(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
2021年4月8日(08.04.2021)

WIPO | PCT

(10) 国際公開番号
WO 2021/065754 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/JP2020/036470

(22) 国際出願日： 2020年9月25日(25.09.2020)

(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 2019-180829 2019年9月30日(30.09.2019) JP

(71) 出願人: ダイキン工業株式会社 (**DAIKIN INDUSTRIES, LTD.**) [JP/JP]; 〒5308323 大阪府大阪市北区中崎西２丁目４番１２号梅田センタービル Osaka (JP).

(72) 発明者: 呼元 文数(**YOBIMOTO, Fumikazu**). 東山 伸(**HIGASHIYAMA, Shin**).

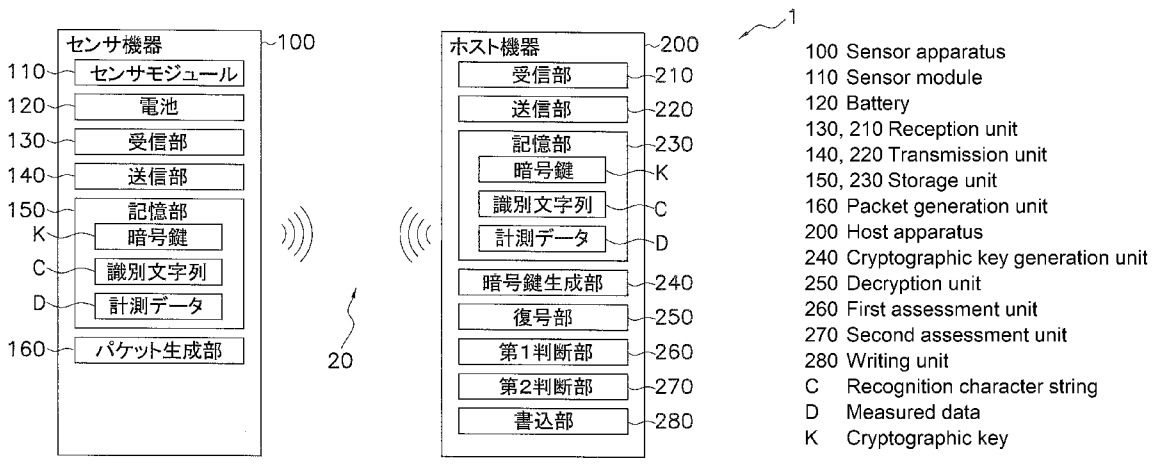
(74) 代理人: 新樹グローバル・アイピー特許業務法人(**SHINJYU GLOBAL IP**); 〒5300054 大阪府大阪市北区南森町１丁目４番１９号サウスホレストビル Osaka (JP).

(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, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, 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,

(54) **Title:** DATA COLLECTION DEVICE AND DATA COLLECTION METHOD

(54) 発明の名称： データ収集システム及びデータ収集方法

[図2]



(57) **Abstract:** Provided is a data collection system comprising a host apparatus and a sensor apparatus for transmitting measured data to the host apparatus via a network, the data collection system being capable of secure communication between the host apparatus and the sensor apparatus and being capable of suppressing the power consumption of the sensor apparatus. A data collection system (1) is provided with a host apparatus (200) and a battery-driven sensor apparatus (100) for transmitting measured data (D) to the host apparatus via a network (20). The host apparatus has a cryptographic key generation unit (240) for generating a cryptographic key that is specific to the sensor apparatus, a storage unit (230) for storing the cryptographic key, a transmission unit (220) for transmitting the cryptographic key to the sensor apparatus using a public-key cryptography infrastructure, and a reception unit (210) for receiving the measured data of the sensor apparatus. The sensor apparatus has a reception unit (130) for receiving the cryptographic key transmitted by the host apparatus, a packet generation unit (160) for generating a packet that includes the measured data that has been encrypted

WO 2021/065754 A1

[続葉有]

QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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:

— 国際調査報告(条約第21条(3))

by the cryptographic key, and a transmission unit (140) for transmitting the packet by broadcast.

