(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2019年2月14日(14.02.2019)

WIPO | PCT

(10) 国際公開番号
WO 2019/031344 A1

(51) 国際特許分類:
H04L 9/08 (2006.01)　　*G06F 21/60* (2013.01)

(21) 国際出願番号：　PCT/JP2018/028827

(22) 国際出願日：　2018年8月1日(01.08.2018)

(25) 国際出願の言語：　日本語

(26) 国際公開の言語：　日本語

(30) 優先権データ：
特願 2017-154765　2017年8月9日(09.08.2017)　JP

(71) 出願人:オムロンヘルスケア株式会社(**OMRON HEALTHCARE CO., LTD.**) [JP/JP]; 〒6170002 京都府向日市寺戸町九ノ坪５３番地 Kyoto (JP). オムロン株式会社(**OMRON CORPORATION**) [JP/JP]; 〒6008530 京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地 Kyoto (JP).

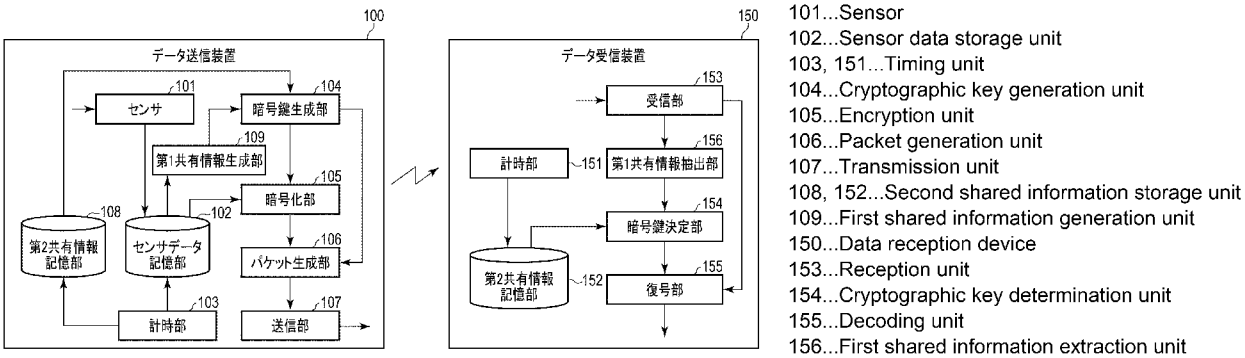
(72) 発明者: 久保 誠雄 (**KUBO, Nobuo**); 〒6170002 京都府向日市寺戸町九ノ坪５３番地 オムロンヘルスケア株式会社内 Kyoto (JP). 出野 徹 (**DENO, Toru**); 〒6170002 京都府向日市寺戸町九ノ坪５３番地 オムロンヘルスケア株式会社内 Kyoto (JP). 近藤 秀規(**KONDO, Hideki**); 〒6170002 京都府向日市寺戸町九ノ坪５３番地 オムロンヘルスケア株式会社内 Kyoto (JP).

(74) 代理人: 蔵田 昌俊, 外 (**KURATA, Masatoshi** et al.); 〒1050014 東京都港区芝三丁目２３番１号 セレスティン芝三井ビルディング１１階 鈴榮特許綜合事務所内 Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,

(54) **Title:** DATA TRANSMISSION DEVICE, DATA RECEPTION DEVICE, METHOD, AND PROGRAM

(54) 発明の名称： データ送信装置、データ受信装置、方法及びプログラム



100...Data transmission device
101...Sensor
102...Sensor data storage unit
103, 151...Timing unit
104...Cryptographic key generation unit
105...Encryption unit
106...Packet generation unit
107...Transmission unit
108, 152...Second shared information storage unit
109...First shared information generation unit
150...Data reception device
153...Reception unit
154...Cryptographic key determination unit
155...Decoding unit
156...First shared information extraction unit

(57) **Abstract:** The present invention makes leakage of data transmitted by one-way communication less prone to occur. The data transmission device according to the present invention is provided with a measurement control unit for measuring a quantity relating to living-body information, a cryptographic key generation control unit for generating, as a cryptographic key, information calculated from first shared information and second shared information shareable with a reception device, an encryption control unit for encrypting the living-body information and generating encrypted data using the first shared information and the cryptographic key, a packet generation control unit for generating a one-way transmission packet including the encrypted data, and a transmission unit for transmitting the packet.

(57) 要約：片方向通信によって送信されたデータの漏洩を生じ難くする。 データ送信装置が、生体の情報に関する量を測定する測定制御部と、受信装置との間で共有できる第１共有情報及び第２共有情報から算出される情報を暗号鍵として生成する暗号鍵生成制御部と、第１共有情報及び暗号鍵を使用して生体の情報を暗号化し暗号化データを生成する暗号化制御部と、暗号化データを含む片方向送信用のパケットを生成するパケット生成制御部と、パケットを送信する送信部と、を備える。

WO 2019/031344 A1

［続葉有］

DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一　国際調査報告(条約第21条(3))

明　細　書

発明の名称 ：

データ送信装置、データ受信装置、方法及びプログラム

技術分野

[0001] この発明は、片方向通信によるデータ送信装置、データ受信装置、方法及びプログラムに関する。

背景技術

[0002] 血圧データをユーザの携帯情報端末に転送する機能を備えた血圧計が市場投入されている。携帯情報端末としては、例えばスマートフォンやタブレット型端末、ノート型パーソナルコンピュータが用いられる。係る機能を利用すれば、ユーザは様々な状況下での自己の血圧の測定結果を携帯情報端末で一覧することができる。また、血圧データの転送には、近距離無線通信技術、特にＢｌｕｅｔｏｏｔｈ（登録商標）技術が典型的には使用される。一般に、Ｂｌｕｅｔｏｏｔｈの通信（コネクション）は、ＷＬＡＮ（Wireless Local Area Network）通信に比べると、小規模かつ省電力に実現可能である。Ｂｌｕｅｔｏｏｔｈの仕様のバージョン４．０は、ＢＬＥ（Bluetooth Low Energy）とも呼ばれ、従前の仕様に比べて消費電力をさらに少なくすることが可能である。

[0003] ＢＬＥでは、コネクションと呼ばれる双方向通信を行うことができる。しかしながら、コネクションは、ペアリングのためにユーザに課される操作が煩雑である、ペアリング後の通信手順が煩雑である、携帯情報端末側がＢＬＥをサポートしている必要がある、携帯情報端末ばかりでなく血圧計にも高性能なハードウェア（プロセッサ、メモリ）が必要となる、開発及び／または評価コストが高い、通信のオーバーヘッド量が大きく小容量のデータ送信に向かない、などの問題がある。

[0004] 他方、ＢＬＥでは、アドバタイジングと呼ばれる片方向通信を行うこともできる。日本国特許第５８５２６２０号公報には、アドバタイズメントパケ

ットのデータフィールドの余白部分に任意のデータを含めて送信する技術が開示されている。

発明の概要

[0005] アドバタイジングを利用して血圧データを送信すれば、ペアリングやその後の煩雑な通信手順が不要となるので、先の問題は解消または軽減される。しかしながら、例えば血圧計が片方向の送信機能しか実装していなければ、携帯情報端末から血圧計に制御データを送って制御したり、逆に、血圧計から携帯情報端末の状態（データの受信状況など）を参照したりすることができなくなる。

[0006] 一般に、血圧計から無線送信されるデータは、その電波の伝播状況次第で、ユーザの携帯情報端末以外のデータ受信装置によっても受信可能である。このとき、仮に血圧データが暗号化されずに送信されていれば、ユーザの血圧データが他人に見られるおそれがある。このようなユーザの健康状態を表す情報の漏洩を予防して、血圧データの転送機能の安全性を高めることが求められる。さらに、前述のように、例えば血圧計が片方向の送信機能しか実装していなければ、血圧計は、携帯情報端末におけるデータの受信状況を参照することはできないので、携帯情報端末におけるデータ欠損が生じないように必要以上に大きな電力でパケットを送信することがあるかもしれない。このような場合には、ユーザの健康状態を表す情報の漏洩が一層生じやすくなる。

[0007] この発明は上記事情に着目してなされたもので、その目的とするところは、片方向通信によって送信されたデータの漏洩を生じ難くするデータ送信装置、データ受信装置、方法及びプログラムを提供することである。

[0008] 本発明は、上述した課題を解決するために、以下の構成を採用する。

[0009] すなわち、本発明の一側面に係るデータ送信装置は、生体の情報に関する量を測定する測定制御部と、受信装置との間で共有できる第１共有情報及び第２共有情報から算出される情報を暗号鍵として生成する暗号鍵生成制御部と、前記暗号鍵を使用して前記生体の情報を暗号化し暗号化データを生成す

る暗号化制御部と、前記第１共有情報及び前記暗号化データを含む片方向送信用のパケットを生成するパケット生成制御部と、前記パケットを送信する送信部と、を備える。

[0010] 上記の構成では、受信装置との間で共有できる第１共有情報及び第２共有情報から算出される情報を暗号鍵として、所望の情報（例えば、生体の情報、以下「生体情報」とも称す）を暗号化する。例えば、受信装置と送信装置とで予め同一の第２共有情報（例えば、任意の同一の数値（初期値））を保存しておき、さらに第１共有情報（例えば、数値化できるイベントに関する数値（イベント数値））をデータ送信装置とデータ受信装置との間で共有する場合には、この第１共有情報と第２共有情報を入力として演算を施した出力値が暗号鍵になる。この演算は、例えば、入力値と出力値が対応する演算であればどんな演算でもよい。理想的には、入力値と出力値が一対一に対応する演算を採用してもよい。この場合、入力値に関して出力値が一意に決定され、さらに、その逆、出力値に関して入力値も一意に決定される。しかしながら、一対一の演算でなくとも、入力値に関して出力値の分布が適度に離散されていればよい。すなわち、入力値が異なっても、出力値が同一値になることがあっても構わない（例えば、完全でないハッシュ関数）。もちろん完全なハッシュ関数を演算に使用して出力値を得てもよい。

[0011] また、入力値は、第１共有情報と第２共有情報とから決定されるが、これらも同様な演算で入力値を決定してもよい。セキュリティ上は、暗号鍵を出力する演算と、入力値を出力する演算は異なることが望ましい。

この暗号鍵を使用して暗号化データを生成し、片方向送信用のパケットに暗号化データと第１共有情報とを含ませてパケットを片方向に送信する。すなわち、パケットはデータ送信装置から送信されるのみで、この装置がパケットを受信することはない。以上のように、第１共有情報及び第２共有情報を入力として演算した暗号鍵に用いて所望の情報を暗号化して送信するので、秘匿性の優れる送信を実現することが可能になるデータ送信装置を提供することができる。なお、暗号化する方式は、共通鍵暗号方式を採用し、具体

的な暗号化方式は特に拘らない。

[0012] 上記の一側面に係るデータ送信装置において、前記第１共有情報、第２共有情報及び前記算出される情報は、前記生体の情報を含まない。

上記の構成では、データ送信装置とデータ受信装置とで第１共有情報、第２共有情報及び前記算出される情報から共通する暗号鍵を生成するために、それぞれの装置でセンサによって生体情報を暗号鍵の生成に使用しないので、データ送信装置及びデータ受信装置を常に生体に装着、または装置を携帯する必要がなくなる。したがって、データ送信装置のみを生体に装着すれば、データ送信装置から送信したい生体情報を取得してこの生体情報を暗号化してデータ受信装置に送信することができる。

[0013] 上記の一側面に係るデータ送信装置において、前記暗号鍵生成制御部は、前記第１共有情報に日時を対応付け、前記第２共有情報に予め設定した日時を対応付ける。

上記の構成では、第１共有情報に日時を対応付け、これをデータ受信装置へパケットに含めて送信するため、データ送信装置とデータ受信装置とでこの第１共有情報を共有することができる。これにより、第２共有情報（例えば、受信装置と送信装置とで予め任意の同一の日時）と、第１共有情報（例えば、生体情報に関する量を測定した日時）とから算出される情報（例えば、これら日時の時間差（経過時間、または経過期間とも称す））を暗号鍵とすることができる。なお、この日時は、データ送信装置で生体情報が測定された日時だけでなく、任意の時刻でもよい（未来でも過去でもよい）。また、時刻のみに限らず年月日を含む日時情報でもよい。なお、時刻は、日にちに関する情報も含んでいると見なし、日時情報と同様の意味で使用する。

[0014] 上記の一側面に係るデータ送信装置において、前記第１共有情報に対応付けられる日時は、前記生体の情報に関する量を測定した日時を含む。

上記の構成では、例えば、受信装置と送信装置とで予め任意の同一の時刻（第２共有情報）と、生体情報に関する量を測定する日時（第１共有情報）とから算出される情報を共有情報として、所定の演算で暗号鍵を生成するこ

とができる。

[0015] 上記の一側面に係るデータ送信装置において、前記第１共有情報及び第２共有情報から算出される情報は、第２共有情報で決まる日時から前記第１共有情報に対応付けられる日時までの経過期間を含む。

上記の構成では、受信装置と送信装置とで予め任意の同一の日時（第２共有情報）と、生体情報に関する量を測定した日時（第１共有情報）とから算出されるこれら日時の時間差である経過期間を暗号鍵とすることになる。したがって、データ送信装置とデータ受信装置との間でのみに通用する暗号鍵を使用して任意のデータ（例えば、生体情報）を暗号化することができる。

