有任意的相同数值(初始值；例如时刻等))。解密部155使用由密钥决定部154生成的

密钥,对由接收部153接收的加密数据进行解密,数据接收装置能够接收在数据发送装置中取得的所希望的数据。在赋予日期和时间数据作为与储存于第二共享信息存储部152的第二共享信息相关联的信息时使用计时部151。作为单纯的例子,在用户使用输入装置将某个所希望的时刻数据记录于第二共享信息存储部152时使用计时部151。

[0054] 从数据发送装置朝向数据接收装置的单向通信方式例如是BLE的广播。利用该通信方式生成单向发送用的包。此外,在本实施方式中发送的所希望的数据例如是生物信息,具体地说,例如是血压值和/或脉搏。传感器数据只要是能够由传感器101检测的数据,则可以是任意的数据,例如是步数和/或三轴加速度。此外,如果能够由传感器检测,则也可以是血压值和/或脉搏等生物信息。此外,加密的方式采用共享密钥加密方式(common key cryptosystem),但是具体的加密方式没有特别限定,例如使用DES(Data Encryption Standard:数据加密标准)或AES(Advanced Encryption Standard高级加密标准)。此外,例如数据发送装置是血压计或脉搏计,数据接收装置是智能手机、便携电话或移动个人计算机等便携信息终端。

[0055] 如上所述,在本实施方式中,数据发送装置100利用根据数据发送装置100生成的第一共享信息以及接收装置和发送装置预先共享的第二共享信息而算出的密钥,对所希望的生物信息进行加密,生成单向发送用的包并发送。数据接收装置150将基于数据发送装置100发送的包中所含的第一共享信息以及接收装置和发送装置预先共享的第二共享信息(例如任意的相同数值)而算出的信息作为密钥,对加密数据进行解密。因此,在数据接收装置150中,能够得到与数据发送装置100相同的第一共享信息和第二共享信息,并且生成根据这些共享信息而算出的密钥。该密钥在数据发送装置100和数据接收装置150中相同。即,在数据发送装置100和数据接收装置150双方中,能够设定基于共享信息而算出的密钥,该共享信息包含由数据发送装置100生成的第一共享信息和预先共享的第二共享信息。因此,按照本实施方式,使用数据发送装置100生成的第一共享信息以及接收装置和发送装置预先共享的第二共享信息(任意的相同数值),在发送侧和接收侧分别生成密钥,由此能够安全地发送单向发送用的包来传递信息。其结果,相比于仅利用与第二共享信息对应的通用密钥的加密方式,第一共享信息对密钥的内容产生影响,因此本实施方式的方式能够安全地传递信息。

[0056] [构成示例]

[0057] (硬件构成)

[0058] <数据发送装置>

[0059] 接着,利用图2,说明本实施方式的数据发送装置100的硬件构成的一例。

[0060] 如图2所示,本实施方式的数据发送装置100包括输出装置211、输入装置212、控制部213、存储部214、驱动器215、外部接口216、通信接口217和电池218电连接而成的计算机。此外,数据发送装置100包括生物传感器219和计时装置220。本实施方式的数据发送装置100相当于本发明的“数据发送装置”。另外,在图2中,通信接口和外部接口分别记载为“通信I/F”和“外部I/F”。

[0061] 控制部213包括:CPU(Central Processing Unit:中央处理器)、RAM(Random Access Memory:随机存取存储器)和ROM(Read Only Memory:只读存储器)等,根据信息处理进行各构成要素的控制。存储部214例如是硬盘驱动器、固态驱动器等辅助存储装置,存

储由控制部213执行的密钥生成和包发送控制程序、由生物传感器219检测到的传感器数据、预定发送的所希望的数据、第二共享信息、以及由计时装置220计时的日期和时间数据等。

[0062] 密钥生成和包发送控制程序是如下的程序:用于根据第一共享信息和第二共享信息生成密钥,并使用所生成的密钥对所希望的数据进行加密,执行由单向发送用的包发送第一共享信息和被加密的数据的处理(图6)。此外,所希望的数据例如是生物信息。生物信息例如是血压值的时间序列数据。

[0063] 通信接口217例如是近距离无线通信(例如蓝牙(注册商标))模块、无线LAN模块等,是用于进行经由网络的无线通信的接口。通信接口217是用于使数据发送装置100与数据接收装置150无线连接的接口。通信接口217由控制部213控制。通信接口217用于接收包含由控制部213生成的加密数据的包,并将该包发送到数据接收装置150。另外,通信接口217不能从数据接收装置150接收信息,而仅仅是发送单向发送用的包。

[0064] 输入装置212例如是鼠标、键盘之类的用于进行输入的装置。输出装置211例如是显示器、扬声器之类的用于进行输出的装置。外部接口216是USB接口等,例如是用于与生物传感器219和/或计时装置220等外部装置进行连接的接口。在图2等中未图示成生物传感器219和计时装置220与外部接口216连接,这是为了后面在图4等中明确它们与控制部213的内部模块的连接,而简便地记载为与控制部213直接连接。

[0065] 存储部214是如下的介质:利用电、磁、光学、机械或化学的作用存储程序等信息,以便计算机及其他装置、设备等可读取记录的程序等信息。数据发送装置100也可以从该存储部214取得密钥生成和包发送控制程序、由生物传感器219检测到的传感器数据、预定发送的所希望的数据、在数据发送装置和数据接收装置之间预先共享的第二共享信息、以及由计时装置220计时的日期和时间数据。

[0066] 驱动器215例如是CD(Compact Disk:光盘)驱动器、DVD(Digital Versatile Disk:数字通用盘)驱动器等,是用于读入存储介质中存储的程序的装置。驱动器215的种类可以根据存储介质的种类来适当选择。上述密钥生成和包发送控制程序、由生物传感器219检测到的传感器数据、预定发送的所希望的数据以及由计时装置220计时的日期和时间数据也可以存储于该存储介质。在此,作为存储介质的一个例子,例示了CD、DVD等盘式存储介质。但是,存储介质的种类并不限定于盘式,也可以是盘式以外的存储介质。盘式以外的存储介质例如可以列举闪存器等半导体存储器。

[0067] 电池218例如是能够充电的二次电池。电池218向搭载于数据发送装置100主体的各要素供电。电池218例如向输出装置211、输入装置212、控制部213、存储部214、驱动器215、外部接口216、通信接口217、生物传感器219和计时装置220供电。

[0068] 生物传感器219例如是血压测定装置。在这种情况下,生物传感器219例如对作为生物的用户的手腕上佩戴的按压袖带的压力进行检测,来检测生物的血压值。生物传感器219将血压数据(例如血压值的时间序列数据)输出到控制部213。此外,生物传感器219也可以是脉搏测定装置,可以与血压一起测定脉搏。

[0069] 计时装置220是计量时间的装置,能够计量日期和时间。例如,计时装置220是包含日历的时钟,将当前的日期和时间的信息传送到控制部213。

[0070] 另外,数据发送装置100的具体硬件构成能够根据实施方式适当地进行构成要素

的省略、替换和追加。例如，控制部213也可以包括多个处理器。数据发送装置100也可以由多台信息处理装置构成。此外，数据发送装置100除了使用针对所提供的服务专用设计的信息处理装置以外，还可以使用通用的台式PC(Personal Computer:个人计算机)和平板PC等。

[0071] <数据接收装置>

[0072] 接着，利用图3，说明本实施方式的数据接收装置150的硬件构成的一例。数据接收装置150的硬件构成与数据发送装置100大体相同。

[0073] 如图3所示，本实施方式的数据接收装置150包括输出装置311、输入装置312、控制部313、存储部314、驱动器315、外部接口316、通信接口317和电池318电连接而成的计算机。此外，数据接收装置150包括计时装置319。本实施方式的数据接收装置150相当于本发明的“数据接收装置”。另外，在图3中将通信接口和外部接口分别记载为“通信I/F”和“外部I/F”。

[0074] 控制部313包括:CPU(Central Processing Unit)、RAM(Random Access Memory)、ROM(Read Only Memory)等，根据信息处理进行各构成要素的控制。存储部314例如是硬盘驱动器、固态驱动器等辅助存储装置，存储由控制部313执行的密钥生成和数据解密控制程序、接收并解密的所希望的数据、在数据发送装置和数据接收装置之间预先共享的第二共享信息、以及由计时装置319计时的日期和时间数据等。

[0075] 密钥生成和数据解密控制程序是如下的程序:用于根据包中所含的第一共享信息和预先共享的第二共享信息来生成密钥，并且使用所生成的密钥，执行对接收到的单向发送用的包中所含的加密数据进行解密的处理(图7)。此外，所希望的数据例如是生物信息。生物信息例如是血压值的时间序列数据。