(57) 要約:ホスト機器と、ネットワークを介してホスト機器に計測データを送信するセンサ機器とを備え、ホスト機器とセンサ機器との間のセキュアな通信が可能で、センサ機器の電力消費を抑制可能なデータ収集システムを提供する。データ収集システム(1)は、ホスト機器(200)と、ネットワーク(20)を介してホスト機器に計測データ(D)を送信する電池駆動式のセンサ機器(100)とを備える。ホスト機器は、センサ機器に固有の暗号鍵を生成する暗号鍵生成部(240)、暗号鍵を記憶する記憶部(230)、公開鍵暗号基盤を用いてセンサ機器に暗号鍵を送信する送信部(220)、及びセンサ機器の計測データを受信する受信部(210)を有する。センサ機器は、ホスト機器の送信する暗号鍵を受信する受信部(130)、暗号鍵で暗号化した計測データを含むパケットを生成するパケット生成部(160)、及びパケットをブロードキャストで送信する送信部(140)を有する。

明　細　書

発明の名称 ： データ収集システム及びデータ収集方法

技術分野

[0001] ホスト機器と、ホスト機器とネットワークを介して接続され、ホスト機器に計測データを送信するセンサ機器とを備えるデータ収集システム、及び、データ収集方法に関する。

背景技術

[0002] ホスト機器と、ホスト機器とネットワークを介して接続されるセンサ機器とを備え、センサ機器の計測データをホスト機器で受信して収集するデータ収集システムが様々な目的で利用されている（例えば、特許文献１（特開２００５－１８２４４１号公報））。

[0003] このようなデータ収集システムでは、本来のセンサ機器以外の機器から偽の情報が送信されるなりすましや、データの盗聴や改ざん等の問題を避けるため、セキュリティ対策が重要となる。

発明の概要

発明が解決しようとする課題

[0004] そこで、セキュアな通信を実現するために、公開鍵暗号基盤を利用した通信を利用することが考えられる。しかし、公開鍵暗号基盤を利用する通信は、通信シーケンスが多いため、電力消費が比較的大きい。センサ機器には、電池が供給する電力や環境発電素子が発電する電力を用いる等の理由で、利用可能な電力に限りがある機器も多いため、電力消費が大きい場合、頻繁に電池交換が必要になる、データ送信に必要な電力が不足する等の不具合が発生する可能性がある。センサ機器が計測データを比較的頻繁に送信する場合、このような問題が特に顕著となる。

課題を解決するための手段

[0005] 第１観点に係るデータ収集システムは、ホスト機器と、センサ機器と、を備える。センサ機器は、ホスト機器とネットワークを介して接続される。セ

ンサ機器は、ホスト機器に計測データを送信する。センサ機器は、電池又は環境発電素子を有し、電池が供給する電力又は環境発電素子が発電する電力で駆動される。ホスト機器は、暗号鍵生成部と、ホスト側記憶部と、暗号鍵送信部と、計測データ受信部と、を有する。暗号鍵生成部は、センサ機器に固有の暗号鍵を生成する。ホスト側記憶部は、暗号鍵生成部が生成した暗号鍵を記憶する。暗号鍵送信部は、公開鍵暗号基盤を用いて、ネットワークを介して、センサ機器に暗号鍵を送信する。計測データ受信部は、センサ機器から計測データを受信する。センサ機器は、暗号鍵受信部と、センサ側記憶部と、パケット生成部と、パケット送信部と、を有する。暗号鍵受信部は、ホスト機器が送信する暗号鍵を受信する。センサ側記憶部は、暗号鍵受信部が受信する暗号鍵を記憶する。パケット生成部は、センサ側記憶部に記憶されている暗号鍵で計測データを暗号化し、暗号化した計測データを含むパケットを生成する。パケット送信部は、パケット生成部の生成するパケットをブロードキャストで送信する。

[0006] 第１観点のデータ収集システムでは、ホスト機器が公開鍵暗号基盤を用いてセキュアな環境でセンサ機器に暗号鍵を送信し、センサ機器はこの暗号鍵を用いて暗号化した計測データを、消費電力の比較的少ないブロードキャストで送信する。このため、第１観点のデータ収集システムでは、ホスト機器とセンサ機器との間のセキュアな通信環境と、センサ機器の省電力化と、を両立できる。

[0007] また、第１観点のデータ収集システムは、ブロードキャストを利用するため、１台のホスト機器で、理論上台数制限なく、多数のセンサ機器から計測データを収集できる。