[0016] 上記の一側面に係るデータ送信装置において、前記生体の情報は、血圧値、及び脈拍の少なくとも１つを含む。

上記の構成では、データ送信装置が第１共有情報及び第２共有情報に基づいて暗号鍵として使用して、生体情報を送信することが可能になる。ここで生体情報は通常、取得日時を含んだ血圧値及び／または脈拍である時系列データである。したがって、所望の生体情報をセキュアに送信することが可能になるデータ送信装置を提供することができる。

[0017] 上記の一側面に係るデータ受信装置において、暗号化されたデータである暗号化データと、送信装置との間で共有できる第１共有情報を含む片方向送信用のパケットを受信する受信部と、前記第１共有情報に基づいて、送信装置との間で共有する第２共有情報から算出される情報を暗号鍵として決定する暗号鍵決定制御部と、前記パケットに含まれる暗号化データを、前記暗号鍵を使用して復号し復号データを生成する復号制御部と、を備え、前記復号データは、前記送信装置で測定された生体の情報を含む。

上記の構成では、データ送信装置との間で共有できる第１共有情報及び第２共有情報から算出される情報を暗号鍵として、所望の情報（例えば、生体情報）が暗号化されている。例えば、第１共有情報及び第２共有情報は数値であり、受信装置と送信装置とで予め任意の同一の初期値（第２共有情報）を記憶しておき、さらに数値化できるイベントに関するイベント数値（第１

共有情報）を送信することにより、データ送信装置とデータ受信装置との間で第１共有情報及び第２共有情報を共有することができる。データ送信装置でもデータ受信装置でも、第１共有情報及び第２共有情報から決まった演算で暗号鍵を生成することにより、データ受信装置は、この暗号鍵によってセキュアに受信することができ、暗号化データを復号して所望の生体情報を得ることができる。

[0018] 上記の一側面に係るデータ受信装置において、前記第１共有情報、第２共有情報及び前記算出される情報は、前記生体の情報を含まない。

上記の構成では、データ送信装置との間で共通する暗号鍵を生成するために、それぞれの装置でセンサによって生体情報を暗号鍵の生成に使用しない。したがって、データ受信装置は、生体情報を使用する暗号鍵を使用する必要がないので、データ受信装置の使用形態が多様になる。例えば、データ受信装置を常に生体に装着、または装置を携帯する必要がなくなる。この結果、データ受信装置は自宅に設置したまま等でも暗号化データの送受信ができるようになる。

[0019] 上記の一側面に係るデータ受信装置において、前記第１共有情報は、前記送信装置で前記生体情報に関する量を測定した日時であり、前記暗号鍵決定制御部は、前記生体情報に関する量を測定した日時に基づいて、前記第２共有情報から前記暗号鍵を決定する。

上記の構成では、送信装置で前記生体情報に関する量を測定した日時をパケットに含めて、データ受信装置が受信するため、データ送信装置とデータ受信装置とでこの日時を共有することができる。例えば、受信装置と送信装置とで予め任意の同一の日時（第２共有情報）と、生体情報に関する量を測定した日時（第１共有情報）とから算出される情報（例えば、これら日時の時間差である経過期間）を暗号鍵とすることができる。なお、この日時は、データ送信装置が生体情報に関する量を測定した日時だけでなく、任意の時刻でもよい（未来でも過去でもよい）。また、時刻のみに限らず年月日を含む日時情報でもよい。なお、時刻は、日にちに関する情報も含んでいると見

なし、日時情報と同様の意味で使用する。

[0020] 上記の一側面に係るデータ受信装置において、前記第１共有情報及び第２共有情報から算出される情報は、第２共有情報で決まる日時から第１共有情報に対応付けられる日時までの経過期間を含む。

上記の構成では、受信装置と送信装置とで予め共有する日時（第２共有情報）から、生体情報に関する量を測定した日時（第１共有情報）までの経過期間を暗号鍵とする。この経過期間は、データ受信装置とデータ送信装置との間でしか知り得ないので、セキュアに生体情報を授受することが可能になるデータ受信装置を提供することができる。

[0021] 上記の一側面に係るデータ受信装置において、前記生体の情報は、血圧値、及び脈拍の少なくとも１つを含む。

上記の構成では、復号データは、データ送信装置のセンサが取得する生体情報であり、例えば、血圧値及び／または脈拍である。データ受信装置が第１共有情報及び第２共有情報に基づいて生成された情報を暗号鍵として使用して、生体情報を復号することが可能になる。ここで生体情報は通常、取得日時を含んだ血圧値及び／または脈拍である時系列データである。したがって、所望の生体情報をセキュアに復号することが可能になるデータ受信装置を提供することができる。

[0022] 上記の一側面に係る前記データ送信装置は血圧計または脈拍計であり、前記データ受信装置は携帯情報端末である。

上記の構成では、血圧計または脈拍計で測定した生体情報を送信し、携帯情報端末がこの生体情報をセキュアに受信することが可能になる。

[0023] 上記の一側面に係るデータ送信装置で生成されるパケットは近距離無線通信方式によって送信される。

上記の構成では、データ送信装置からデータ受信装置への送信は近距離無線通信方式（例えば、ＢＬＥ）にしたがうことによって、他の無線通信方式よりも低消費電力かつ安価な機器で送信を実現することが可能になる。

[0024] 本発明によれば、片方向通信によって送信されたデータの漏洩を生じ難く

することができるデータ送信装置、データ受信装置、方法及びプログラムを提供することができる。

図面の簡単な説明

[0025] [図1]図１は、実施の形態に係るデータ送信装置及びデータ受信装置の適用場面の一例を模式的に例示する図である。

[図2]図２は、実施の形態に係るデータ送信装置のハードウェア構成の一例を模式的に例示する図である。

[図3]図３は、実施の形態に係るデータ受信装置のハードウェア構成の一例を模式的に例示する図である。

[図4]図４は、実施の形態に係るデータ送信装置のソフトウェア構成の一例を模式的に例示する図である。

[図5]図５は、実施の形態に係るデータ受信装置のソフトウェア構成の一例を模式的に例示する図である。

[図6]図６は、実施の形態に係るデータ送信装置の処理手順の一例を例示する図である。

[図7]図７は、実施の形態に係るデータ受信装置の処理手順の一例を例示する図である。

[図8]図８は、ＢＬＥにおいて行われるアドバタイジングの説明図である。

[図9]図９は、ＢＬＥにおいて送受信されるパケットのデータ構造を例示する図である。

[図10]図１０は、アドバタイズメントパケットのＰＤＵフィールドのデータ構造を例示する図である。

[図11]図１１は、実施の形態に係るデータ送信装置が送信するパケットのＰＤＵフィールドのペイロードに格納されるデータ構造の一例を示す図である。

[図12]図１２は、実施の形態に係るデータ送信装置及びデータ受信装置を含むデータ伝送システムの一例を例示する図である。

発明を実施するための形態

[0026] 以下、本発明の一側面に係る実施の形態（以下、「本実施形態」とも表記する）を、図面に基づいて説明する。なお、以下の実施形態では、同一の番号を付した部分については同様の動作を行うものとして、重ねての説明を省略する。

[0027] ［適用例］

まず、図１を用いて、本発明が適用される場面の一例について説明する。図１は、本実施形態に係るデータ送信装置１００及びデータ受信装置１５０の適用場面の一例を模式的に例示する。本実施形態に係るデータ送信装置１００は、センサ１０１が生体から取得したセンサデータと計時部１０３によって時刻とを対応付けた時系列のセンサデータを、センサデータ記憶部１０２に記憶する。第１共有情報生成部１０９がセンサデータ記憶部１０２から第１共有情報を生成し、暗号鍵生成部１０４が第２共有情報記憶部１０８から第２共有情報を取得する。そして、データ送信装置１００とデータ受信装置１５０との第１共有情報及び第２共有情報に基づいて暗号鍵生成部１０４が暗号鍵を生成し、暗号化部１０５がセンサデータ記憶部１０２から取得した送信したい所望のデータ（例えば、生体情報）をこの暗号鍵で暗号化する。次に、パケット生成部１０６が第１共有情報及び暗号化データを含んだパケットを生成し、送信部１０７が生成された片方向送信用のパケット（例えば、ＢＬＥのアドバタイジングを使用）を送信する。なお、暗号鍵生成部１０４が本発明の「暗号鍵生成制御部」に相当し、暗号化部１０５が本発明の「暗号化制御部」に相当する。第１共有情報は、例えば、センサデータがセンサで取得（または検出）された日時であり、第２共有情報は、例えば、予めデータ送信装置とデータ受信装置との間で共有している日時である。センサデータがセンサに取得（または測定、検出）された日時は、より正確に言えば、センサデータの元になる生体情報がセンサに取得（または測定、検出）された日時であるが、便宜上、以下の説明と特許請求の範囲では同一の意味で使用する。第２共有情報は、ユーザが任意に設定することができることが望ましい。この結果、複数のデータ送信装置及びデータ受信装置があって

も、同一の暗号鍵が生成される可能性が低くなる。したがって、復号化されるべきでない任意のデータ受信装置が第１共有情報を受信しても、データ受信装置が暗号化データを復号化できる可能性は低くなる。

[0028] 本実施形態に係るデータ受信装置１５０は、受信部１５３が片方向送信用のパケットを受信し、第１共有情報抽出部１５６がパケットにから抽出した第１共有情報（例えば、センサデータがセンサに取得された日時データ）と第２共有情報記憶部１５２に含まれる情報に基づいて、暗号鍵決定部１５４が暗号鍵を生成し決定する。第２共有情報記憶部１５２には、データ受信装置とデータ送信装置とで第２共有情報（例えば、予め任意の同一の数値（初期値；例えば、時刻等））が記憶されている。復号部１５５は、暗号鍵決定部１５４で生成された暗号鍵を使用して受信部１５３で受信された暗号化データを復号し、データ受信装置はデータ送信装置で取得した所望のデータを受け取ることができる。計時部１５１は、第２共有情報記憶部１５２に格納される第２共有情報に関連した情報として日時データを付す際に使用される。単純な例としては、ユーザが入力装置を使用してある所望の時刻データを第２共有情報記憶部１５２に記録する際に使用する。

[0029] データ送信装置からデータ受信装置への片方向の通信方式は、例えば、ＢＬＥのアドバタイジングである。この通信方式によって片方向送信用のパケットが生成される。また、本実施形態で送信される所望のデータは、例えば、生体情報であり、具体的には例えば、血圧値及び／または脈拍である。センサデータは、センサ１０１で検出できるデータであれば何でもよく、例えば、歩数及び／または３軸加速度である。さらに、センサで検出できれば血圧値及び／または脈拍等の生体情報でも構わない。また、暗号化する方式は、共通鍵暗号方式を採用し、具体的な暗号化方式は特に拘らないが、例えば、ＤＥＳ（Data Encryption Standard）、またはＡＥＳ（Advanced Encryption Standard）を使用する。また、例えば、データ送信装置は血圧計または脈拍計であり、データ受信装置はスマートフォン、携帯電話機、またはモバイルパソコンなどの携帯情報端末である。

[0030] 以上の通り、本実施形態では、データ送信装置１００は、データ送信装置１００で生成した第１共有情報と、受信装置と送信装置とで予め共有している第２共有情報とから算出される暗号鍵で所望の生体情報を暗号化し、片方向送信用のパケットを生成し送信する。データ受信装置１５０は、データ送信装置１００から送信されたパケットに含まれる第１共有情報と、受信装置と送信装置とで予め共有している第２共有情報（例えば、任意の同一の数値）とに基づいて算出した情報を暗号鍵として暗号化データを復号する。そのため、データ受信装置１５０では、データ送信装置１００と同一の第１共有情報及び第２共有情報を得ることができ、これら共有情報から算出される暗号鍵を生成することにする。この暗号鍵はデータ送信装置１００とデータ受信装置１５０とで同じものになる。つまり、データ送信装置１００とデータ受信装置１５０との双方で、データ送信装置１００で生成した第１共有情報と、予め共有している第２共有情報とを含む共有情報に基づいて算出した暗号鍵を設定することができる。したがって、本実施形態によれば、データ送信装置１００が生成した第１共有情報と、受信装置及び送信装置で予め共有している第２共有情報（任意の同一の数値）を使用して、送信側と受信側でそれぞれ暗号鍵を生成することにより、片方向送信用のパケットを安全に送信して情報を伝達することができる。この結果、第２共有情報に対応した共通暗号鍵のみによる暗号化方式よりも、第１共有情報が暗号鍵の内容に影響するので、本実施形態による方式は安全に情報を伝達することが可能になる。

[0031] ［構成例］

（ハードウェア構成）

＜データ送信装置＞

次に、図２を用いて、本実施形態に係るデータ送信装置１００のハードウェア構成の一例について説明する。

図２に示される通り、本実施形態に係るデータ送信装置１００は、出力装置２１１、入力装置２１２、制御部２１３、記憶部２１４、ドライブ２１５

、外部インタフェース２１６、通信インタフェース２１７、及び電池２１８が電気的に接続されたコンピュータを含む。さらにデータ送信装置１００は、生体センサ２１９、及び計時装置２２０を備える。本実施形態に係るデータ送信装置１００は、本発明の「データ送信装置」に相当する。なお、図２では、通信インタフェース及び外部インタフェースをそれぞれ、「通信Ｉ／Ｆ」及び「外部Ｉ／Ｆ」と記載している。

[0032] 制御部２１３は、ＣＰＵ（Central Processing Unit）、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）等を含み、情報処理に応じて各構成要素の制御を行う。記憶部２１４は、例えば、ハードディスクドライブ、ソリッドステートドライブ等の補助記憶装置であり、制御部２１３で実行される暗号鍵生成及びパケット送信制御プログラム、生体センサ２１９及が検出したセンサデータ、送信予定の所望のデータ、第２共有情報、及び計時装置２２０が計時した日時データ等を記憶する。