[0076] 通信接口317与通信接口217大体相同。通信接口317是用于从数据发送装置100接收数据的接口。通信接口317从数据发送装置100接收包并传送到控制部313。

[0077] 输入装置312、输出装置311和外部接口316分别与输入装置212、输出装置211和外部接口216相同。

[0078] 存储部314是如下的介质:利用电、磁、光学、机械或化学的作用来存储程序等信息，以便计算机及其他装置、设备等可读取记录的程序等信息。数据接收装置150也可以从该存储部314取得密钥生成和数据解密控制程序、接收并解密的所希望的数据、在数据发送装置与数据接收装置之间共享的第二共享信息、以及由计时装置319计时的日期和时间数据。

[0079] 驱动器315例如是CD(Compact Disk)驱动器、DVD(Digital Versatile Disk)驱动器等，是用于读入存储介质中存储的程序的装置。驱动器315的种类可以根据存储介质的种类来适当选择。上述密钥生成和数据解密控制程序、由计时装置319和/或动作传感器320检测到的传感器数据、接收并解密的所希望的数据、以及由计时装置319计时的日期和时间数据也可以存储于该存储介质。在此，作为存储介质的一个例子，例示了CD、DVD等盘式存储介质。但是，存储介质的种类并不限定于盘式，也可以是盘式以外的存储介质。盘式以外的存储介质例如可以列举闪存器等半导体存储器。

[0080] 电池318与电池218相同。电池318向搭载于数据接收装置150主体的各要素供电。

[0081] 计时装置319与计时装置220相同。

[0082] 另外，数据接收装置150的具体硬件构成能够根据实施方式适当地进行构成要素的省略、替换和追加。例如，控制部313也可以包括多个处理器。数据接收装置150也可以由多台信息处理装置构成。此外，数据接收装置150除了使用针对所提供的服务专用设计的信息处理装置以外，还可以使用通用的台式PC(Personal Computer)和平板PC等。

[0083] (软件构成)

[0084] <数据发送装置>

[0085] 接着，利用图4，说明本实施方式的数据发送装置100的软件构成的一例。

[0086] 数据发送装置100的控制部213在执行必要的程序时，将存储于存储部214的密钥生成和包发送控制程序在RAM中展开。并且，控制部213利用CPU来解释并执行在RAM中展开的密钥生成和包发送控制程序，控制各构成要素。由此，如图4所示，本实施方式的数据发送装置100作为包括生物信息测定部401、存储控制部402、密钥生成部403、加密部404、包生成部405、发送部406和第一共享信息生成部407的计算机发挥功能。

[0087] 生物信息测定部401将生物传感器219检测生物信息而输出的传感器数据与从计时装置220取得的日期和时间信息一起传送到存储控制部402。此外，生物信息测定部401也可以将组合有该生物信息以及日期和时间信息的生物信息的时间序列数据传送到存储控制部402。

[0088] 存储控制部402把从生物信息测定部401接收到的将传感器数据与日期和时间信息相关联的数据存储于存储部214。此外，存储控制部402也可以从计时装置220取得日期和时间信息，并且将日期和时间信息与其他的接收到的信息相对应地存储于存储部214。

[0089] 第一共享信息生成部407生成与可数值化的事件相关的数值(事件数值)。具体地说，第一共享信息生成部407例如生成由数据发送装置测定与生物信息相关的量的日期和时间信息作为事件数值。

[0090] 密钥生成部403根据由第一共享信息生成部407生成的第一共享信息和存储部214所存储的第二共享信息来生成密钥。共享信息例如是如下的数值(事件数值)：在接收装置和发送装置中预先保存任意的相同数值(初始值)，进而与可数值化的事件相关。具体地说，例如初始值是某个特定的日期和时间信息，在这种情况下，密钥生成部403例如算出从初始值的日期和时间到事件数值的日期和时间的经过期间，并且将该经过期间作为密钥。

[0091] 此外，密钥除了包括共享信息以外，还可以包括预先设定的与数据接收装置150共享的其他数据。例如也可以预先使数据发送装置100的MAC(media access control：介质访问控制)地址包含于密钥。该MAC地址在数据接收装置150中也预先设定为已知。在这种情况下，数据发送装置100的MAC地址预先存储于存储部214和存储部314。

[0092] 加密部404接收存储部214中存储的应当发送的所希望的数据，并且利用从密钥生成部403接收的密钥对所希望的数据进行加密。加密的方式采用共享密钥加密方式，但是具体的加密方式没有特别限定。具体的加密方式例如有DES、AES。

[0093] 包生成部405从密钥生成部403取得与密钥相关的信息，并且生成包含与密钥相关的该信息和由加密部404加密的所希望的数据的包。该包是单向发送用的包，例如是BLE的广播包。此外，与密钥相关的信息例如包含事件数值，该事件数值成为包含于密钥的算出的数值的来源。具体地说，包含于密钥的算出的数值例如是经过期间，事件数值是生成密钥的日期和时间。

[0094] 另外，与密钥相关的信息也可以包含传感器的位置信息。在由密钥对数据进行解密时使用该日期和时间以及位置信息。

[0095] 发送部406将由包生成部405生成的包用于单向发送，并以预定的通信方式经由通信接口217发送。该通信方式例如是BLE，发送部406利用BLE的广播来发送包。

[0096] 〈数据接收装置〉

[0097] 接着，利用图5，说明本实施方式的数据接收装置150的软件构成的一例。

[0098] 数据接收装置150的控制部313在执行必要的程序时，将存储于存储部314的密钥生成和数据解密控制程序在RAM中展开。并且，控制部313利用CPU来解释并执行在RAM中展开的密钥生成和数据解密控制程序，控制各构成要素。由此，如图5所示，本实施方式的数据接收装置150作为包括存储控制部501、接收部502、密钥决定部503、解密部504和第一共享信息提取部505的计算机发挥功能。

[0099] 存储控制部501从计时装置319取得日期和时间信息，并且将日期和时间信息与其他的接收到的信息相对应地存储于存储部314。

[0100] 接收部502经由通信接口317接收来自数据发送装置100的包。在该包中至少包含加密数据和与密钥相关的信息。

[0101] 第一共享信息提取部505提取接收部502接收的包中所含的第一共享信息。第一共享信息例如是在数据发送装置中由传感器测定与生物信息相关的量的日期和时间信息。

[0102] 密钥决定部503取得由第一共享信息提取部505生成的第一共享信息和存储于存储部314的第二共享信息(预先共享的任意的相同数值;初始值、即在接收装置和发送装置中预先共享的任意的相同数值)。包中所含的第一共享信息例如包含与可数值化的事件相关的数值(事件数值)。更具体地说，事件数值例如是传感器测定传感器数据的日期和时间。将包中所含的该事件数值和存储于存储部314的初始值作为输入并实施运算而得到的输出值成为密钥。该运算例如使用(不完美的)散列函数。此外，也可以将完美的散列函数用于运算。

[0103] 此外，在包中还含有MAC地址的情况下，密钥决定部503从存储部314还取得该MAC地址。密钥决定部503确认存储部314中存储的MAC地址是否与接收到的包中所含的MAC地址一致。例如在一致的情况下，密钥决定部503原状继续处理，在不一致的情况下，视为接收方不同而废弃该包。

[0104] 解密部504从接收部502接收加密数据，并且还接收由密钥决定部503生成的密钥。并且，解密部504利用该密钥对加密数据进行解密来接收所希望的数据。解密部504将该所希望的数据存储于存储部314。

[0105] 〈其他〉

[0106] 利用后述的动作示例对数据发送装置100和数据接收装置150的各功能进行详细说明。另外，在本实施方式中，说明了数据发送装置100和数据接收装置150的各功能均由通用的CPU来实现的例子。但是，以上的功能的一部分或全部也可以由一个或多个专用的处理器来实现。此外，关于数据发送装置100的功能构成，也可以根据实施方式适当地进行功能的省略、替换和追加。

[0107] [动作示例]

[0108] 〈数据发送装置〉

[0109] 接着，利用图6对数据发送装置100的动作示例进行说明。图6是例示数据发送装置100的处理步骤的一例的流程图。另外，以下说明的处理步骤仅是一例，各处理可以尽可能地变更。此外，以下说明的处理步骤能够根据实施方式适当地进行步骤的省略、替换和追加。

[0110] (启动)