[0008] 第２観点に係るデータ収集システムは、第１観点のデータ収集システムであって、ホスト機器とセンサ機器とはＢｌｕｅｔｏｏｔｈ（登録商標）規格を用いて通信を行う。暗号鍵送信部は、ホスト機器とセンサ機器とのペアリング時にセンサ機器に暗号鍵を送信する。パケット生成部は、暗号化した計測データを含むアドバタイズパケットをパケットとして生成する。

[0009] 第２観点のデータ収集システムでは、Ｂｌｕｅｔｏｏｔｈ（登録商標）規格を用いて、セキュアな通信環境と、センサ機器の省電力化と、を両立できる。

[0010] 第３観点に係るデータ収集システムは、第１観点又は第２観点のデータ収集システムであって、ホスト側記憶部及びセンサ側記憶部は、共通の識別文字列を記憶する。パケット生成部は、暗号化した計測データ及び識別文字列を含むパケットを生成する。

[0011] 第３観点のデータ収集システムでは、パケットにホスト機器及びセンサ機器が記憶する共通の識別文字列が含まれるので、セキュアなシステムが実現されやすい。

[0012] 第４観点に係るデータ収集システムは、第３観点のデータ収集システムであって、ホスト機器は、復号部と、第１判断部と、を更に備える。復号部は、暗号鍵を用いて、受信したパケットに含まれる、暗号化された計測データ及び識別文字列を復号する。第１判断部は、復号部により復号された識別文字列と、ホスト側記憶部に記憶されている識別文字列とが一致するか否かを判断する。

[0013] 第４観点のデータ収集システムでは、不適切な計測データが誤って収集される事態の発生を抑制できる。

[0014] 第５観点に係るデータ収集システムは、第４観点のデータ収集システムであって、第１判断部は、復号部により復号された識別文字列とホスト側記憶部に記憶されている識別文字列とが一致しないと判断した場合に、受信したパケットを、データ収集の対象外の機器の送信したパケットと判断する。

[0015] 第５観点のデータ収集システムでは、識別文字列の不一致に基づきデータ収集の対象外の機器が判断されるため、セキュアなシステムを実現できる。

[0016] 第６観点に係るデータ収集システムは、第１観点から第５観点のいずれかのデータ収集システムであって、ホスト機器は、第２判断部を更に備える。第２判断部は、計測データ受信部が受信する計測データの時間変化に基づき、受信した計測データがデータ収集の対象外の機器の送信した計測データで

あるか否かを判断する。

[0017] 第６観点のデータ収集システムでは、計測データの時間変化に基づいて、その計測データが、なりすまし機器（偽装デバイス）等のデータ収集の対象外の機器の送信した計測データであることを判断できる。

[0018] 第７観点に係るデータ収集システムは、ホスト機器と、センサ機器と、を備える。センサ機器は、ホスト機器とネットワークを介して接続される。センサ機器は、ホスト機器に計測データを送信する。センサ機器は、電池又は環境発電素子を有し、電池が供給する電力又は環境発電素子が発電する電力で駆動される。センサ機器は、暗号鍵生成部と、センサ側記憶部と、暗号鍵送信部と、パケット生成部と、パケット送信部と、を有する。暗号鍵生成部は、センサ機器に固有の暗号鍵を生成する。センサ側記憶部は、暗号鍵生成部が生成する暗号鍵を記憶する。暗号鍵送信部は、公開鍵暗号基盤を用いて、ネットワークを介して、ホスト機器に暗号鍵を送信する。パケット生成部は、センサ側記憶部に記憶されている暗号鍵で計測データを暗号化し、暗号化した計測データを含むパケットを生成する。パケット送信部は、パケット生成部の生成するパケットをブロードキャストで送信する。ホスト機器は、暗号鍵受信部と、ホスト側記憶部と、計測データ受信部と、を有する。暗号鍵受信部は、センサ機器が送信する暗号鍵を受信する。ホスト側記憶部は、暗号鍵受信部が受信する暗号鍵を記憶する。計測データ受信部は、センサ機器の送信する計測データを受信する。

[0019] 第７観点のデータ収集システムでは、センサ機器が公開鍵暗号基盤を用いてセキュアな環境でホスト機器に暗号鍵を送信し、センサ機器は自ら作成した暗号鍵を用いて暗号化した計測データを、消費電力の比較的少ないブロードキャストで送信する。このため、第７観点のデータ収集システムでは、ホスト機器とセンサ機器との間のセキュアな通信環境と、センサ機器の省電力化と、を両立できる。