[0033] 暗号鍵生成及びパケット送信制御プログラムは、第１共有情報及び第２共有情報から暗号鍵を生成し、生成された暗号鍵を使用して所望のデータを暗号化し、第１共有情報と暗号化されたデータとを片方向送信用のパケットで送信する処理を実行させる（図６）ためのプログラムである。また、所望のデータは、例えば、生体情報である。生体情報は例えば、血圧値の時系列データである。

[0034] 通信インタフェース２１７は、例えば、近距離無線通信（例えば、ブルートゥース（登録商標））モジュール、無線ＬＡＮモジュール等であり、ネットワークを介した無線通信を行うためのインタフェースである。通信インタフェース２１７は、データ送信装置１００をデータ受信装置１５０に無線接続するためのインタフェースである。通信インタフェース２１７は、制御部２１３によって制御される。通信インタフェース２１７は、制御部２１３が生成した暗号化データを含んだパケットを受け取り、データ受信装置１５０へ送信するために使用される。なお、通信インタフェース２１７は、情報をデータ受信装置１５０から受信することはできず、片方向送信用のパケット

を送信するのみである。

[0035] 入力装置２１２は、例えば、マウス、キーボード等の入力を行うための装置である。出力装置２１１は、例えば、ディスプレイ、スピーカ等の出力を行うための装置である。外部インタフェース２１６は、ＵＳＢポート等であり、例えば、生体センサ２１９及び／または計時装置２２０等の外部装置と接続するためのインタフェースである。図２等では生体センサ２１９、及び計時装置２２０が外部インタフェース２１６に接続しているように図示されていないが、これは後に図４等で制御部２１３の内部のブロックとの接続を明確にするために便宜的に制御部２１３に直接接続しているように記載しているためである。

[0036] 記憶部２１４は、コンピュータその他の装置、機械等が記録されたプログラム等の情報を読み取り可能なように、当該プログラム等の情報を、電気的、磁気的、光学的、機械的、または化学的作用によって蓄積する媒体である。データ送信装置１００は、この記憶部２１４から、暗号鍵生成及びパケット送信制御プログラム、生体センサ２１９が検出したセンサデータ、送信予定の所望のデータ、データ送信装置とデータ受信装置との間で予め共有する第２共有情報、及び計時装置２２０が計時した日時データを取得してもよい。

[0037] ドライブ２１５は、例えば、ＣＤ（Compact Disk）ドライブ、ＤＶＤ（Digital Versatile Disk）ドライブ等であり、記憶媒体に記憶されたプログラムを読み込むための装置である。ドライブ２１５の種類は、記憶媒体の種類に応じて適宜選択されてよい。上記の暗号鍵生成及びパケット送信制御プログラム、生体センサ２１９が検出したセンサデータ、送信予定の所望のデータ、及び計時装置２２０が計時した日時データは、この記憶媒体に記憶されていてもよい。ここでは、記憶媒体の一例として、ＣＤ、ＤＶＤ等のディスク型の記憶媒体を例示している。しかしながら、記憶媒体の種類は、ディスク型に限定される訳ではなく、ディスク型以外であってもよい。ディスク型以外の記憶媒体として、例えば、フラッシュメモリ等の半導体メモリを挙げる

ことができる。

[0038] 電池２１８は、例えば、充電可能な２次電池である。電池２１８は、データ送信装置１００本体に搭載されている各要素へ電力を供給する。電池２１８は、例えば、出力装置２１１、入力装置２１２、制御部２１３、記憶部２１４、ドライブ２１５、外部インタフェース２１６、通信インタフェース２１７、生体センサ２１９、及び計時装置２２０へ電力を供給する。

[0039] 生体センサ２１９は、例えば、血圧測定装置である。この場合、生体センサ２１９は、例えば、生体であるユーザの手首に装着された押圧カフの圧力を検出して生体の血圧値を検出する。生体センサ２１９は、血圧データ（例えば、血圧値の時系列データ）を制御部２１３へ出力する。また、生体センサ２１９は脈拍測定装置でもよいし、血圧と共に脈拍を測定してもよい。

[0040] 計時装置２２０は、時間を計測する装置であり、日時を計測できる。例えば、計時装置２２０はカレンダーを含む時計であり、現在の日時の情報を制御部２１３へ渡す。

[0041] なお、データ送信装置１００の具体的なハードウェア構成に関して、実施形態に応じて、適宜、構成要素の省略、置換及び追加が可能である。例えば、制御部２１３は、複数のプロセッサを含んでもよい。データ送信装置１００は、複数台の情報処理装置で構成されてもよい。また、データ送信装置１００は、提供されるサービス専用に設計された情報処理装置の他、汎用のデスクトップＰＣ（Personal Computer）、タブレットＰＣ等が用いられてもよい。

[0042] ＜データ受信装置＞

次に、図３を用いて、本実施形態に係るデータ受信装置１５０のハードウェア構成の一例について説明する。データ受信装置１５０のハードウェア構成はデータ送信装置１００とほぼ同様である。

図３に示される通り、本実施形態に係るデータ受信装置１５０は、出力装置３１１、入力装置３１２、制御部３１３、記憶部３１４、ドライブ３１５、外部インタフェース３１６、通信インタフェース３１７、及び電池３１８

が電気的に接続されたコンピュータを含む。さらにデータ受信装置１５０は、計時装置３１９を備える。本実施形態に係るデータ受信装置１５０は、本発明の「データ受信装置」に相当する。なお、図３では、通信インタフェース及び外部インタフェースをそれぞれ、「通信Ｉ／Ｆ」及び「外部Ｉ／Ｆ」と記載している。

[0043] 制御部３１３は、ＣＰＵ（Central Processing Unit）、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）等を含み、情報処理に応じて各構成要素の制御を行う。記憶部３１４は、例えば、ハードディスクドライブ、ソリッドステートドライブ等の補助記憶装置であり、制御部３１３で実行される暗号鍵生成及びデータ復号制御プログラム、受信して復号した所望のデータ、データ送信装置とデータ受信装置との間で予め共有する第２共有情報、及び計時装置３１９が計時した日時データ等を記憶する。

[0044] 暗号鍵生成及びデータ復号制御プログラムは、パケットに含まれる第１共有情報と予め共有している第２共有情報とから暗号鍵を生成し、生成された暗号鍵を使用して片方向送信用の受信したパケットに含まれる暗号化データを復号する処理を実行させる（図７）ためのプログラムである。また、所望のデータは、例えば、生体情報である。生体情報は例えば、血圧値の時系列データである。

[0045] 通信インタフェース３１７は、通信インタフェース２１７とほぼ同様である。通信インタフェース３１７は、データ送信装置１００からデータを受信するためのインタフェースである。通信インタフェース３１７は、データ送信装置１００からパケットを受け取り、制御部３１３へ渡す。

[0046] 入力装置３１２、出力装置３１１、及び外部インタフェース３１６はそれぞれ、入力装置２１２、出力装置２１１、及び外部インタフェース２１６と同様である。

[0047] 記憶部３１４は、コンピュータその他の装置、機械等が記録されたプログラム等の情報を読み取り可能なように、当該プログラム等の情報を、電気的、磁気的、光学的、機械的、または化学的作用によって蓄積する媒体である

。データ受信装置１５０は、この記憶部３１４から、暗号鍵生成及びデータ復号制御プログラム、受信して復号した所望のデータ、データ送信装置とデータ受信装置との間で共有する第２共有情報、及び計時装置３１９が計時した日時データを取得してもよい。

[0048] ドライブ３１５は、例えば、ＣＤ（Compact Disk）ドライブ、ＤＶＤ（Digital Versatile Disk）ドライブ等であり、記憶媒体に記憶されたプログラムを読み込むための装置である。ドライブ３１５の種類は、記憶媒体の種類に応じて適宜選択されてよい。上記の暗号鍵生成及びデータ復号制御プログラム、計時装置３１９及び／または動きセンサ３２０が検出したセンサデータ、受信して復号した所望のデータ、及び計時装置３１９が計時した日時データは、この記憶媒体に記憶されていてもよい。ここでは、記憶媒体の一例として、ＣＤ、ＤＶＤ等のディスク型の記憶媒体を例示している。しかしながら、記憶媒体の種類は、ディスク型に限定される訳ではなく、ディスク型以外であってもよい。ディスク型以外の記憶媒体として、例えば、フラッシュメモリ等の半導体メモリを挙げることができる。

[0049] 電池３１８は、電池２１８と同様である。電池３１８は、データ受信装置１５０本体に搭載されている各要素へ電力を供給する。

[0050] 計時装置３１９は、計時装置２２０と同様である。

[0051] なお、データ受信装置１５０の具体的なハードウェア構成に関して、実施形態に応じて、適宜、構成要素の省略、置換及び追加が可能である。例えば、制御部３１３は、複数のプロセッサを含んでもよい。データ受信装置１５０は、複数台の情報処理装置で構成されてもよい。また、データ受信装置１５０は、提供されるサービス専用に設計された情報処理装置の他、汎用のデスクトップＰＣ（Personal Computer）、タブレットＰＣ等が用いられてもよい。

[0052] （ソフトウェア構成）

＜データ送信装置＞

次に、図４を用いて、本実施形態に係るデータ送信装置１００のソフトウ

ェア構成の一例を説明する。

データ送信装置１００の制御部２１３は、必要なプログラムを実行する際に、記憶部２１４に記憶された、暗号鍵生成及びパケット送信制御プログラムをＲＡＭに展開する。そして、制御部２１３は、ＲＡＭに展開された暗号鍵生成及びパケット送信制御プログラムをＣＰＵにより解釈及び実行して、各構成要素を制御する。これによって、図４に示される通り、本実施形態に係るデータ送信装置１００は、生体情報測定部４０１、記憶制御部４０２、暗号鍵生成部４０３、暗号化部４０４、パケット生成部４０５、送信部４０６、第１共有情報生成部４０７を備えるコンピュータとして機能する。

[0053] 生体情報測定部４０１は、生体センサ２１９が生体情報を検出し出力するセンサデータと、計時装置２２０から取得した日時情報と共に記憶制御部４０２に渡す。また、生体情報測定部４０１は、この生体情報と日時情報とを合わせた生体情報の時系列データを記憶制御部４０２に渡してもよい。

記憶制御部４０２は、生体情報測定部４０１から受け取った、センサデータと日時情報とを関連付けたデータを記憶部２１４に記憶させる。また、記憶制御部４０２は、計時装置２２０から日時情報を取得し、日時情報を他の受け取った情報に対応付けて記憶部２１４に記憶させてもよい。

[0054] 第１共有情報生成部４０７は、数値化できるイベントに関する数値（イベント数値）を生成する。具体的には、第１共有情報生成部４０７は、例えば、イベント数値はデータ送信装置で生体情報に関する量を測定した日時情報を生成する。

[0055] 暗号鍵生成部４０３は、第１共有情報生成部４０７で生成される第１共有情報と、記憶部２１４が記憶している第２共有情報とから、暗号鍵を生成する。共有情報は、例えば、受信装置と送信装置とで予め任意の同一の数値（初期値）を保存しておき、さらに数値化できるイベントに関する数値（イベント数値）である。具体的には、例えば、初期値はある特定の日時情報であり、この場合には、暗号鍵生成部４０３は、例えば、初期値の日時からイベント数値の日時までの経過期間を算出し、この経過期間を暗号鍵とする。

また、暗号鍵は、共有情報の他に予め設定された、データ受信装置１５０と共有している他のデータを含んでもよい。例えば、予めデータ送信装置１００のＭＡＣ（media access control）アドレスを暗号鍵に含めてもよい。このＭＡＣアドレスはデータ受信装置１５０も予め既知に設定しておく。この場合、データ送信装置１００のＭＡＣアドレスは、記憶部２１４及び記憶部３１４に記憶しておく。

[0056] 暗号化部４０４は、記憶部２１４に記憶されている送信すべき所望のデータを受け取り、暗号鍵生成部４０３から受け取る暗号鍵で、所望のデータを暗号化する。暗号化する方式は、共通鍵暗号方式を採用し、具体的な暗号化方式は特に拘らない。具体的な暗号化方式は、例えば、ＤＥＳ、ＡＥＳがある。

[0057] パケット生成部４０５は、暗号鍵生成部４０３から暗号鍵に関する情報を取得し、暗号鍵に関するこの情報と、暗号化部４０４で暗号化された所望のデータとを含むパケットを生成する。このパケットは片方向送信用のパケットであり、例えば、ＢＬＥのアドバタイズメントパケットである。また、暗号鍵に関する情報は、例えば、暗号鍵に含まれる算出された数値の元になるイベント数値を含む。具体的には、暗号鍵に含まれる算出された数値は、例えば、経過期間であり、イベント数値は暗号鍵が生成された日時である。

なお、暗号鍵に関する情報は、センサの位置情報を含んでもよい。この日時と位置の情報は、暗号鍵でデータを復号する際に使用される。

[0058] 送信部４０６は、パケット生成部４０５で生成されたパケットを、片方向送信用として所定の通信方式で通信インタフェース２１７を介して送信する。この通信方式は、例えば、ＢＬＥであり、送信部４０６はＢＬＥのアドバタイジングを利用してパケットを送信する。