[0111] 首先，用户启动数据发送装置100，并且使启动的数据发送装置100执行密钥生成和包发送控制程序。数据发送装置100的控制部213按照以下的处理步骤，生成第一共享信息，并且基于第一共享信息以及与数据接收装置预先共享的第二共享信息来生成密钥，利用密钥对预定发送的所希望的数据进行加密，并且发送包含第一共享信息和加密数据的单向发送用的包。

[0112] (步骤S601)

[0113] 在步骤S601中，控制部213作为密钥生成部403和第一共享信息生成部407发挥功能，例如，取得来自存储部214的与数据接收装置共享的第二共享信息(例如初始值的日期和时间信息)、以及第一共享信息(例如在数据发送装置中由传感器测定传感器数据的日期和时间信息)。并且，密钥生成部403计算从第二共享信息的日期和时间到第一共享信息的日期和时间的经过期间，将包含该经过期间的信息生成为密钥。

[0114] (步骤S602)

[0115] 在步骤S602中，控制部213作为加密部404发挥功能，使用在步骤S601中决定的密钥，对预定发送的所希望的数据(例如生物信息)进行加密而生成加密数据。

[0116] (步骤S603)

[0117] 在步骤S603中，控制部213作为包生成部405发挥功能，以包含步骤S602中生成的加密数据和在密钥生成部403中生成的密钥所使用的第一共享信息(在此为测定传感器数据的日期和时间信息)的方式生成包。

[0118] (步骤S604)

[0119] 在步骤S604中，控制部213作为发送部406发挥功能，经由通信接口217以单侧用发送的方式发送步骤S603中生成的包。例如，发送部406经由通信接口217发送广播包。

[0120] 接着，利用图7对数据接收装置150的动作示例进行说明。图7是例示数据接收装置150的处理步骤的一例的流程图。另外，以下说明的处理步骤仅是一例，各处理可以尽可能地变更。此外，以下说明的处理步骤能够根据实施方式适当地进行步骤的省略、替换和追加。

[0121] (启动)

[0122] 首先，用户启动数据接收装置150，并且使启动的数据接收装置150执行密钥生成和数据解密控制程序。数据接收装置150的控制部313按照以下的处理步骤，根据从接收到的包提取的第一共享信息和预先存储的第二共享信息来生成密钥，利用密钥对接收到的包中所含的加密数据进行解密，取得接收包中所含的所希望的数据。

[0123] (步骤S701)

[0124] 在步骤S701中，控制部313作为接收部502发挥功能，经由通信接口317接收广播包。

[0125] (步骤S702)

[0126] 在步骤S702中，控制部313作为第一共享信息提取部505发挥功能，从在步骤S701中接收到的包提取第一共享信息。在此，第一共享信息是指包含测定传感器数据的日期和时间的信息。

[0127] (步骤S703)

[0128] 在步骤S703中，控制部313作为密钥决定部503发挥功能，从存储部314取得接收装置和发送装置预先共享的第二共享信息(任意的相同数值亦即初始值的日期和时间信息)。并且，密钥决定部503根据在步骤S702中取得的第一共享信息、以及第二共享信息，例如计算从初始值的日期和时间到测定传感器数据的日期和时间的经过期间，并且将该经过期间生成为密钥。

[0129] 在接收到的包中含有MAC地址的情况下，密钥决定部503确认该地址是否与存储于存储部314的MAC地址一致。在一致的情况下，密钥决定部503原状继续处理，在不一致的情况下，视为接收方不同而废弃该包。

[0130] (步骤S704)

[0131] 在步骤S704中，控制部313作为解密部504发挥功能，使用在步骤S703中生成的密钥，对由接收部502接收的广播包进行解密。

[0132] (步骤S705)

[0133] 在步骤S705中，控制部313作为解密部504发挥功能，取得在步骤S704中被解密的所希望的数据。所希望的数据例如是由数据发送装置100取得的生物信息(例如血压值和/或脉搏)。

[0134] <作用和效果>

[0135] 如上所述，本实施方式中，在数据发送装置100中，计算在上述步骤S601中从第二共享信息所示的日期和时间(初始值的日期和时间)到第一共享信息所示的日期和时间(测定传感器数据的日期和时间)的经过期间，制作包含该经过期间的密钥，在数据接收装置150中，在步骤S702和步骤S703中取得第一共享信息且从存储部314选择第二共享信息，能够计算经过期间并生成密钥。由于在数据发送装置100和数据接收装置150中独自地计算相同的经过期间，所以能够在发送侧和接收侧拥有通用的密钥。

[0136] 即，在本实施方式中，在数据发送装置100中，密钥生成部403从存储部214取得在接收装置和发送装置中预先共享的任意的相同数值亦即初始值(第二共享信息)，此外，第一共享信息生成部407生成与可数值化的事件相关的数值亦即事件数值(第一共享信息)，密钥生成部403生成密钥，该密钥包含根据该第一共享信息和第二共享信息算出的数值。加密部404使用该密钥，能够以预先设定的加密方式对想要发送的所希望的信息(例如生物信息)进行加密。根据第一共享信息和第二共享信息运算的数值是在数据发送装置和数据接收装置中特有的数据，因此成为再现性低、隐匿性优异的密钥。并且，包生成部405生成包含加密数据和第一共享信息的包，发送部406对该包进行单向发送(发送广播包)。

[0137] 此后，在数据接收装置150中，接收部502接收广播包，第一共享信息提取部505从包中提取第一共享信息，密钥决定部503取得包中所含的第一共享信息，并且从存储部314取得第二共享信息。密钥决定部503利用与密钥生成部403相同的运算，从第一共享信息和第二共享信息得到数值并生成密钥，该密钥包含根据该数值运算的信息(例如经过期间)。如此，能够在数据发送装置100和数据接收装置150中具有相同的通用的密钥。并且，解密部

504能够使用密钥决定部503生成的密钥对从接收部502接收到的所希望的加密数据进行解密，取得所希望的数据。因此，按照本实施方式，利用单向通信发送的数据能够不容易发生泄漏。

[0138] [BLE的广播]

[0139] 在此，对BLE的广播进行简要说明。

[0140] 在BLE中所采用的被动扫描方式中，如图8所例示的那样，新节点(对应于本实施方式的数据发送装置100)定期地发送告知自己的存在的广播包。在从发送一次广播包到下一次发送广播包为止的期间，该新节点通过进入低耗电的休眠状态而能够节约耗电。此外，由于广播包的接收侧也间歇地动作，所以广播包的收发所导致的耗电是少量的。

[0141] 图9示出了BLE无线通信包的基本结构。BLE无线通信包中含有1字节的前导码、4字节的访问地址、2～39字节(可变)的协议数据单元(PDU:Protocol Data Unit)、以及3字节的循环冗余校验(CRC:Cyclic Redundancy Checksum)。BLE无线通信包的长度依赖于PDU的长度，为10～47字节。10字节的BLE无线通信包(PDU为2字节)也称为Empty PDU包，在主机与从机之间定期地交换。

[0142] 前导码字段是为了BLE无线通信的同步而准备的，储存“01”或“10”的重复。关于访问地址，在广播通道中储存固定数值的访问地址，在数据通道中储存随机数的访问地址。在本实施方式中，将在广播通道上传送的BLE无线通信包亦即广播包作为对象。CRC字段用于检测接收错误。CRC的计算范围仅为PDU字段。

[0143] 接着，利用图10对广播包的PDU字段进行说明。另外，在数据通道上传送的BLE无线通信包亦即数据通信包的PDU字段具有与图10不同的数据结构，但是在本实施方式中，不以数据通信包为对象，因此省略了说明。

[0144] 广播包的PDU字段包含2字节的标头和0～37字节(可变)的净荷。标头还包含4位的PDU Type字段、2位的未使用字段、1位的TxAdd字段、1位的RxAdd字段、6位的Length字段和2位的未使用字段。

[0145] 在PDU Type字段中储存有表示该PDU的类型的值。已定义有“可连接广播”、“非连接广播”之类的几个值。在TxAdd字段中储存有表示在净荷中是否存在发送地址的标志。同样，在RxAdd字段中储存有表示在净荷中是否存在接收地址的标志。在Length字段中储存有表示净荷的字节尺寸的值。

[0146] 在净荷中能够储存任意的数据。因此，数据发送装置100使用预先决定的数据结构，将成为密钥的传感器数据的种类、检测传感器数据的日期和时间、以及已经被加密的生物信息储存于净荷。该数据结构例如包含表示用户的识别符、表示作为发送源装置的数据发送装置100的识别符或表示作为接收方装置的数据接收装置150的识别符、日期和时间数据、与日期和时间数据相关联的生物信息(例如有收缩压值、舒张压值、脉搏数、活动量)。