[0020] また、第７観点のデータ収集システムでは、ブロードキャストを利用するため、１台のホスト機器で、理論上台数制限なく、多数のセンサ機器から計

測データを収集できる。

[0021] 第８観点に係るデータ収集方法は、センサ機器が送信する計測データを、センサ機器とネットワークを介して接続されるホスト機器で収集するデータ収集方法である。センサ機器は、電池又は環境発電素子を有し、電池の電力又は環境発電素子が発電する電力で駆動される。データ収集方法は、暗号鍵生成ステップと、第１記憶ステップと、暗号鍵送信ステップと、暗号鍵受信ステップと、第２記憶ステップと、パケット生成ステップと、パケット送信ステップと、を備える。暗号鍵生成ステップでは、ホスト機器が、センサ機器に固有の暗号鍵を生成する。第１記憶ステップでは、ホスト機器が、ホスト機器のホスト側記憶部に、生成されたセンサ機器に固有の暗号鍵を記憶する。暗号鍵送信ステップでは、ホスト機器が、公開鍵暗号基盤を用いて、ネットワークを介して、センサ機器に暗号鍵を送信する。暗号鍵受信ステップでは、センサ機器が、ホスト機器が送信した暗号鍵を受信する。第２記憶ステップでは、センサ機器が、受信した暗号鍵をセンサ機器のセンサ側記憶部に記憶する。パケット生成ステップでは、センサ機器が、センサ側記憶部に記憶されている暗号鍵で計測データを暗号化し、暗号化した計測データを含むパケットを生成する。パケット送信ステップでは、センサ機器が、生成されたパケットをブロードキャストで送信する。

[0022] 第９観点に係るデータ収集方法は、センサ機器が送信する計測データを、センサ機器とネットワークを介して接続されるホスト機器で収集するデータ収集方法である。センサ機器は、電池又は環境発電素子を有し、電池の電力又は環境発電素子が発電する電力で駆動される。データ収集方法は、暗号鍵生成ステップと、第１記憶ステップと、暗号鍵送信ステップと、暗号鍵受信ステップと、第２記憶ステップと、パケット生成ステップと、パケット送信ステップと、を備える。暗号鍵生成ステップでは、センサ機器が、センサ機器に固有の暗号鍵を生成する。第１記憶ステップでは、センサ機器が、センサ機器のセンサ側記憶部に、生成されたセンサ機器に固有の暗号鍵を記憶する。暗号鍵送信ステップでは、センサ機器が、公開鍵暗号基盤を用いて、ネ

ットワークを介して、ホスト機器に暗号鍵を送信する。暗号鍵受信ステップでは、ホスト機器が、センサ機器が送信した暗号鍵を受信する。第２記憶ステップでは、ホスト機器が、受信した暗号鍵をホスト機器のホスト側記憶部に記憶する。パケット生成ステップでは、センサ機器が、センサ側記憶部に記憶されている暗号鍵で計測データを暗号化し、暗号化した計測データを含むパケットを生成する。パケット送信ステップでは、センサ機器が、生成されたパケットをブロードキャストで送信する。

図面の簡単な説明

[0023] [図1]データ収集システムの概略構成図である。

[図2]第１実施形態に係るデータ収集システムの概略ブロック図である。

[図3]図２のデータ収集システムで行われるホスト機器とセンサ機器とのデータのやりとりを主に説明するためのシーケンスチャートである。

[図4]図２のデータ収集システムで行われるセンサ機器への暗号鍵送信のフローチャートである。

[図5]図２のデータ収集システムで行われるセンサ機器の計測データの収集に関する処理のフローチャートである。

[図6]第２実施形態に係るデータ収集システムの概略ブロック図である。

[図7]図６のデータ収集システムで行われるホスト機器とセンサ機器とのデータのやりとりを主に説明するためのシーケンスチャートである。

[図8]変形例Ａのデータ収集システムの概略ブロック図である。

[図9]変形例Ｂのデータ収集システムの概略ブロック図である。

発明を実施するための形態

[0024] 以下、データ収集システム及びデータ収集方法の実施形態を説明する。

[0025] ＜第１実施形態＞

（１）全体概要

第１実施形態のデータ収集システム１の全体概要について、図１を参照して説明する。図１は、データ収集システム１の概略構成図である。

[0026] データ収集システム１は、概して、センサ機器１００ａ～１００ｎの計測

データを収集するシステムである。用途を限定するものではないが、データ収集システム１により収集された計測データは、例えば、各種モニタリングや、各種解析や、各種装置の制御等に利用される。