[0059] ＜データ受信装置＞

次に、図５を用いて、本実施形態に係るデータ受信装置１５０のソフトウェア構成の一例を説明する。

データ受信装置１５０の制御部３１３は、必要なプログラムを実行する際

に、記憶部３１４に記憶された、暗号鍵生成及びデータ復号制御プログラムをＲＡＭに展開する。そして、制御部３１３は、ＲＡＭに展開された暗号鍵生成及びデータ復号制御プログラムをＣＰＵにより解釈及び実行して、各構成要素を制御する。これによって、図５に示される通り、本実施形態に係るデータ受信装置１５０は、記憶制御部５０１、受信部５０２、暗号鍵決定部５０３、復号部５０４、及び第１共有情報抽出部５０５を備えるコンピュータとして機能する。

[0060] 記憶制御部５０１は計時装置３１９から日時情報を取得し、日時情報を他の受け取った情報に対応付けて記憶部３１４に記憶させる。

[0061] 受信部５０２は、データ送信装置１００からのパケットを、通信インタフェース３１７を介して受信する。このパケットには、暗号化データと、暗号鍵に関する情報とが少なくとも含まれている。

[0062] 第１共有情報抽出部５０５は、受信部５０２が受信したパケットに含まれる第１共有情報を抽出する。第１共有情報は、例えば、データ送信装置でセンサが生体情報に関する量を測定した日時情報である。

[0063] 暗号鍵決定部５０３は、第１共有情報抽出部５０５が生成した第１共有情報と、記憶部３１４に記憶されている第２共有情報（予め共有している任意の同一数値；初期値、すなわち、受信装置と送信装置とで予め任意の同一の数値）と、を取得する。パケットに含まれる第１共有情報は、例えば、数値化できるイベントに関する数値（イベント数値）が含まれる。より具体的には、イベント数値は、例えば、センサデータをセンサが測定した日時である。パケットに含まれるこのイベント数値と記憶部３１４に記憶されている初期値とを入力として演算を施した出力値が暗号鍵になる。この演算は、例えば、（完全でない）ハッシュ関数が使用される。また、完全なハッシュ関数を演算に使用してもよい。

[0064] また、パケットが他にＭＡＣアドレスを含んでいる場合には、そのＭＡＣアドレスも記憶部３１４から暗号鍵決定部５０３が取得する。暗号鍵決定部５０３は、記憶部３１４に記憶されるＭＡＣアドレスが、受信したパケット

に含まれるＭＡＣアドレスに一致しているかを確認する。暗号鍵決定部５０３は、例えば、一致している場合にはそのまま処理を進め、一致していない場合にはこのパケットは宛先が異なるとして棄却する。

[0065] 復号部５０４は、受信部５０２から暗号化データを受け取り、さらに暗号鍵決定部５０３で生成された暗号鍵を受け取る。そして、復号部５０４は、この暗号鍵で暗号化データを復号し、所望のデータを受け取る。復号部５０４はこの所望のデータを記憶部３１４に記憶させる。

[0066] ＜その他＞

データ送信装置１００及びデータ受信装置１５０の各機能に関しては後述する動作例で詳細に説明する。なお、本実施形態では、データ送信装置１００及びデータ受信装置１５０の各機能がいずれも汎用のＣＰＵによって実現される例について説明している。しかしながら、以上の機能の一部または全部が、１または複数の専用のプロセッサにより実現されてもよい。また、データ送信装置１００の機能構成に関して、実施形態に応じて、適宜、機能の省略、置換及び追加が行われてもよい。

[0067] ［動作例］

＜データ送信装置＞

次に、図６を用いて、データ送信装置１００の動作例を説明する。図６は、データ送信装置１００の処理手順の一例を例示するフローチャートである。なお、以下で説明する処理手順は一例に過ぎず、各処理は可能な限り変更されてよい。また、以下で説明する処理手順について、実施の形態に応じて、適宜、ステップの省略、置換、及び追加が可能である。

[0068] （起動）

まず、ユーザは、データ送信装置１００を起動し、起動したデータ送信装置１００に暗号鍵生成及びパケット送信制御プログラムを実行させる。データ送信装置１００の制御部２１３は、以下の処理手順にしたがって、第１共有情報を生成し、第１共有情報と、データ受信装置と予め共有している第２共有情報とに基づいて暗号鍵を生成し、送信予定の所望のデータを暗号鍵で

暗号化し、第１共有情報及び暗号化データを含んだ片方向送信用のパケットを送信する。

[0069] （ステップＳ６０１）

ステップＳ６０１では、制御部２１３は、暗号鍵生成部４０３及び第１共有情報生成部４０７として機能し、例えば、記憶部２１４からデータ受信装置と共有している第２共有情報（例えば、初期値の日時情報）と、第１共有情報（例えば、データ送信装置でセンサデータがセンサに測定された日時情報）とを取得する。そして、暗号鍵生成部４０３は、第２共有情報の日時から第１共有情報の日時までの経過期間を計算し、この経過期間を含む情報を暗号鍵として生成する。

[0070] （ステップＳ６０２）

ステップＳ６０２では、制御部２１３は、暗号化部４０４として機能し、ステップＳ６０１で決定した暗号鍵を使用して、送信予定の所望のデータ（例えば、生体情報）を暗号化して暗号化データを生成する。

[0071] （ステップＳ６０３）

ステップＳ６０３では、制御部２１３は、パケット生成部４０５として機能し、ステップＳ６０２で生成された暗号化データと、暗号鍵生成部４０３で生成された暗号鍵に使用された第１共有情報（ここでは、センサデータを測定した日時情報）を含めてパケットを生成する。

[0072] （ステップＳ６０４）

ステップＳ６０４では、制御部２１３は、送信部４０６として機能し、ステップＳ６０３で生成されたパケットを、通信インタフェース２１７を介して片側用送信で送信する。例えば、送信部４０６は通信インタフェース２１７を介してアドバタイズメントパケットを送信する。

[0073] 次に、図７を用いて、データ受信装置１５０の動作例を説明する。図７は、データ受信装置１５０の処理手順の一例を例示するフローチャートである。なお、以下で説明する処理手順は一例に過ぎず、各処理は可能な限り変更されてよい。また、以下で説明する処理手順について、実施の形態に応じて

、適宜、ステップの省略、置換、及び追加が可能である。

[0074] （起動）

まず、ユーザは、データ受信装置１５０を起動し、起動したデータ受信装置１５０に暗号鍵生成及びデータ復号制御プログラムを実行させる。データ受信装置１５０の制御部３１３は、以下の処理手順にしたがって、受信したパケットから抽出した第１共有情報と、予め記憶している第２共有情報とから暗号鍵を生成し、受信したパケットに含まれる暗号化データを暗号鍵で復号し、受信パケットに含まれる所望のデータを取得する。

[0075] （ステップＳ７０１）

ステップＳ７０１では、制御部３１３は、受信部５０２として機能し、通信インタフェース３１７を介してアドバタイズメントパケットを受信する。

[0076] （ステップＳ７０２）

ステップＳ７０２では、制御部３１３は、第１共有情報抽出部５０５として機能し、ステップＳ７０１で受信されたパケットから第１共有情報を抽出する。第１共有情報とは、ここでは、センサデータを測定した日時を含む情報である。

[0077] （ステップＳ７０３）

ステップＳ７０３では、制御部３１３は、暗号鍵決定部５０３として機能し、受信装置と送信装置とで予め共有している第２共有情報（任意の同一の数値である初期値の日時情報）を記憶部３１４から取得する。そして、暗号鍵決定部５０３は、ステップＳ７０２で取得した第１共有情報と、第２共有情報とから、例えば、初期値の日時からセンサデータを測定した日時までの経過期間を計算して、この経過期間を暗号鍵として生成する。

受信したパケットがＭＡＣアドレスを含む場合には、暗号鍵決定部５０３は、このアドレスが記憶部３１４に記憶しているＭＡＣアドレスと一定しているかどうかを確認する。暗号鍵決定部５０３は、一致している場合にはそのまま処理を進め、一致していない場合にはこのパケットは宛先が異なるとして棄却する。

[0078] （ステップＳ７０４）

ステップＳ７０４では、制御部３１３は、復号部５０４として機能し、ステップＳ７０３で生成された暗号鍵を使用して、受信部５０２で受信されたアドバタイズメントパケットを復号する。

[0079] （ステップＳ７０５）

ステップＳ７０５では、制御部３１３は、復号部５０４として機能し、ステップＳ７０４で復号された所望のデータを取得する。所望のデータは、例えば、データ送信装置１００で取得した生体情報（例えば、血圧値及び／または脈拍）である。

[0080] ＜作用と効果＞

以上のように、本実施形態では、データ送信装置１００において上記のステップＳ６０１で第２共有情報が示す日時（初期値の日時）から第１共有情報が示す日時（センサデータを測定した日時）までの経過期間を計算し、この経過期間を含む暗号鍵を作成し、データ受信装置１５０においてステップＳ７０２及びステップＳ７０３で、第１共有情報を取得し、第２共有情報を記憶部３１４から選択して、経過期間を計算し暗号鍵を生成することができる。同一の経過期間をデータ送信装置１００とデータ受信装置１５０で独自に計算するので、共通の暗号鍵を送信側と受信側で所有することができる。

[0081] すなわち、本実施形態では、データ送信装置１００で、暗号鍵生成部４０３が受信装置と送信装置とで予め任意の同一の数値である初期値（第２共有情報）を記憶部２１４から取得し、さらに、第１共有情報生成部４０７が、数値化できるイベントに関する数値であるイベント数値（第１共有情報）を生成し、暗号鍵生成部４０３がこの第２共有情報と第２共有情報とから演算した数値を含んだ暗号鍵を生成する。暗号化部４０４がこの暗号鍵を使用し、送信したい所望の情報（例えば、生体情報）を予め設定した暗号化方式で暗号化することができる。第１共有情報と第２共有情報とから演算した数値はデータ送信装置とデータ受信装置に特有なデータであるため、再現性が低く秘匿性に優れた暗号鍵になる。そして、パケット生成部４０５が暗号化デ

ータと、第１共有情報を含むパケットを生成し、送信部４０６がこのパケットを片方向送信する（アドバタイズメントパケットを送信する）。

[0082] その後、データ受信装置１５０で、受信部５０２がアドバタイズメントパケットを受信し、第１共有情報抽出部５０５がパケットから第１共有情報を抽出し、暗号鍵決定部５０３がパケットに含まれる第１共有情報を取得し、第２共有情報を記憶部３１４から取得する。暗号鍵決定部５０３は、暗号鍵生成部４０３と同一の演算により、第１共有情報と第２共有情報とから数値を得てこの数値から演算した情報（例えば、経過期間）を含む暗号鍵を生成する。このようにして、データ送信装置１００とデータ受信装置１５０とにおいて同一である共通の暗号鍵を有することが可能になる。そして、復号部５０４が、受信部５０２から受信した所望の暗号化データを、暗号鍵決定部５０３が生成した暗号鍵を使用して復号し、所望のデータを取得することができる。したがって、本実施形態によれば、片方向通信によって送信されたデータの漏洩を生じ難くすることができるようになる。

[0083] ［ＢＬＥのアドバタイズメント］

ここで、ＢＬＥのアドバタイズメントについて概略的に説明する。

ＢＬＥにおいて採用されるパッシブスキャン方式では、図８に例示するように、新規ノード（本実施形態のデータ送信装置１００が対応）は自己の存在を周知するアドバタイズメントパケットを定期的に送信する。この新規ノードは、アドバタイズメントパケットを一度送信してから次に送信するまでの間に、低消費電力のスリープ状態に入ることで消費電力を節約できる。また、アドバタイズメントパケットの受信側も間欠的に動作するので、アドバタイズメントパケットの送受信に伴う消費電力は僅かである。

[0084] 図９にＢＬＥ無線通信パケットの基本構造を示す。ＢＬＥ無線通信パケットは、１バイトのプリアンブルと、４バイトのアクセスアドレスと、２～３９バイト（可変）のプロトコルデータユニット（ＰＤＵ：Protocol Data Unit）と、３バイトの巡回冗長チェックサム（ＣＲＣ：Cyclic Redundancy Checksum）とを含む。ＢＬＥ無線通信パケットの長さは、ＰＤＵの長さに依存し

、１０～４７バイトである。１０バイトのＢＬＥ無線通信パケット（ＰＤＵは２バイト）は、Ｅｍｐｔｙ　ＰＤＵパケットとも呼ばれ、マスタとスレイブとの間で定期的に交換される。

[0085] プリアンブルフィールドは、ＢＬＥ無線通信の同期のために用意されており、「０１」または「１０」の繰り返しが格納される。アクセスアドレスは、アドバタイジングチャネルでは固定数値、データチャネルでは乱数のアクセスアドレスが格納される。本実施形態では、アドバタイジングチャネル上で伝送されるＢＬＥ無線通信パケットであるアドバタイズメントパケットを対象とする。ＣＲＣフィールドは、受信誤りの検出に用いられる。ＣＲＣの計算範囲は、ＰＤＵフィールドのみである。

[0086] 次に、図１０を用いて、アドバタイズメントパケットのＰＤＵフィールドについて説明する。なお、データチャネル上で伝送されるＢＬＥ無線通信パケットであるデータ通信パケットのＰＤＵフィールドは図１０とは異なるデータ構造を有するが、本実施形態ではデータ通信パケットを対象としていないので説明を省略する。

[0087] アドバタイズメントパケットのＰＤＵフィールドは、２バイトのヘッダと、０～３７バイト（可変）のペイロードとを含む。ヘッダは、さらに、４ビットのＰＤＵ　Ｔｙｐｅフィールドと、２ビットの未使用フィールドと、１ビットのＴｘＡｄｄフィールドと、１ビットのＲｘＡｄｄフィールドと、６ビットのＬｅｎｇｔｈフィールドと、２ビットの未使用フィールドとを含む。