[0147] 接着，利用图11对净荷的数据结构进行具体说明。

[0148] 数据结构1100包含ID字段1101、传感器数据测定日期和时间字段1102、以及加密数据字段1103。

[0149] ID字段1101储存有表示用户的识别符。另外，也可以代替表示用户的识别符，而是储存有表示数据发送装置100或数据接收装置150的识别符，或者除了表示用户的识别符以外，还储存有表示数据发送装置100或数据接收装置150的识别符。

[0150] 传感器数据测定生成日期和时间字段1102储存有在数据发送装置100中测定传感器数据的日期和时间信息。

[0151] 加密数据字段1103储存有利用与包含于密钥生成日期和时间字段1102的日期和时间信息对应的密钥而加密的希望发送的数据。

[0152] [变形例]

[0153] 以上,对本发明的实施方式进行了详细说明,但是至此为止的说明在所有方面仅是本发明的例示。当然能够在不脱离本发明范围的情况下进行各种改良或变形。例如,能够进行以下方式的变更。此外,在本发明的实施中,也可以适当采用与实施方式对应的具体构成。另外,以下与上述实施方式相同的构成要素采用相同的附图标记,对与上述实施方式相同的方面适当省略了说明。能够适当地组合以下的变形例。

[0154] 〈1〉

[0155] (系统示例)

[0156] 利用图12,对包括网络的数据传送系统的一例进行说明。

[0157] 在数据发送装置100中,包生成部405将由数据发送装置100测定传感器数据而示出日期和时间的第一共享信息以及由密钥加密的加密数据包含于广播包进行发送,数据接收装置150接收该包,提取第一共享信息并基于第一共享信息和第二共享信息生成密钥,利用该密钥对加密数据进行解密。并且,数据接收装置150将解密的数据(例如生物信息)经由网络发送到服务器1200。

[0158] 数据接收装置150例如利用移动通信或WLAN向服务器1200进行发送。另外,在图12的例子中,作为数据发送装置100表示了手表型的可穿戴血压计的外观,但是数据发送装置100的外观并不限定于此,也可以是固定型的血压计,还可以是测定与其他生物信息或活动信息相关的量的传感器装置。

[0159] 〈2〉

[0160] (硬件构成)

[0161] 在上述实施方式中,如图2所示,数据发送装置100包括输出装置211、输入装置212、控制部213、存储部214、驱动器215、外部接口216、通信接口217和电池218电连接而成的计算机。但是,也可以除此以外还包括用于进行各种信息处理的装置。例如,数据发送装置100也可以包括气压传感器和温湿度传感器。

[0162] 加速度传感器检测生物的动作并将该动作信息传送到控制部213。加速度传感器例如是三轴加速度传感器,针对线性独立的三轴(例如彼此正交的三轴)检测生物的加速度。并且,计时装置220将表示三个方向的加速度的加速度信号输出到控制部213。

[0163] 气压传感器检测气压并将气压数据输出到控制部213。

[0164] 温湿度传感器测量数据发送装置100周边的环境温度和环境湿度,并将温度和湿度数据输出到控制部213。

[0165] 此外,数据发送装置100也可以包括GPS接收机。GPS接收机分别接收从多个GPS卫星发送的GPS信号,并且将接收到的GPS信号输出到控制部213。控制部213通过基于上述各GPS信号进行测距运算,从而算出数据发送装置100的当前位置信息、即佩戴了数据发送装置100的被测定者(用户)的位置。

[0166] 另外,在这种情况下,电池218例如向输出装置211、控制部213、存储部214、气压传

感器、温湿度传感器、通信接口217、生物传感器219、计时装置220和GPS接收机供电。

[0167] 数据接收装置150也可以包括以上的变形例的硬件构成。在这种情况下，可以使GPS的位置信息、气压数据以及温度和湿度包含于传感器数据，并且使用包含这些信息的密钥。

[0168] 〈3〉

[0169] (软件构成)

[0170] 本实施方式的数据发送装置100也可以作为进一步包括活动量测定部、步数测量部、睡眠状态测量部和环境(温度和湿度)测量部的计算机发挥功能。存储部214例如存储分别与活动量测定部、步数测量部、睡眠状态测量部和环境(温度和湿度)测量部对应的程序(活动量测定程序、步数测量程序、睡眠状态测量程序和环境(温度和湿度)测量程序)，在执行必要的程序时，将所希望的程序在RAM中展开。并且，控制部213利用CPU来解释并执行在RAM中展开的程序，控制各构成要素。

[0171] 活动量测定部利用加速度传感器检测加速度来算出活动量。活动量测定部利用加速度信号，不仅能够算出被测定者的步行中的活动量，还能够算出家务和案头工作等各种活动中的活动量。活动量例如是步行距离、消耗卡路里或脂肪燃烧量之类的与被测定者的活动相关联的指标。

[0172] 步数测量部利用加速度传感器检测加速度，利用气压传感器检测气压，从而算出步数、快走步数和上台阶步数。利用加速度信号算出被测定者的步行。步数测量部能够利用气压数据和加速度信号，算出被测定者的步数、快走步数和上台阶步数等。

[0173] 睡眠状态测量部利用加速度传感器检测加速度，利用加速度信号检测翻身的状态，由此能够推定睡眠状态。

[0174] 环境(温度和湿度)测量部将示出由温湿度传感器测量的环境温度和环境湿度的环境数据与温湿度传感器中的测量时刻相关联地存储于存储部214。气温(气温的变化)例如被认为是能够引起人的血压变动的要素之一。因此，环境数据是能够成为被测定者的血压变动的主要原因的信息。

[0175] 数据接收装置150也可以包括以上的变形例的软件构成。在这种情况下，也可以使用将包含活动量、上台阶步数和睡眠状态的信息包含在内的密钥。

[0176] 〈4〉

[0177] 数据发送装置100与数据接收装置150分体构成。但是，数据发送装置100和数据接收装置150的构成可以不限定于这种例子，也可以由一台计算机实现具有数据发送装置100和数据接收装置150双方的功能的系统。

[0178] 〈5〉

[0179] 也可以在输入装置212所包含的操作部被按压(导通)时，数据发送装置100开始生物信息的测定。并且，也可以在测定结束后，继续进行图6的动作。

[0180] 〈6〉

[0181] 在上述实施方式中记载了血压测定，以下对能够应用于本实施方式的血压测定方式进行说明。作为一般的方法具有使用袖带结构件并利用示波方式测定用户的血压值的方法。但是，在仅测定血压值的情况下也可以不限于此。例如，也可以包括针对每次心搏检测压力脉搏波的压力脉搏波传感器，检测经过被测定部位(例如左手腕)的桡骨动脉的压力脉

搏波来测定血压值(收缩压值和舒张压值)(张力测量方式)。压力脉搏波传感器也可以将经过被测定部位(例如左手腕)的桡骨动脉的脉搏波检测为阻抗的变化来测定血压值(阻抗方式)。压力脉搏波传感器也可以包括:发光元件,向经过被测定部位中的对应的部分的动脉照射光;以及受光元件,接收该光的反射光(或透射光),并且压力脉搏波传感器将动脉的脉搏波检测为容积的变化来测定血压值(光电方式)。此外,压力脉搏波传感器也可以包括与被测定部位抵接的压电传感器,将经过被测定部位中的对应的部分的动脉的压力导致的形变检测为电阻的变化来测定血压值(压电方式)。此外,压力脉搏波传感器也可以包括:发送元件,向经过被测定部位中的对应的部分的动脉发送电波(发送波);以及接收元件,接收该电波的反射波,并且压力脉搏波传感器将基于动脉的脉搏波的动脉与传感器之间的距离变化检测为发送波与反射波之间的相位偏差来测定血压值(电波照射方式)。另外,只要能够观测可算出血压值的物理量,则也可以应用这些方式以外的方式。

[0182] 〈7〉

[0183] 本发明的装置也能够由计算机和程序来实现,并且能够将程序记录于记录介质(或存储介质),也能够通过网络来提供程序。

[0184] 此外,以上的各装置和这些装置部分也能够分别以硬件构成或硬件资源和软件的组合构成来实施。作为组合构成的软件使用如下的程序:预先从网络或计算机可读取的记录介质(或存储介质)安装于计算机,通过由该计算机的处理器执行,从而用于使该计算机实现各装置的功能。