[0027] データ収集システム１は、図１のように、ホスト機器２００と、センサ機器１００ａ～１００ｎと、を備えている。限定するものではないが、データ収集システム１は、複数のセンサ機器１００ａ～１００ｎを含む。例えば、データ収集システム１は、１０台以上のセンサ機器１００ａ～１００ｂを含む。ホスト機器２００と複数のセンサ機器１００ａ～１００ｎとは、ネットワーク２０により通信可能に接続されている。各センサ機器１００ａ～１００ｎは、所定の計測を行い、ネットワーク２０を介してホスト機器２００に計測データを送信する。ホスト機器２００は、センサ機器１００ａ～１００ｎから取得した計測データを、ホスト機器２００の記憶部２３０に記憶する。

[0028] 本実施形態では、ホスト機器２００は、空調装置１０の室内機に搭載されている。例えば、ホスト機器２００は、空調装置１０の制御装置とは独立した装置である。ホスト機器２００は、空調装置１０の制御装置に組み込まれていてもよい。言い換えれば、空調装置１０の制御装置の一部が、ホスト機器２００として機能してもよい。また、ホスト機器２００は、空調装置以外の他の装置に搭載されていてもよい。例えば、ホスト機器２００は、対象空間の温度、湿度、放射温度、風量、風向、空気質、照度、輝度、及び色温度の中の少なくとも１つを調整可能な、空調装置以外の設備装置に搭載されていてもよい。このような設備機器には、例えば、除湿機、加湿器、床暖房装置、送風機、空気清浄機、換気装置、及び照明装置を含む。また、例えば、ホスト機器２００は、ビルや工場等の中央監視装置に搭載されていてもよい。また、ホスト機器２００は、他の装置に搭載されている必要はなく、独立した装置であってもよい。

[0029] 各センサ機器１００ａ～１００ｎは、所定の計測を行うセンサである。センサ機器の種類を限定するものではないが、センサ機器１００ａ～１００ｎ

は、例えば、温度、湿度、放射温度、風量、風向、空気質（例えばＣＯ２濃度）、照度、輝度、及び色温度の少なくとも１つを計測するセンサである。また、センサ機器１００ａ～１００ｎは、人検知センサ等のデジタル信号タイプのセンサ機器であってもよい。また、センサ機器１００ａ～１００ｎは、設置式ではなく、人が携帯するスマートフォンやウェアラブル機器に内蔵されているセンサ機器（位置情報や生体情報を計測するセンサ機器）であってもよい。なお、複数のセンサ機器１００ａ～１００ｎは、全て同種のセンサである必要はなく、互いに異なる種類のセンサであってもよい。本実施形態では、センサ機器１００ａ～１００ｎは、空調装置１０の空調対象空間に配置されている温度センサである。

[0030] ホスト機器２００とセンサ機器１００ａ～１００ｂとは、無線ネットワークであるネットワーク２０を介して接続される。本実施形態では、ホスト機器２００とセンサ機器１００ａ～１００ｂとは、Ｂｌｕｅｔｏｏｔｈ（登録商標）規格を用いて通信を行う。

[0031] 本開示のデータ収集システム１で行われる処理について概説する。

[0032] データ収集システム１では、暗号鍵を共有するため、ホスト機器２００が生成する各センサ機器１００ａ～１００ｎに固有の暗号鍵（共通鍵）を、公開鍵暗号基盤を用いて、ネットワーク２０を介して各センサ機器１００ａ～１００ｎに送信する。そして、暗号鍵を共有した後、各センサ機器１００ａ～１００ｎは、各センサ機器１００ａ～１００ｎに固有の暗号鍵で暗号化した計測データを、消費電力の比較的少ないブロードキャストでホスト機器２００に送信する。要するに、本データ収集システム１では、セキュアな環境下で、ホスト機器２００から各センサ機器１００ａ～１００ｎに、各センサ機器１００ａ～１００ｎに固有の暗号鍵が送信される。そして、センサ機器１００ａ～１００ｎは、計測データを、各センサ機器１００ａ～１００ｎに固有の暗号鍵を用いて、省電力化が可能なブロードキャストで送信する。詳細は後述する。