[0088] ＰＤＵ　Ｔｙｐｅフィールドには、このＰＤＵのタイプを示す値が格納される。「接続可能アドバタイジング」、「非接続アドバタイジング」などのいくつかの値が定義済みである。ＴｘＡｄｄフィールドには、ペイロード中に送信アドレスがあるか否かを示すフラグが格納される。同様に、ＲｘＡｄｄフィールドには、ペイロード中に受信アドレスがあるか否かを示すフラグが格納される。Ｌｅｎｇｔｈフィールドには、ペイロードのバイトサイズを示す値が格納される。

[0089] ペイロードには、任意のデータを格納することができる。そこで、データ送信装置１００は、予め定められたデータ構造を用いて、暗号鍵になるセンサデータの種類、センサデータが検出された日時、暗号化された生体情報をペイロードに格納する。このデータ構造は、例えば、ユーザを表す識別子、送信元装置であるデータ送信装置１００を表す識別子、または宛先装置であるデータ受信装置１５０を表す識別子、日時データ、日時データに関連付けられる生体情報（例えば、収縮期血圧値、拡張期血圧値、脈拍数、活動量がある）を含む。

[0090] 次に、図１１を用いて、ペイロードのデータ構造を具体的に説明する。

データ構造１１００は、ＩＤフィールド１１０１、センサデータ測定日時フィールド１１０２、及び暗号データフィールド１１０３を含む。

[0091] ＩＤフィールド１１０１は、ユーザを表す識別子が格納される。なお、ユーザを表す識別子の代わりに、または、これに加えて、データ送信装置１００またはデータ受信装置１５０を表す識別子が格納されてもよい。

[0092] センサデータ測定生成日時フィールド１１０２は、データ送信装置１００でセンサデータが測定された日時情報が格納される。

[0093] 暗号データフィールド１１０３は、暗号鍵生成日時フィールド１１０２に含まれる日時情報に対応する暗号鍵で暗号化された送信する所望のデータが格納される。

[0094] ［変形例］

以上、本発明の実施の形態を詳細に説明してきたが、前述までの説明はあらゆる点において本発明の例示に過ぎない。本発明の範囲を逸脱することなく種々の改良や変形を行うことができることは言うまでもない。例えば、以下のような変更が可能である。また、本発明の実施にあたって、実施形態に応じた具体的構成が適宜採用されてもよい。なお、以下では、上記実施形態と同様の構成要素に関しては同様の符号を用い、上記実施形態と同様の点については、適宜説明を省略した。以下の変形例は適宜組み合わせ可能である。

[0095] ＜１＞

（システム例）

図１２を用いて、ネットワークを含めたデータ伝送システムの一例を説明する。

データ送信装置１００は、パケット生成部４０５が、データ送信装置１００でセンサデータが測定されて日時を示す第１共有情報と、暗号鍵によって暗号化された暗号化データとをアドバタイズメントパケットに含めて送信し、データ受信装置１５０はこのパケットを受信し、第１共有情報を抽出し第１共有情報と第２共有情報に基づいて暗号鍵を生成し、この暗号鍵で暗号化データを復号する。そして、データ受信装置１５０は復号したデータ（例えば、生体情報）をネットワーク経由でサーバ１２００へ送信する。

データ受信装置１５０は、例えば移動通信またはＷＬＡＮを利用してサーバ１２００へ送信する。なお、図１２の例では、データ送信装置１００として腕時計型のウェアラブル血圧計の外観が示されているが、データ送信装置１００の外観はこれに限られず据え置き型の血圧計であってもよいし、他の生体情報または活動情報に関する量を測定するセンサ装置であり得る。

[0096] ＜２＞

（ハードウェア構成）

上記の実施形態では、データ送信装置１００は、図２に示すように、出力装置２１１、入力装置２１２、制御部２１３、記憶部２１４、ドライブ２１５、外部インタフェース２１６、通信インタフェース２１７、及び電池２１８が電気的に接続されたコンピュータを含んでいる。しかしながら、この他にさらに種々の情報処理を行うための装置を備えていてもよい。例えば、データ送信装置１００は、さらに、気圧センサ及び温湿度センサを備えていてもよい。

[0097] 加速度センサは、生体の動きを検出し、その動き情報を制御部２１３へ渡す。加速度センサは、例えば、３軸加速度センサであり、生体の加速度を線型独立な３軸（例えば、互いに直交した３軸）に関して検出する。そして、

計時装置２２０は、３方向の加速度を表す加速度信号を制御部２１３へ出力する。

気圧センサは、気圧を検出し、気圧データを制御部２１３へ出力する。

温湿度センサは、データ送信装置１００の周辺の環境温度及び環境湿度を計測し、温度及び湿度データを制御部２１３へ出力する。

[0098] また、データ送信装置１００は、ＧＰＳ受信機を備えていてもよい。ＧＰＳ受信機は、複数のＧＰＳ衛星から送信されるＧＰＳ信号をそれぞれ受信し、受信したＧＰＳ信号を制御部２１３へ出力する。制御部２１３は、上記各ＧＰＳ信号を基に測距演算を行うことで、データ送信装置１００の現在位置情報、つまりデータ送信装置１００を装着している被測定者（ユーザ）の位置を算出する。

[0099] なお、この場合、電池２１８は、例えば、出力装置２１１、制御部２１３、記憶部２１４、気圧センサ、温湿度センサ、通信インタフェース２１７、生体センサ２１９、計時装置２２０、及びＧＰＳ受信機へ電力を供給する。

以上の変形例のハードウェア構成は、データ受信装置１５０も備えてもよい。この場合、ＧＰＳによる位置情報、気圧データ、及び温度及び湿度データを、センサデータに含めて、これらの情報を含んだ暗号鍵を使用してもよい。

[0100] ＜３＞

（ソフトウェア構成）

本実施形態に係るデータ送信装置１００は、活動量測定部、歩数計測部、睡眠状態計測部、及び、環境（温度及び湿度）計測部をさらに備えるコンピュータとして機能してもよい。記憶部２１４は、例えば、それぞれに対応するプログラム（活動量測定プログラム、歩数計測プログラム、睡眠状態計測プログラム、及び、環境（温度及び湿度）計測プログラム）を記憶し、必要なプログラムを実行する際に、所望のプログラムをＲＡＭに展開する。そして、制御部２１３は、ＲＡＭに展開されたプログラムをＣＰＵにより解釈及び実行して、各構成要素を制御する。

[0101] 活動量測定部は、加速度センサより加速度を検出し、活動量を算出する。活動量測定部は、加速度信号を用いて、被測定者の歩行だけでなく、家事やデスクワークなどの様々な活動における活動量を算出することができる。活動量は、例えば、歩行距離、消費カロリー、または、脂肪燃焼量などの被測定者の活動に関連する指標である。

[0102] 歩数計測部は、加速度センサにより加速度、気圧センサにより気圧を検出し、歩数、早歩き歩数、階段上り歩数を算出する。加速度信号を用いて、被測定者の歩行を算出する。歩数計測部は、気圧データ及び加速度信号を用いて、被測定者の歩数、早歩き歩数、及び、階段上り歩数などを算出することができる。

[0103] 睡眠状態計測部は、加速度センサにより加速度を検出し、加速度信号によって寝返りの状態を検出することで、睡眠状態を推定することができる。

[0104] 環境（温度及び湿度）計測部は、温湿度センサにより計測された環境温度及び環境湿度を示す環境データを温湿度センサにおける計測時刻と紐づけて記憶部２１４に記憶させる。気温（気温の変化）は、例えば、人間の血圧変動を引き起こしうる要素の１つとして考えられる。このため、環境データは、被測定者の血圧変動の要因となりうる情報である。

[0105] 以上の変形例のソフトウェア構成は、データ受信装置１５０も備えてもよい。この場合、活動量、階段上り歩数、及び睡眠状態を含んだ情報を含めた暗号鍵を使用してもよい。

[0106] ＜４＞

データ送信装置１００は、データ受信装置１５０と別体で構成されている。しかしながら、データ送信装置１００及びデータ受信装置１５０の構成はこのような例に限定されなくてもよく、データ送信装置１００及びデータ受信装置１５０の両方の機能を有するシステムを１台のコンピュータで実現してもよい。

[0107] ＜５＞

入力装置２１２に含まれる操作部が押される（オンされる）と、データ送

信装置１００は生体情報の測定が開始されてもよい。そして、測定が終了後、図６の動作が続いてもよい

[0108] ＜６＞

上述の実施形態では、血圧測定について記載したが、本実施形態に適用可能な血圧測定方式について説明する。一般的な手法としては、カフ構造体を使用してオシロメトリック方式によりユーザの血圧値を測定する手法がある。しかしながら、血圧値を測定するだけの場合にはこれに限らなくてもよい。例えば、圧脈波を心拍ごとに検出する圧脈波センサを備え、被測定部位（例えば、左手首）を通る橈骨動脈の圧脈波を検出して血圧値（収縮期血圧値と拡張期血圧値）を測定してもよい（トノメトリ方式）。圧脈波センサは、被測定部位（例えば、左手首）を通る橈骨動脈の脈波をインピーダンスの変化として検出して血圧値を測定してもよい（インピーダンス方式）。圧脈波センサは、被測定部位のうち対応する部分を通る動脈へ向けて光を照射する発光素子と、その光の反射光（または透過光）を受光する受光素子とを備えて、動脈の脈波を容積の変化として検出して血圧値を測定してもよい（光電方式）。また、圧脈波センサは、被測定部位に当接された圧電センサを備えて、被測定部位のうち対応する部分を通る動脈の圧力による歪みを電気抵抗の変化として検出して血圧値を測定してもよい（圧電方式）。さらに、圧脈波センサは、被測定部位のうち対応する部分を通る動脈へ向けて電波（送信波）を送る送信素子と、その電波の反射波を受信する受信素子とを備えて、動脈の脈波による動脈とセンサとの間の距離の変化を送信波と反射波との間の位相のずれとして検出して血圧値を測定してもよい（電波照射方式）。なお、血圧値を算出することができる物理量を観測することができれば、これらの以外の方式を適用してもよい。

[0109] ＜７＞

本発明の装置は、コンピュータとプログラムによっても実現でき、プログラムを記録媒体（または記憶媒体）に記録することも、ネットワークを通して提供することも可能である。

また、以上の各装置及びそれらの装置部分は、それぞれハードウェア構成、またはハードウェア資源とソフトウェアとの組み合せ構成のいずれでも実施可能となっている。組み合せ構成のソフトウェアとしては、予めネットワークまたはコンピュータ読み取り可能な記録媒体（または記憶媒体）からコンピュータにインストールされ、当該コンピュータのプロセッサに実行されることにより、各装置の機能を当該コンピュータに実現させるためのプログラムが用いられる。

[0110] なお、この発明は、上記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上記実施形態に開示されている複数の構成要素の適宜な組み合せにより種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。さらに、異なる実施形態に亘る構成要素を適宜組み合せてもよい。

[0111] また、「及び／または」とは、「及び／または」でつながれて列記される事項のうちの任意の１つ以上の事項という意味である。具体例を挙げると、「ｘ及び／またはｙ」とは、３要素からなる集合｛（ｘ），（ｙ），（ｘ，ｙ）｝のうちのいずれかの要素という意味である。もう１つの具体例を挙げると、「ｘ、ｙ、及び／またはｚ」とは、７要素からなる集合｛（ｘ），（ｙ），（ｚ），（ｘ，ｙ），（ｘ，ｚ），（ｙ，ｚ），（ｘ，ｙ，ｚ）｝のうちのいずれかの要素という意味である。

[0112] ＜８＞

また、上記の実施形態の一部または全部は、以下の付記のようにも記載されうるが、以下には限られない。

[0113] （付記１）

ハードウェアプロセッサと、メモリとを備える生体の情報に関する量を測定するデータ送信装置であって、

前記ハードウェアプロセッサは、

生体の情報に関する量を測定し、

受信装置との間で共有できる第１共有情報及び第２共有情報から算出される情報を暗号鍵として生成し、

前記暗号鍵を使用して前記生体の情報を暗号化し暗号化データを生成し、

前記第１共有情報及び前記暗号化データを含む片方向送信用のパケットを生成し、

前記パケットを送信するように構成され、

前記メモリは、

前記第１共有情報及び前記暗号化データを記憶する記憶部と、を備えるデータ送信装置。

[0114] （付記２）

ハードウェアプロセッサと、メモリとを備える生体の情報に関する量を測定するデータ受信装置であって、

前記ハードウェアプロセッサは、

暗号化されたデータである暗号化データと、送信装置との間で共有できる第１共有情報を含む片方向送信用のパケットを受信し、

前記第１共有情報に基づいて、送信装置との間で共有する第２共有情報から算出される情報を暗号鍵として決定し、

前記パケットに含まれる暗号化データを、前記暗号鍵を使用して復号し、前記送信装置で測定された生体の情報を含む復号データを生成するように構成され、

前記メモリは、

前記第１共有情報及び前記復号データを記憶する記憶部と、を備えるデータ受信装置。

[0115] （付記３）

少なくとも１つのハードウェアプロセッサを用いて、生体の情報に関する量を測定し、

少なくとも１つのハードウェアプロセッサを用いて、受信装置との間で共有できる第１共有情報及び第２共有情報から算出される情報を暗号鍵として

生成し、

少なくとも１つのハードウェアプロセッサを用いて、前記暗号鍵を使用して前記生体の情報を暗号化し暗号化データを生成し、

少なくとも１つのハードウェアプロセッサを用いて、前記第１共有情報及び前記暗号化データを含む片方向送信用のパケットを生成し、

少なくとも１つのハードウェアプロセッサを用いて、前記パケットを送信することを備えるデータ送信方法。

[0116] （付記４）

少なくとも１つのハードウェアプロセッサを用いて、暗号化されたデータである暗号化データと、送信装置との間で共有できる第１共有情報を含む片方向送信用のパケットを受信し、