[0185] 另外,本发明不限定于上述实施方式本身,能够在实施阶段中在不脱离本发明宗旨的范围内对构成要素进行变形而具体化。此外,通过上述实施方式公开的多个构成要素的适当组合,能够形成各种发明。例如,可以从实施方式所示的全部构成要素中删除一些构成要素。此外,也可以适当组合不同的实施方式中的构成要素。

[0186] 此外,“和/或”是指通过“和/或”而相连地列举的事项中的任意一个以上的事项。如果列举具体示例,则“x和/或y”是指由三个要素构成的集合{(x)、(y)、(x,y)}中的任意一个要素。如果列举另一个具体示例,则“x、y和/或z”是指由七个要素构成的集合{(x)、(y)、(z)、(x,y)、(x,z)、(y,z)、(x,y,z)}中的任意一个要素。

[0187] 〈8〉

[0188] 此外,上述实施方式的一部分或全部也可以记载成以下的附记那样,但是并不限于以下的附记。

[0189] (附记1)

[0190] 一种数据发送装置,包括硬件处理器和存储器,测定与生物的信息相关的量,所述硬件处理器构成为:测定与生物的信息相关的量;将根据能够与接收装置之间共享的第一共享信息和第二共享信息而算出的信息生成为密钥;使用所述密钥对所述生物的信息进行加密来生成加密数据;生成包含所述第一共享信息和所述加密数据的单向发送用的包;以及发送所述包,所述存储器包括存储所述第一共享信息和所述加密数据的存储部。

[0191] (附记2)

[0192] 一种数据接收装置,包括硬件处理器和存储器,测定与生物的信息相关的量,所述硬件处理器构成为:接收单向发送用的包,所述单向发送用的包中含有作为被加密的数据的加密数据和能够与发送装置之间共享的第一共享信息;将基于所述第一共享信息并根据

与发送装置之间共享的第二共享信息而算出的信息决定为密钥;以及使用所述密钥对所述包中所含的加密数据进行解密,生成包含由所述发送装置测定的生物的信息的解密数据,所述存储器包括存储所述第一共享信息和所述解密数据的存储部。

[0193] (附记3)

[0194] 一种数据发送方法,包括:利用至少一个硬件处理器,测定与生物的信息相关的量;利用至少一个硬件处理器,将根据能够与接收装置之间共享的第一共享信息和第二共享信息而算出的信息生成为密钥;利用至少一个硬件处理器,使用所述密钥对所述生物的信息进行加密来生成加密数据;利用至少一个硬件处理器,生成包含所述第一共享信息和所述加密数据的单向发送用的包;以及利用至少一个硬件处理器,发送所述包。

[0195] (附记4)

[0196] 一种数据接收方法,包括:利用至少一个硬件处理器,接收单向发送用的包,所述单向发送用的包中含有作为被加密的数据的加密数据和能够与发送装置之间共享的第一共享信息;利用至少一个硬件处理器,将基于所述第一共享信息并根据与发送装置之间共享的第二共享信息而算出的信息决定为密钥;以及利用至少一个硬件处理器,使用所述密钥对所述包中所含的加密数据进行解密,生成包含由所述发送装置测定的生物的信息的解密数据。

[0197] 附图标记说明

[0198] 100…数据发送装置

[0199] 101…传感器

[0200] 102…传感器数据存储部

[0201] 103…计时部

[0202] 104…密钥生成部

[0203] 105…加密部

[0204] 106…包生成部

[0205] 107…发送部

[0206] 108…第二共享信息存储部

[0207] 109…第一共享信息生成部

[0208] 150…数据接收装置

[0209] 151…计时部

[0210] 152…钥信息存储部

[0211] 153…接收部

[0212] 154…密钥决定部

[0213] 155…解密部

[0214] 156…第一共享信息提取部

[0215] 211…输出装置

[0216] 212…输入装置

[0217] 213…控制部

[0218] 214…存储部

[0219] 215…驱动器

[0220] 216…外部接口

[0221] 217…通信接口

[0222] 218…电池

[0223] 219…生物传感器

[0224] 220…计时装置

[0225] 311…输出装置

[0226] 312…输入装置

[0227] 313…控制部

[0228] 314…存储部

[0229] 315…驱动器

[0230] 316…外部接口

[0231] 317…通信接口

[0232] 318…电池

[0233] 319…计时装置

[0234] 320…动作传感器

[0235] 401…生物信息测定部

[0236] 402…存储控制部

[0237] 403…密钥生成部

[0238] 404…加密部

[0239] 405…包生成部

[0240] 406…发送部

[0241] 407…第一共享信息生成部

[0242] 501…存储控制部

[0243] 502…接收部

[0244] 503…密钥决定部

[0245] 504…解密部

[0246] 505…第一共享信息提取部

[0247] 1100…数据结构

[0248] 1101…ID字段

[0249] 1102…传感器数据测定日期和时间字段

[0250] 1103…加密数据字段

[0251] 1200…服务器。

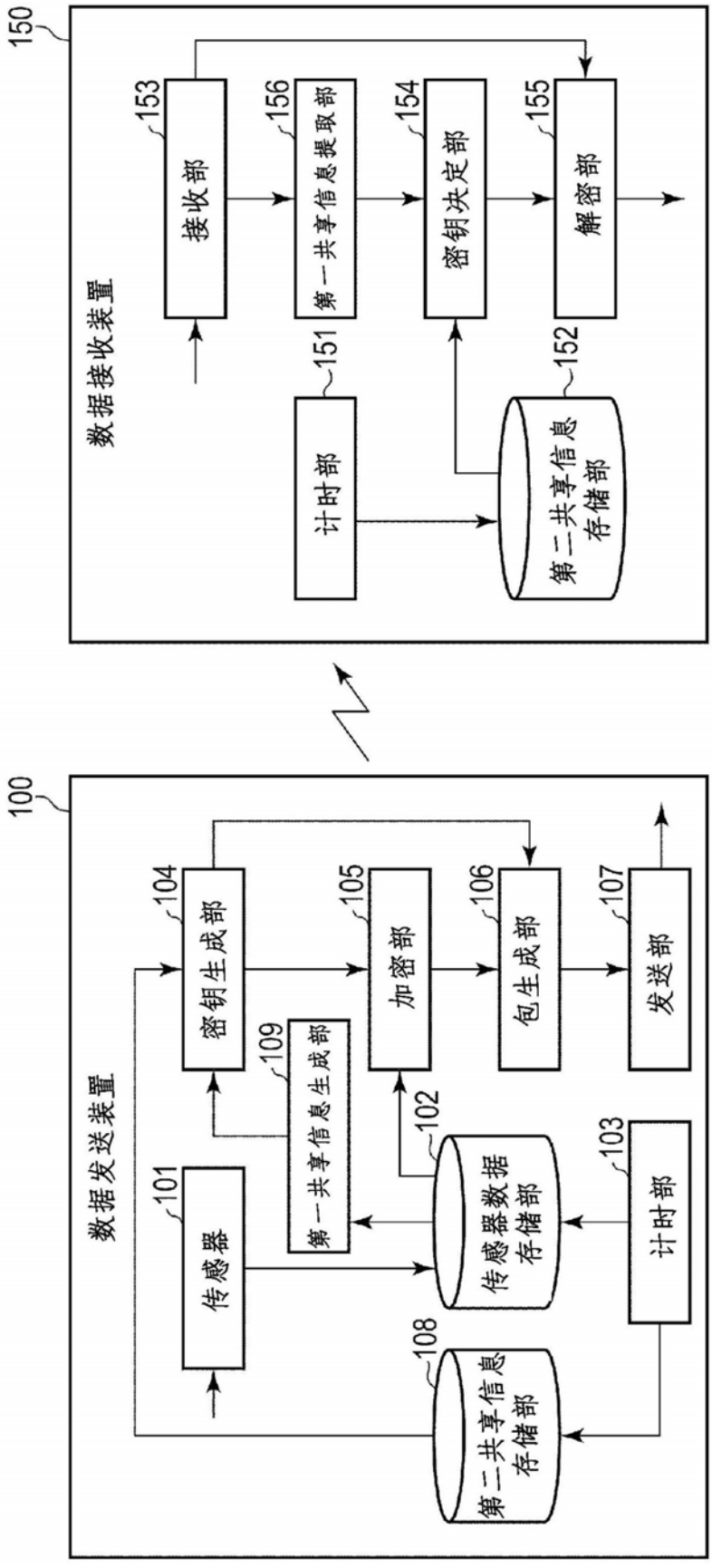

150
数据接收装置
153
接收部
156
第一共享信息提取部
154
密钥决定部
155
解密部
151
计时部
152
第二共享信息存储部
100
数据发送装置
104
密钥生成部
105
加密部
106
包生成部
107
发送部
109
第一共享信息生成部
102
传感器数据存储部
103
计时部
101
传感器
108
第二共享信息存储部