少なくとも１つのハードウェアプロセッサを用いて、前記第１共有情報に基づいて、送信装置との間で共有する第２共有情報から算出される情報を暗号鍵として決定し、

少なくとも１つのハードウェアプロセッサを用いて、前記パケットに含まれる暗号化データを、前記暗号鍵を使用して復号し、前記送信装置で測定された生体の情報を含む復号データを生成することを備えるデータ受信方法。

符号の説明

[0117] １００…データ送信装置

１０１…センサ

１０２…センサデータ記憶部

１０３…計時部

１０４…暗号鍵生成部

１０５…暗号化部

１０６…パケット生成部

１０７…送信部

１０８…第２共有情報記憶部

１０９…第１共有情報生成部

１５０…データ受信装置

１５１…計時部

１５２…鍵情報記憶部

１５３…受信部

１５４…暗号鍵決定部

１５５…復号部

１５６…第１共有情報抽出部

２１１…出力装置

２１２…入力装置

２１３…制御部

２１４…記憶部

２１５…ドライブ

２１６…外部インタフェース

２１７…通信インタフェース

２１８…電池

２１９…生体センサ

２２０…計時装置

３１１…出力装置

３１２…入力装置

３１３…制御部

３１４…記憶部

３１５…ドライブ

３１６…外部インタフェース

３１７…通信インタフェース

３１８…電池

３１９…計時装置

３２０…動きセンサ

４０１…生体情報測定部

４０２…記憶制御部

４０３…暗号鍵生成部

４０４…暗号化部

４０５…パケット生成部

４０６…送信部

４０７…第１共有情報生成部

５０１…記憶制御部

５０２…受信部

５０３…暗号鍵決定部

５０４…復号部

５０５…第１共有情報抽出部

１１００…データ構造

１１０１…ＩＤフィールド

１１０２…センサデータ測定日時フィールド

１１０３…暗号データフィールド

１２００…サーバ

請求の範囲

[請求項1] 生体の情報に関する量を測定する測定制御部と、

受信装置との間で共有できる第１共有情報及び第２共有情報から算出される情報を暗号鍵として生成する暗号鍵生成制御部と、

前記暗号鍵を使用して前記生体の情報を暗号化し暗号化データを生成する暗号化制御部と、

前記第１共有情報及び前記暗号化データを含む片方向送信用のパケットを生成するパケット生成制御部と、

前記パケットを送信する送信部と、を備える、データ送信装置。

[請求項2] 前記第１共有情報、第２共有情報及び前記算出される情報は、前記生体の情報を含まない、請求項１に記載のデータ送信装置。

[請求項3] 前記暗号鍵生成制御部は、前記第１共有情報に日時を対応付け、前記第２共有情報に予め設定した日時を対応付ける請求項２に記載のデータ送信装置。

[請求項4] 前記第１共有情報に対応付けられる日時は、前記生体の情報に関する量を測定した日時を含む、請求項３に記載のデータ送信装置。

[請求項5] 前記第１共有情報及び第２共有情報から算出される情報は、第２共有情報で決まる日時から前記第１共有情報に対応付けられる日時までの経過期間を含む、請求項３または４に記載のデータ送信装置。

[請求項6] 前記生体の情報は、血圧値、及び脈拍の少なくとも１つを含む、請求項１乃至５のいずれか１項に記載のデータ送信装置。

[請求項7] 暗号化されたデータである暗号化データと、送信装置との間で共有できる第１共有情報を含む片方向送信用のパケットを受信する受信部と、

前記第１共有情報に基づいて、送信装置との間で共有する第２共有情報から算出される情報を暗号鍵として決定する暗号鍵決定制御部と、

前記パケットに含まれる暗号化データを、前記暗号鍵を使用して復

号し復号データを生成する復号制御部と、を備え、

前記復号データは、前記送信装置で測定された生体の情報を含む、データ受信装置。

[請求項8] 前記第１共有情報、第２共有情報及び前記算出される情報は、前記生体の情報を含まない、請求項７に記載のデータ受信装置。

[請求項9] 前記第１共有情報は、前記送信装置で前記生体の情報に関する量を測定した日時であり、

前記暗号鍵決定制御部は、前記生体の情報に関する量を測定した日時に基づいて、前記第２共有情報から前記暗号鍵を決定する、請求項７または８に記載のデータ受信装置。

[請求項10] 前記第１共有情報及び第２共有情報から算出される情報は、第２共有情報で決まる日時から第１共有情報に対応付けられる日時までの経過期間を含む、請求項９に記載のデータ受信装置。

[請求項11] 前記生体の情報は、血圧値、及び脈拍の少なくとも１つを含む、請求項７乃至９のいずれか１項に記載のデータ受信装置。

[請求項12] 生体の情報に関する量を測定し、

受信装置との間で共有できる第１共有情報及び第２共有情報から算出される情報を暗号鍵として生成し、

前記暗号鍵を使用して前記生体の情報を暗号化し暗号化データを生成し、

前記第１共有情報及び前記暗号化データを含む片方向送信用のパケットを生成し、

前記パケットを送信すること、を備える、データ送信方法。

[請求項13] 暗号化されたデータである暗号化データと、送信装置との間で共有できる第１共有情報を含む片方向送信用のパケットを受信し、

前記第１共有情報に基づいて、送信装置との間で共有する第２共有情報から算出される情報を暗号鍵として決定し、

前記パケットに含まれる暗号化データを、前記暗号鍵を使用して復

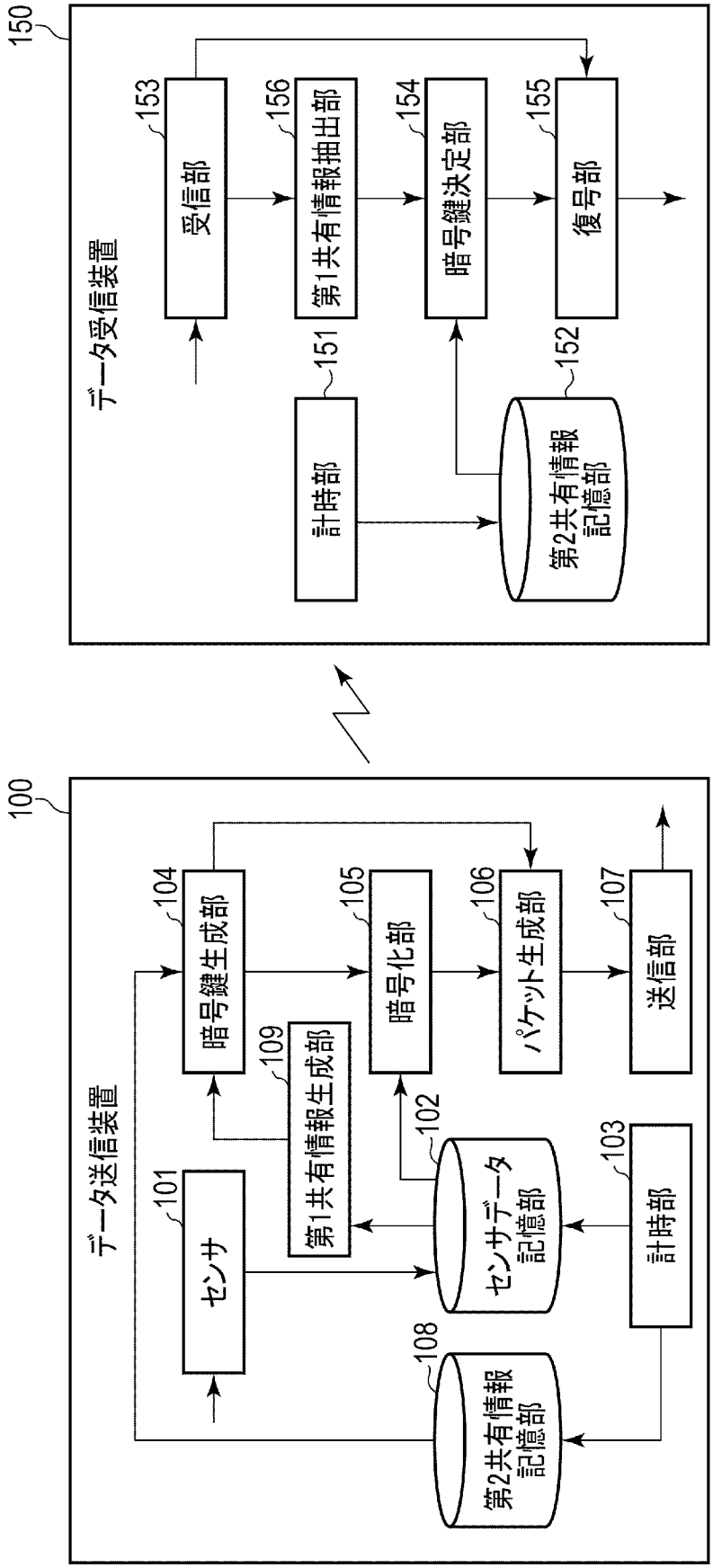
号し復号データを生成すること、を備え、

前記復号データは、前記送信装置で測定された生体の情報を含む、データ受信方法。

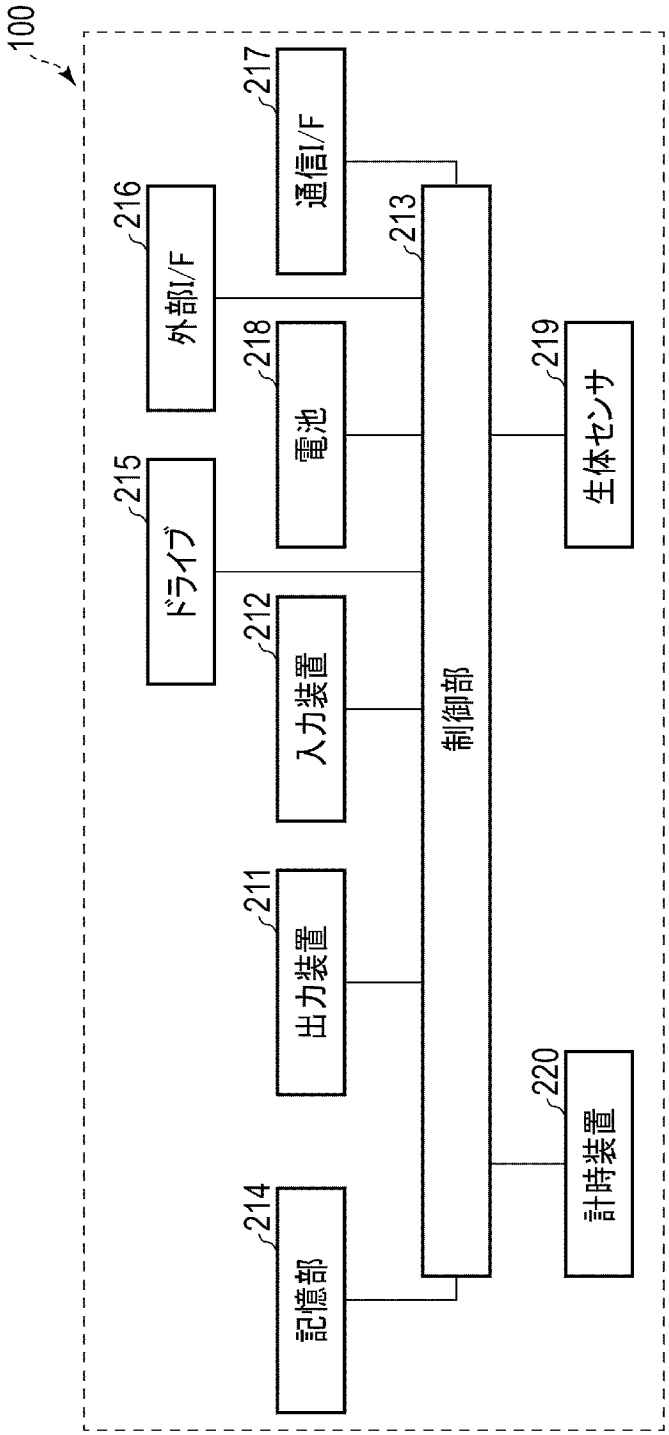
[請求項14] コンピュータを、請求項１乃至６のいずれか１項に記載のデータ送信装置が備える各制御部として機能させるためのプログラム。