图1

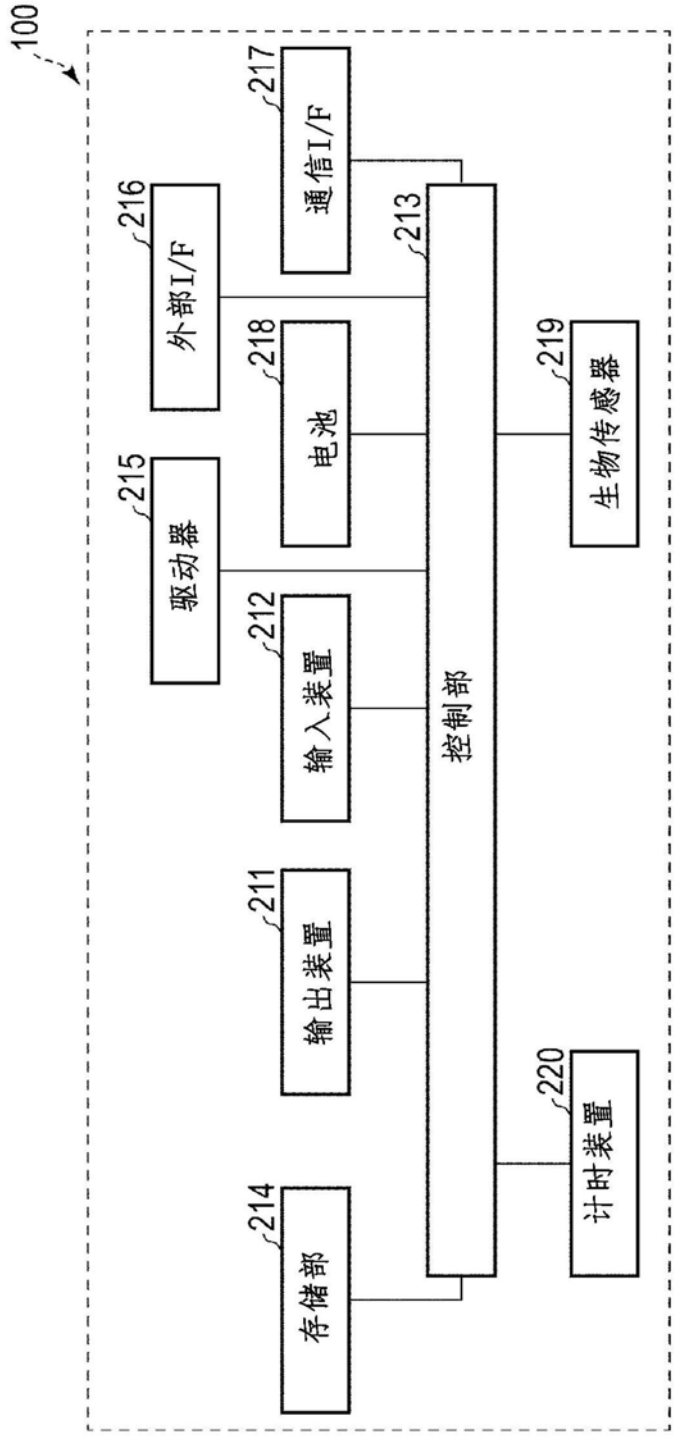

100
217
通信I/F
216
外部I/F
213
218
电池
219
生物传感器
215
驱动器
212
输入装置
控制部
211
输出装置
220
计时装置
214
存储部

图2

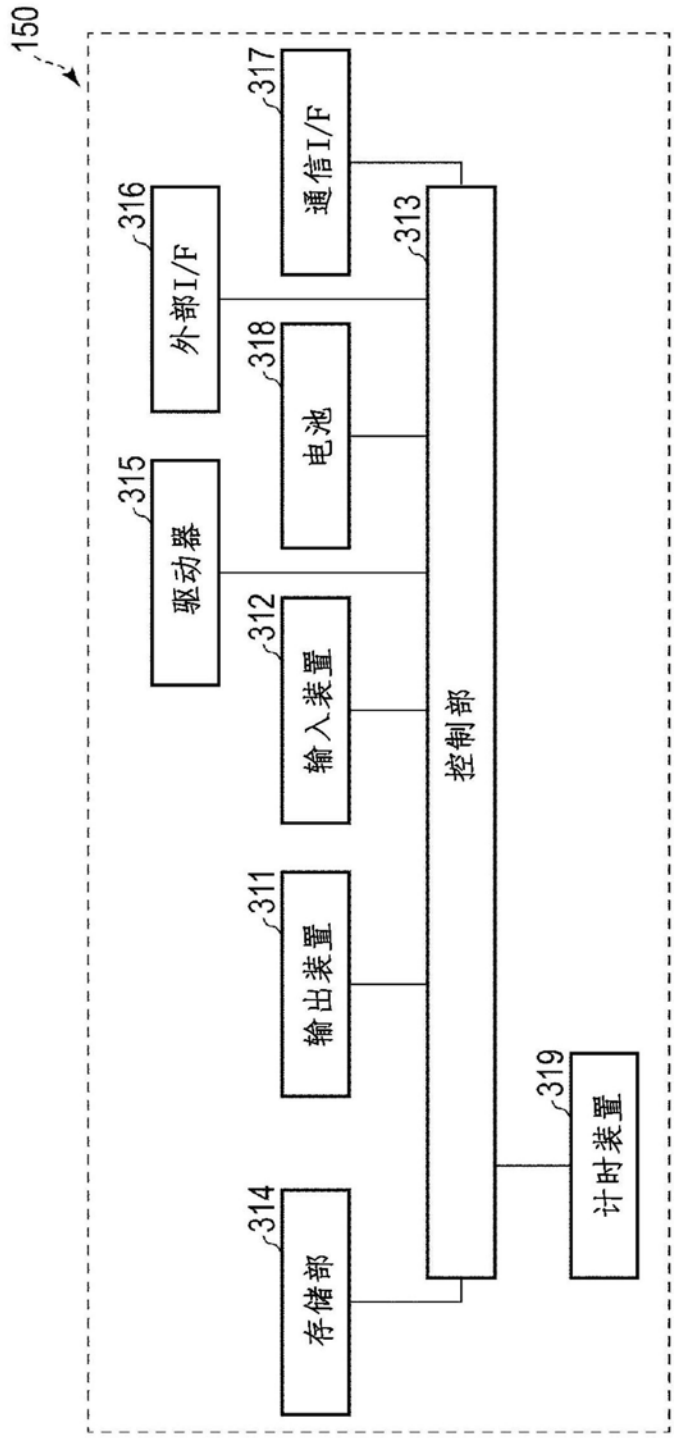

150
317
通信I/F
316
外部I/F
313
318
电池
315
驱动器
312
输入装置
控制部
311
输出装置
319
计时装置
314
存储部

图3

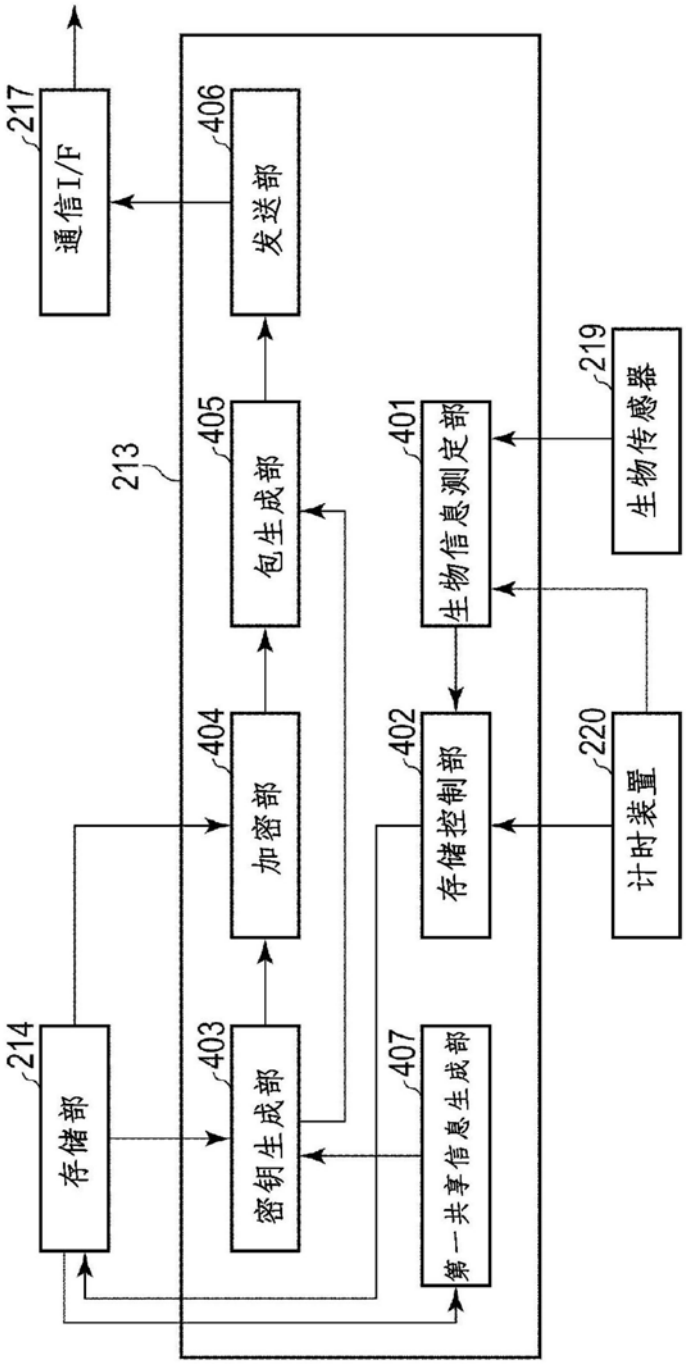

217
通信I/F
406
发送部
213
405
包生成部
401
生物信息测定部
219
生物传感器
404
加密部
402
存储控制部
220
计时装置
214
存储部
403
密钥生成部
407
第一共享信息生成部

图4

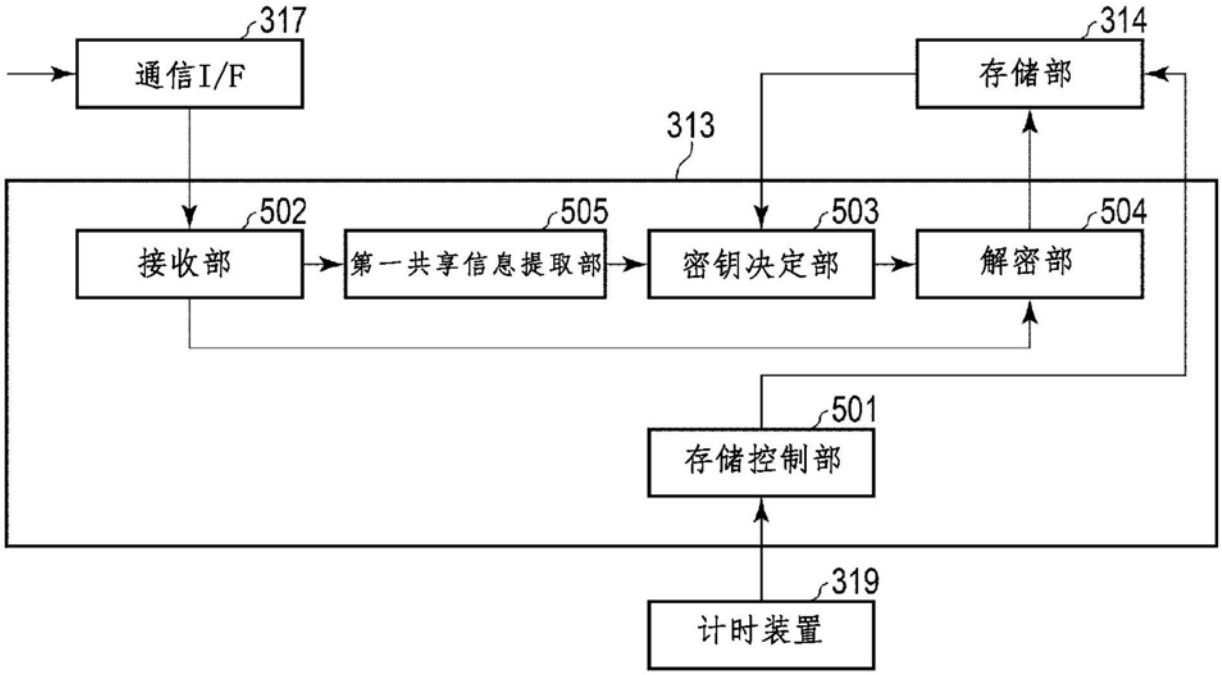

317
通信I/F
314
存储部
313
502
接收部
505
第一共享信息提取部
503
密钥决定部
504
解密部
501
存储控制部
319
计时装置

图5

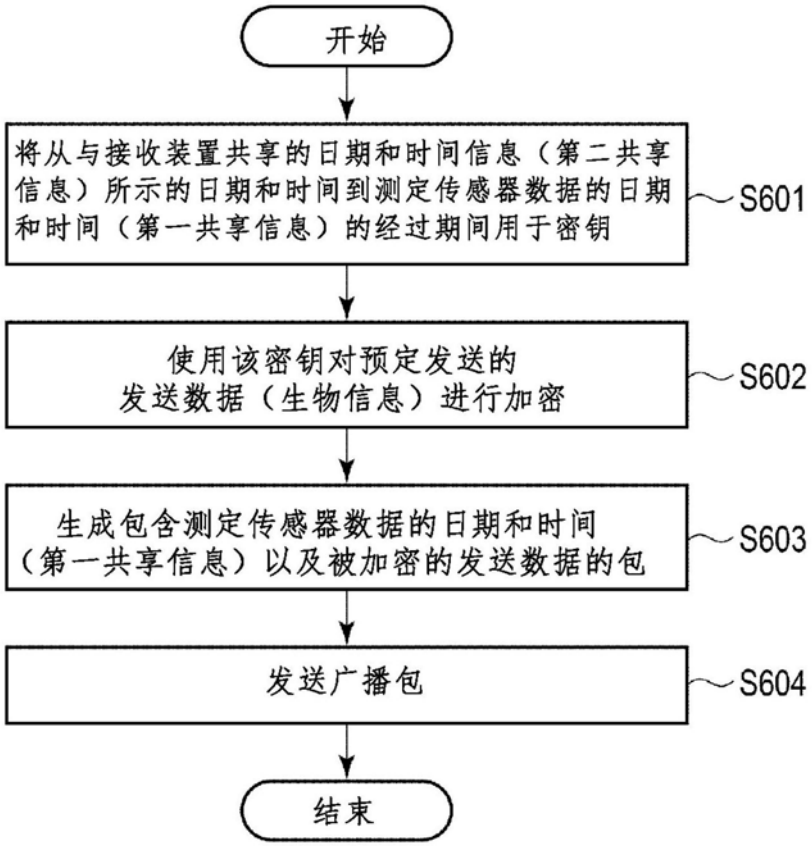

开始
将从与接收装置共享的日期和时间信息（第二共享信息）所示的日期和时间到测定传感器数据的日期和时间（第一共享信息）的经过期间用于密钥
S601
使用该密钥对预定发送的发送数据（生物信息）进行加密
S602
生成包含测定传感器数据的日期和时间（第一共享信息）以及被加密的发送数据的包
S603
发送广播包
S604
结束