[請求項15] コンピュータを、請求項７乃至１１のいずれか１項に記載のデータ受信装置が備える各制御部として機能させるためのプログラム。

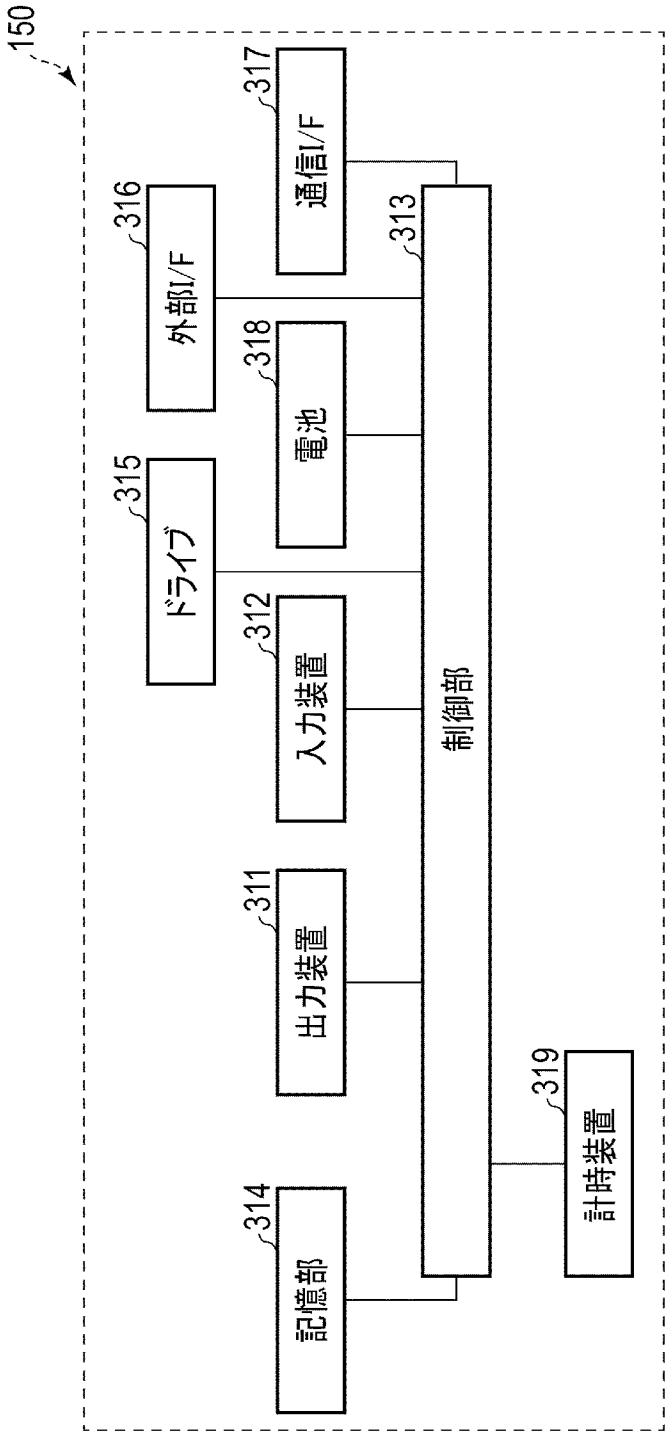
[図1]


150
データ受信装置
153
受信部
156
第1共有情報抽出部
154
暗号鍵決定部
155
復号部
151
計時部
152
第2共有情報
記憶部
100
データ送信装置
104
暗号鍵生成部
105
暗号化部
106
パケット生成部
107
送信部
109
第1共有情報生成部
102
センサデータ
記憶部
101
センサ
103
計時部
108
第2共有情報
記憶部

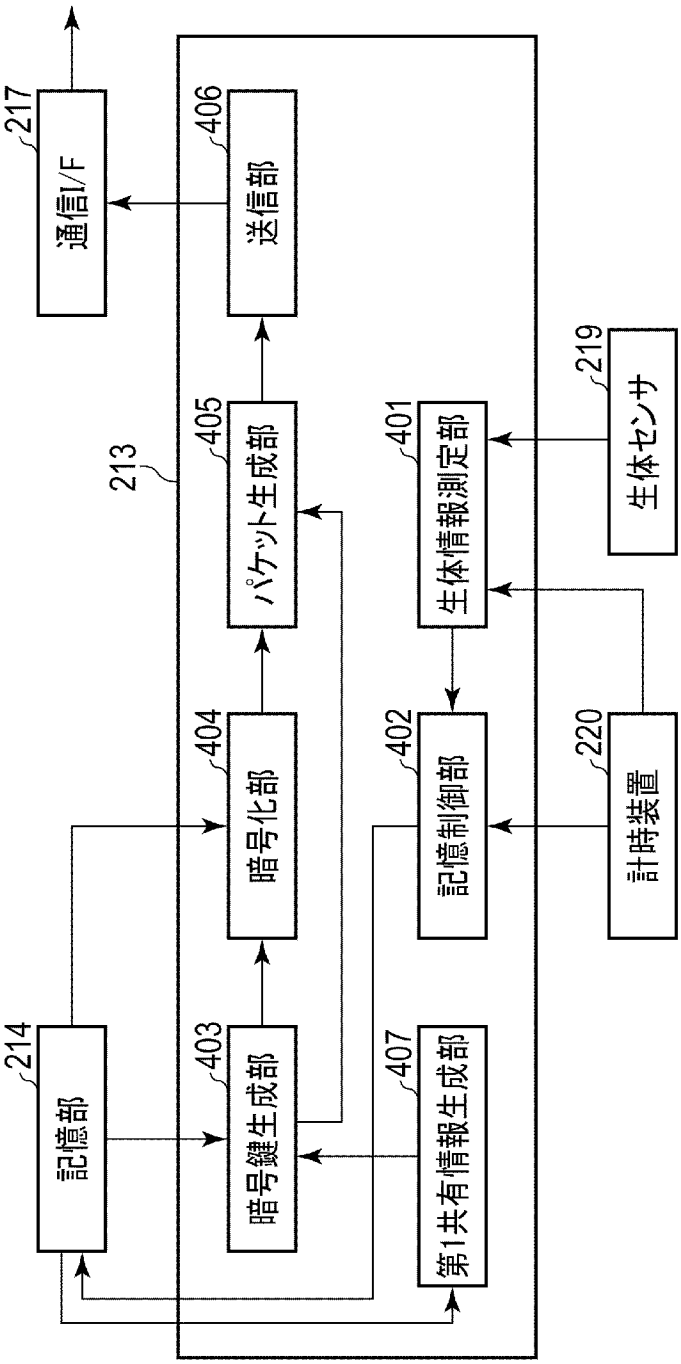
[図2]


100
217
通信I/F
216
外部I/F
213
218
電池
219
生体センサ
215
ドライブ
212
入力装置
制御部
211
出力装置
220
計時装置
214
記憶部

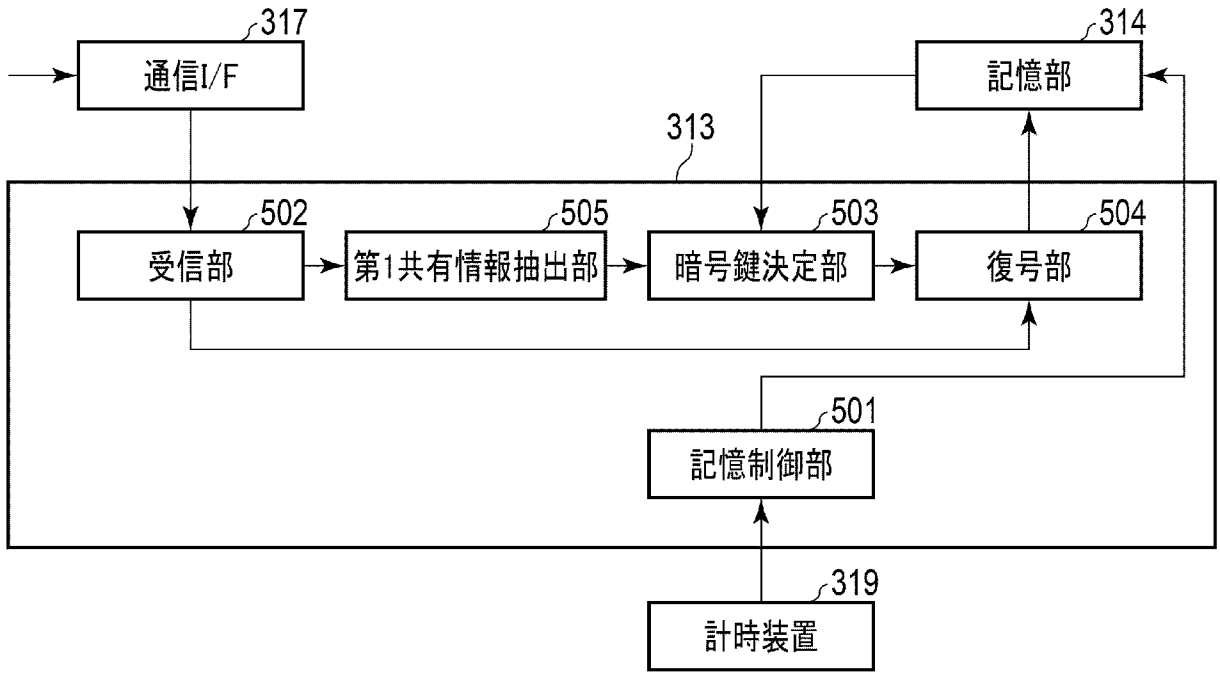
[図3]


150
317
通信I/F
316
外部I/F
313
318
電池
315
ドライブ
312
入力装置
制御部
311
出力装置
319
計時装置
314
記憶部

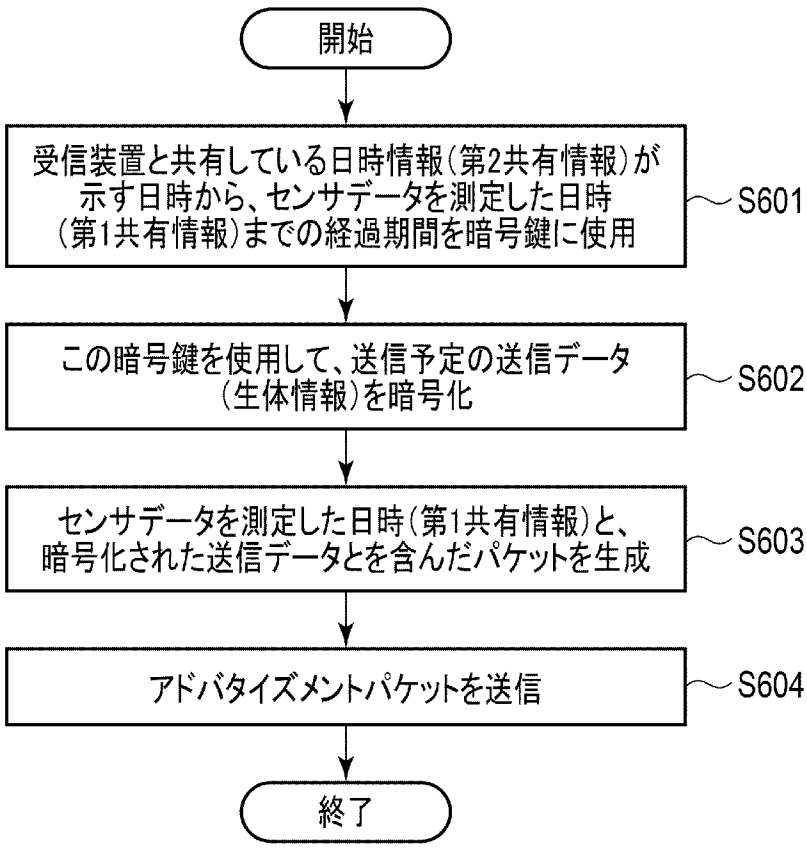
[図4]


217
通信I/F
406
送信部
213
405
パケット生成部
401
生体情報測定部
219
生体センサ
404
暗号化部
402
記憶制御部
220
計時装置
214
記憶部
403
暗号鍵生成部
407
第1共有情報生成部

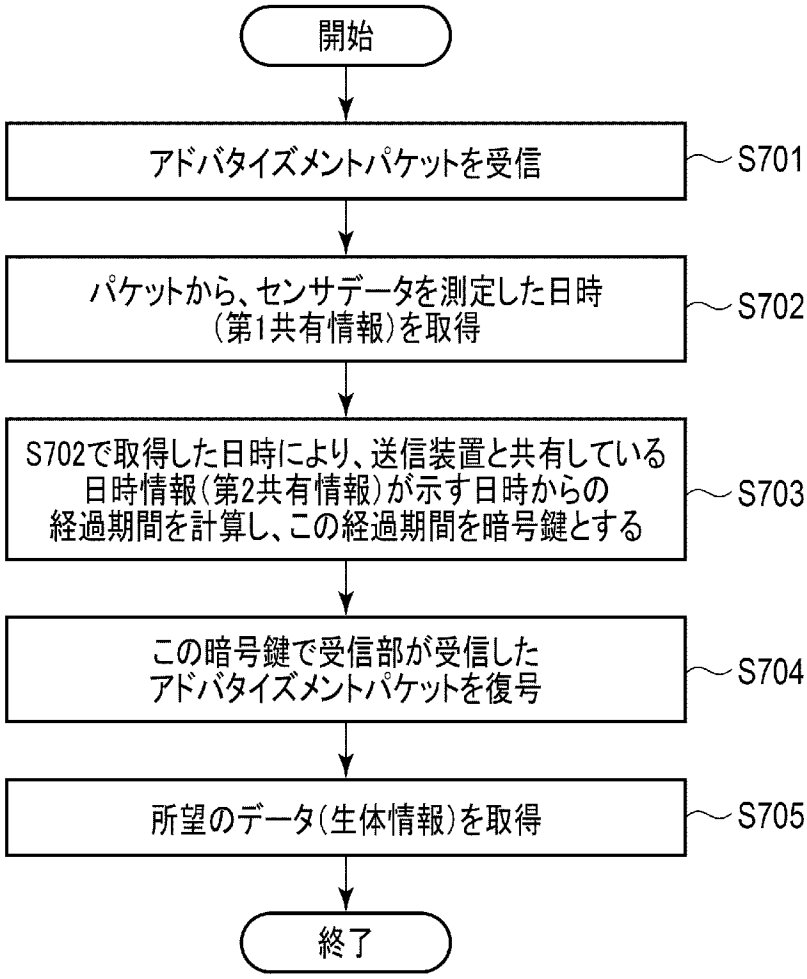
[図5]