图6

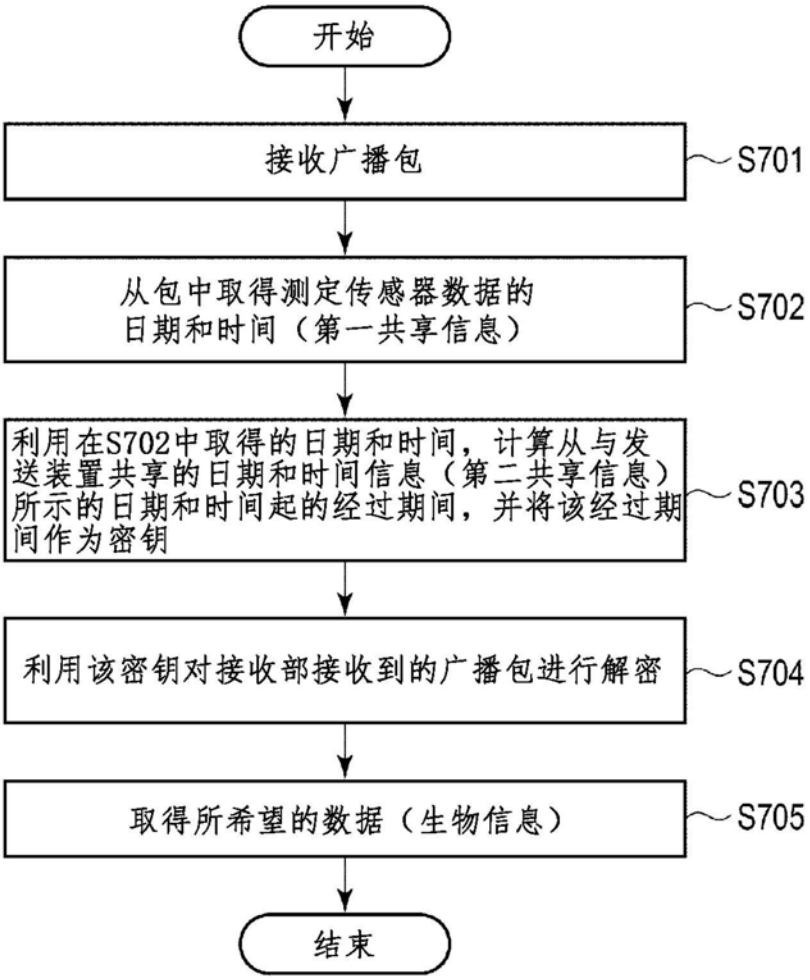

开始
接收广播包
S701
从包中取得测定传感器数据的
日期和时间（第一共享信息）
S702
利用在S702中取得的日期和时间，计算从与发送装置共享的日期和时间信息（第二共享信息）所示的日期和时间起的经过期间，并将该经过期间作为密钥
S703
利用该密钥对接收部接收到的广播包进行解密
S704
取得所希望的数据（生物信息）
S705
结束

图7

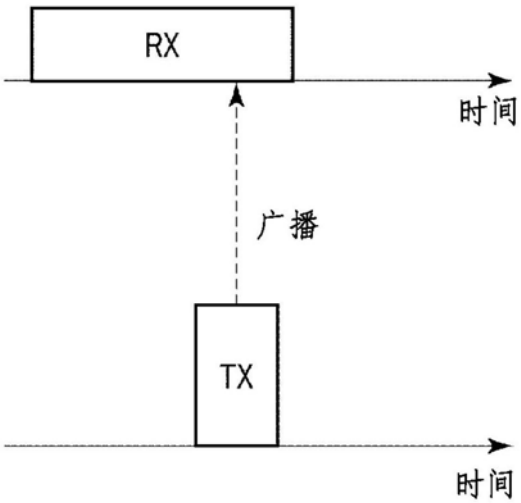

RX
时间
广播
TX
时间

图8

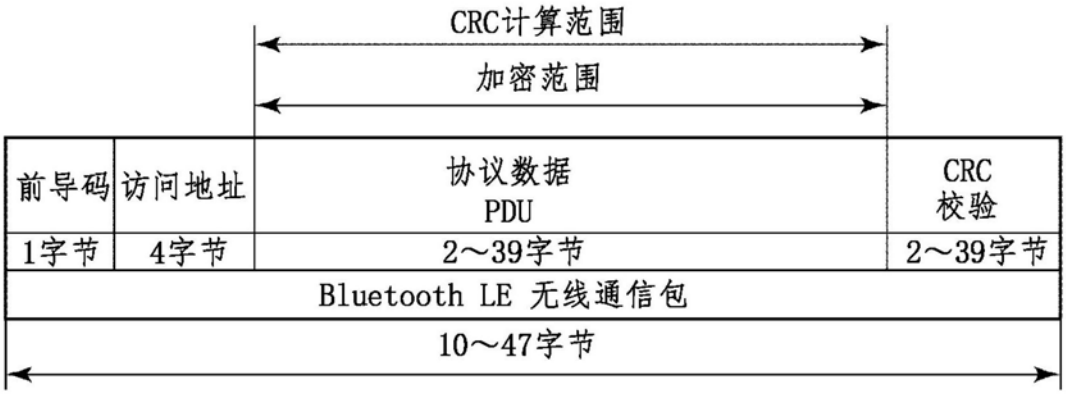

CRC计算范围
加密范围
前导码
访问地址
协议数据
PDU
CRC
校验
1字节
4字节
2～39字节
2～39字节
Bluetooth LE 无线通信包
10～47字节

图9

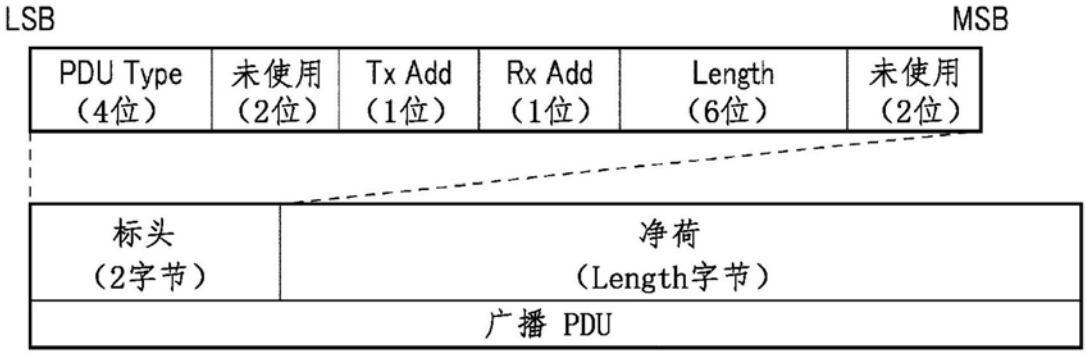

LSB
MSB
PDU Type
（4位）
未使用
（2位）
Tx Add
（1位）
Rx Add
（1位）
Length
（6位）
未使用
（2位）
标头
（2字节）
净荷
（Length字节）
广播 PDU

图10

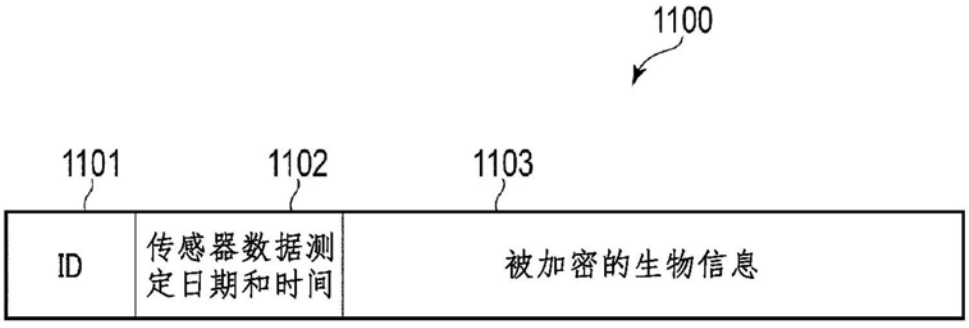

1100
1101
1102
1103
ID
传感器数据测定日期和时间
被加密的生物信息

图11

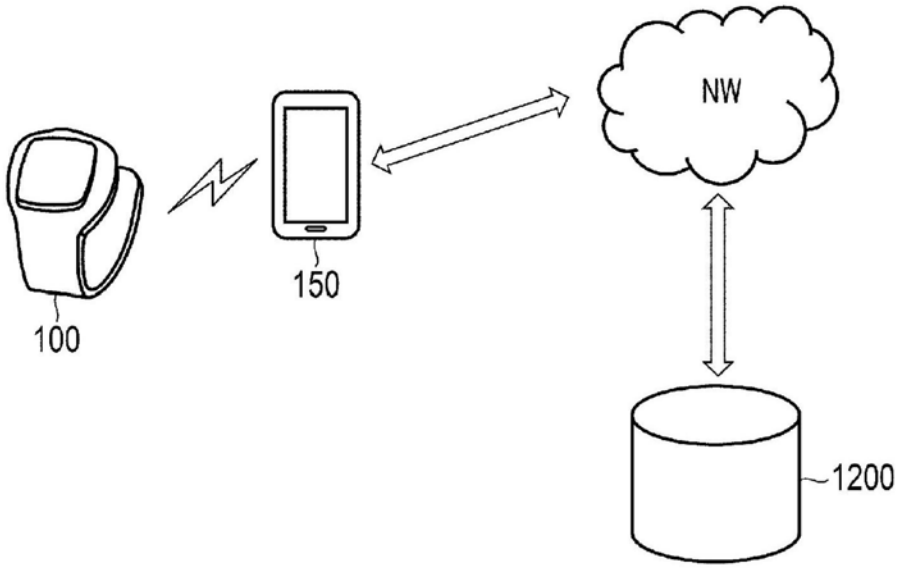


图12