317
通信I/F
314
記憶部
313
502
受信部
505
第1共有情報抽出部
503
暗号鍵決定部
504
復号部
501
記憶制御部
319
計時装置

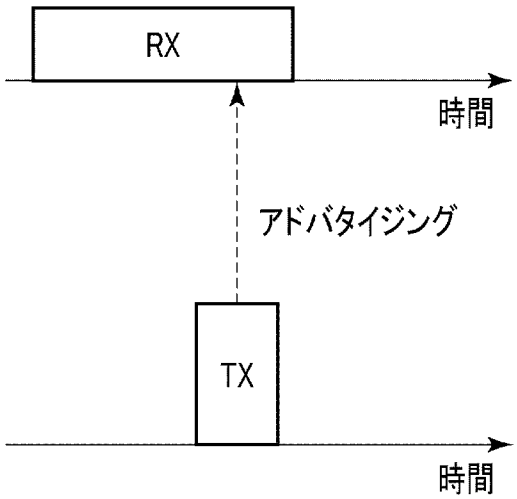
[図6]


開始
受信装置と共有している日時情報(第2共有情報)が示す日時から、センサデータを測定した日時(第1共有情報)までの経過期間を暗号鍵に使用
S601
この暗号鍵を使用して、送信予定の送信データ(生体情報)を暗号化
S602
センサデータを測定した日時(第1共有情報)と、暗号化された送信データとを含んだパケットを生成
S603
アドバタイズメントパケットを送信
S604
終了

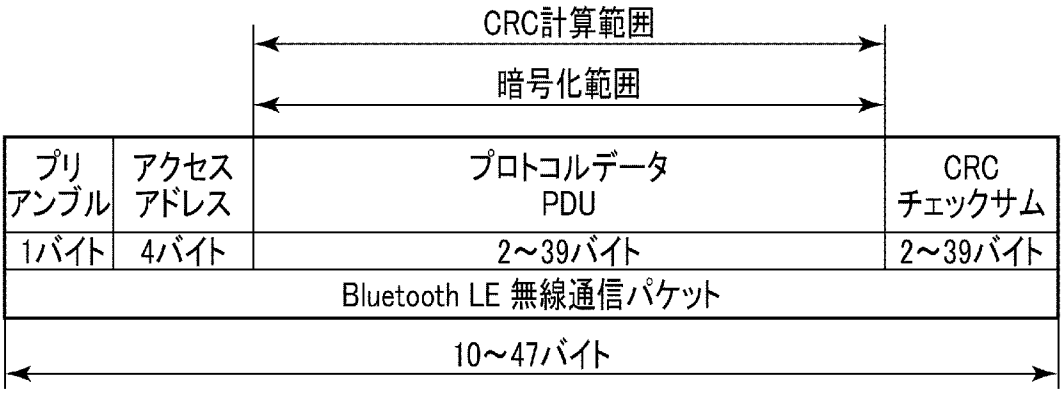
[図7]


開始
アドバタイズメントパケットを受信
S701
パケットから、センサデータを測定した日時
(第1共有情報)を取得
S702
S702で取得した日時により、送信装置と共有している
日時情報(第2共有情報)が示す日時からの
経過期間を計算し、この経過期間を暗号鍵とする
S703
この暗号鍵で受信部が受信した
アドバタイズメントパケットを復号
S704
所望のデータ(生体情報)を取得
S705
終了

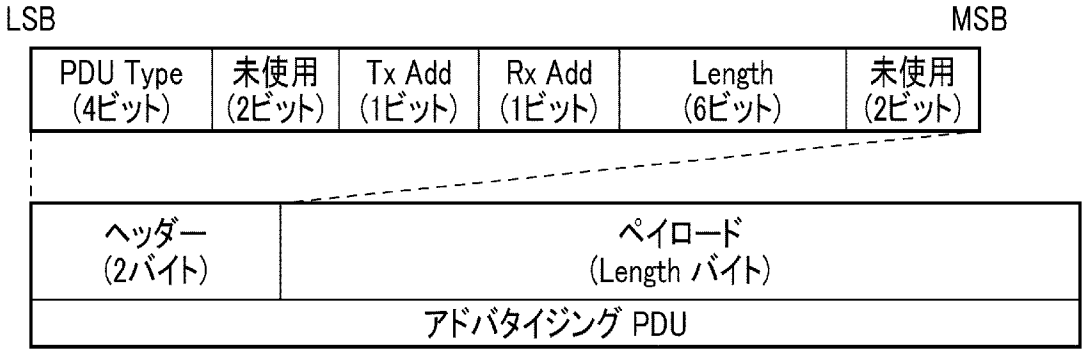
[図8]


RX
時間
アドバタイジング
TX
時間

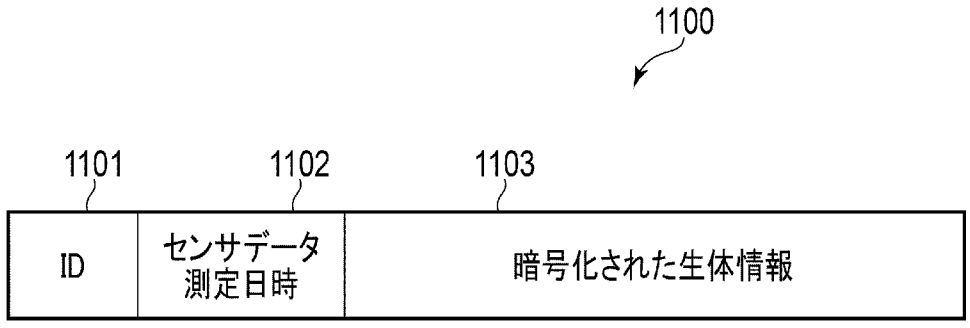
[図9]


CRC計算範囲
暗号化範囲
プリアンブル
アクセスアドレス
プロトコルデータPDU
CRCチェックサム
1バイト
4バイト
2～39バイト
2～39バイト
Bluetooth LE 無線通信パケット
10～47バイト

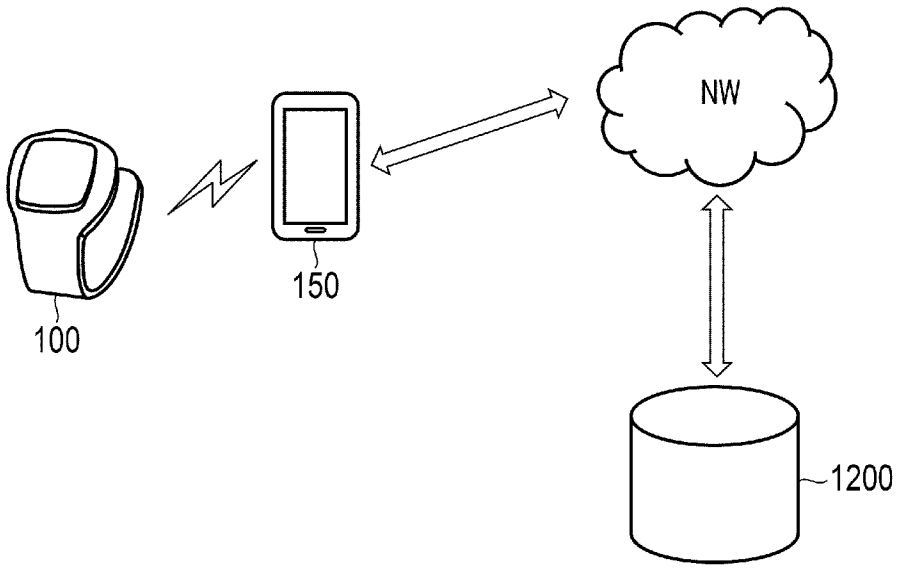
[図10]


LSB
MSB
PDU Type (4ビット)
未使用 (2ビット)
Tx Add (1ビット)
Rx Add (1ビット)
Length (6ビット)
未使用 (2ビット)
ヘッダー (2バイト)
ペイロード (Length バイト)
アドバタイジング PDU

[図11]


1100
1101
1102
1103
ID
センサデータ測定日時
暗号化された生体情報

[図12]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/028827

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. H04L9/08(2006.01)i, G06F21/60(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl. H04L9/08, G06F21/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2018
Registered utility model specifications of Japan	1996-2018
Published registered utility model applications of Japan	1994-2018

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2016/0080372 A1 (NYMI INC.) 17 March 2016, paragraphs [0026]-[0134], [0186]-[0201], [0212], [0226]-[0240]	1-15
Y	JP 2000-224158 A (TOYO COMMUNICATION EQUIPMENT CO., LTD.) 11 August 2000, paragraphs [0002], [0003]	1-15
Y	JP 2002-111652 A (RPK NEW ZEALAND LTD.) 12 April 2002, paragraphs [0007]-[0013]	1-15

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 October 2018 (29.10.2018)	06 November 2018 (06.11.2018)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/028827

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2011-120051 A (PANASONIC CORP.) 16 June 2011, paragraphs [0037]-[0060]	1-15
Y	US 2016/0066212 A1 (ASHOKA SATHANUR VISWESWARA) 03 March 2016, paragraphs [0032]-[0049]	1-15
Y	JP 2017-67735 A (INFORMATION SSEVICES INTERNATIONAL-DENTSU, LTD.) 06 April 2017, paragraphs [0019]-[0061]	1-15
Y	JP 2016-519861 A (TOMTOM SOFTWARE LIMITED) 07 July 2016, paragraphs [0007]-[0009], [0014], [0015], [0115]-[0123]	1-15
Y	JP 2006-122610 A (IPSQUARE INC.) 18 May 2006, paragraphs [0001]-[0049]	6, 11, 14, 15

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2018/028827

US 2016/0080372 A1	17 March 2016	EP 3076585 A1 05 October 2016 CA 2898609 A1 18 February 2016
JP 2000-224158 A	11 August 2000	Family: none
JP 2002-111652 A	12 April 2002	US 2002/0025045 A1, 28 February 2002 paragraphs [0024]-[0035] EP 1195968 A2 10 April 2002 NZ 506002 A 31 January 2003 AU 5592601 A 31 January 2002
JP 2011-120051 A	16 June 2011	US 2012/0201383 A1, 09 August 2012 paragraphs [0034]-[0057] WO 2011/067876 A1 09 June 2011
US 2016/0066212 A1	03 March 2016	Family: none
JP 2017-67735 A	06 April 2017	Family: none
JP 2016-519861 A	07 July 2016	US 2016/0029148 A1, 28 January 2016 paragraphs [0120]-[0126], [0144]-[0152] WO 2014/135711 A1 12 September 2014 EP 2965563 A1 13 January 2016 CN 105210420 A 30 December 2015
JP 2006-122610 A	18 May 2006	Family: none

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１８／０２８８２７

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08(2006.01)i, G06F21/60(2013.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08, G06F21/60

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１８年
日本国実用新案登録公報	１９９６－２０１８年
日本国登録実用新案公報	１９９４－２０１８年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	US 2016/0080372 A1 (NYMI INC.) 2016.03.17, 段落[0026]-[0134],[0186]-[0201],[0212],[0226]-[0240]	1-15
Y	JP 2000-224158 A（東洋通信機株式会社）2000.08.11, 段落[0002],[0003]	1-15
Y	JP 2002-111652 A（アールピーケー　ニュージーランド　リミティド）2002.04.12, 段落[0007]-[0013]	1-15

☑　Ｃ欄の続きにも文献が列挙されている。

☑　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
２９．１０．２０１８	０６．１１．２０１８

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　９３６４
中里　裕正
電話番号　０３－３５８１－１１０１　内線　３５４６

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	JP 2011-120051 A (パナソニック株式会社) 2011.06.16, 段落[0037]-[0060]	1-15
Y	US 2016/0066212 A1 (ASHOKA SATHANUR VISWESWARA) 2016.03.03, 段落[0032]-[0049]	1-15
Y	JP 2017-67735 A (株式会社電通国際情報サービス) 2017.04.06, 段落[0019]-[0061]	1-15
Y	JP 2016-519861 A (トムトム　ソフトウェア　リミテッド) 2016.07.07, 段落[0007]-[0009],[0014],[0015],[0115]-[0123]	1-15
Y	JP 2006-122610 A (株式会社アイピースクエア) 2006.05.18, 段落[0001]-[0049]	6,11,14,15

US 2016/0080372 A1	2016.03.17	EP 3076585 A1	2016.10.05
		CA 2898609 A1	2016.02.18
JP 2000-224158 A	2000.08.11	ファミリーなし	
JP 2002-111652 A	2002.04.12	US 2002/0025045 A1, 段落[0024]-[0035]	2002.02.28
		EP 1195968 A2	2002.04.10
		NZ 506002 A	2003.01.31
		AU 5592601 A	2002.01.31
JP 2011-120051 A	2011.06.16	US 2012/0201383 A1, 段落[0034]-[0057]	2012.08.09
		WO 2011/067876 A1	2011.06.09
US 2016/0066212 A1	2016.03.03	ファミリーなし	
JP 2017-67735 A	2017.04.06	ファミリーなし	
JP 2016-519861 A	2016.07.07	US 2016/0029148 A1, 段落[0120]-[0126], [0144]-[0152]	2016.01.28
		WO 2014/135711 A1	2014.09.12
		EP 2965563 A1	2016.01.13
		CN 105210420 A	2015.12.30
JP 2006-122610 A	2006.05.18	ファミリーなし	