[0033] （２）詳細構成

センサ機器１００ａ～１００ｎ及びホスト機器２００の詳細を、図２を参照して以下に説明する。図２は、データ収集システム１の概略ブロック図である。

[0034] なお、センサ機器１００ａ～１００ｎは、上記のように異なる種類の計測を行うセンサ機器である場合がある。しかし、センサ機器１００ａ～１００ｎは、計測データを含むパケットの生成や、ホスト機器２００に対するパケットの送信に関してはいずれも同様の動作を行う。そこで、ここでは、センサ機器１００ａ～１００ｎのそれぞれについて説明する代わりに、センサ機器１００ａ～１００ｎを代表的に表すセンサ機器１００について説明する。

[0035] （２－１）センサ機器

センサ機器１００は、通信機能を有し、計測データを、ネットワーク２０を介して送信する機器である。センサ機器１００は、計測を行うセンサ装置と、センサ装置とは独立している、ネットワーク２０を介してホスト機器２００と通信可能な通信装置と、を組み合わせた機器であってもよい。

[0036] センサ機器１００は、電力系統には接続されていない。センサ機器１００は、電池駆動式である。電池駆動式のセンサ機器１００は、電力系統からの電力供給を必要とするセンサ機器に比べ、設置場所の選択の自由度が高く、設置も容易である。一方で、電池駆動式のセンサ機器１００では、消費電力が大きいと、頻繁に電池交換等が必要になる。

[0037] センサ機器１００は、センサモジュール１１０と、電池１２０と、を含む。また、センサ機器１００は、図示しない、ＣＰＵやメモリを有するマイクロコンピュータ、入出力装置、無線通信モジュール等を含む。ＣＰＵがメモリに記憶されているプログラムを実行することで、センサ機器１００は、受信部１３０、送信部１４０、記憶部１５０、及びパケット生成部１６０として機能する。

[0038] （２－１－１）センサモジュール

センサモジュール１１０は、図示しないセンサデバイスを用いて、所定の計測を行う。本実施形態では、センサモジュール１１０は、図示しないセン

サデバイスとしてのサーミスタを用いて、センサデバイスの設置場所の空気の温度を計測する。

[0039] （２－１－２）電池

電池１２０は、センサ機器１００の駆動に用いられる。要するに、センサ機器１００に含まれる各種装置は、電池１２０の供給する電力により駆動される。

[0040] （２－１－３）受信部

受信部１３０は、ホスト機器２００がネットワーク２０を介して送信する各種信号を受信する。

[0041] 受信部１３０は、例えば、ホスト機器２００が送信する暗号鍵Ｋを受信する。要するに、受信部１３０は、暗号鍵受信部の一例である。受信部１３０の受信した暗号鍵Ｋは、記憶部１５０に記憶される。

[0042] なお、暗号鍵Ｋは、後述するホスト機器２００の暗号鍵生成部２４０が生成する、センサ機器１００に固有の暗号鍵Ｋである。言い換えれば、センサ機器１００ａ～１００ｎには、それぞれ異なる暗号鍵が送信される。暗号鍵Ｋは、情報の暗号化にも復号化にも用いられる共通鍵である。

[0043] （２－１－４）送信部

送信部１４０は、ネットワーク２０を介してホスト機器２００に各種信号を送信する。

[0044] 送信部１４０は、例えば、後述するパケット生成部１６０の生成するパケットを、ネットワーク２０を介して、ホスト機器２００にブロードキャストで送信する。要するに、送信部１４０は、パケット送信部の一例である。具体的には、送信部１４０は、パケット生成部１６０の生成する、センサモジュール１１０の計測データＤを含むアドバタイズパケットを、ブロードキャストで送信する。

[0045] （２－１－５）記憶部

記憶部１５０は、各種情報を記憶する。

[0046] 記憶部１５０は、センサ側記憶部の一例である。記憶部１５０は、受信部

１３０が受信する暗号鍵Ｋを記憶する。

[0047] また、記憶部１５０は、識別文字列Ｃ及び計測データＤを記憶する。

[0048] 識別文字列Ｃは、センサ機器１００の記憶部１５０に予め記憶されている情報である。後述するホスト機器２００の記憶部２３０にも、同一の識別文字列Ｃが予め記憶されている。言い換えれば、センサ機器１００の記憶部１５０及びホスト機器２００の記憶部２３０は、共通の識別文字列Ｃを記憶する。

[0049] 計測データＤは、センサモジュール１１０の計測データである。記憶部１５０には、センサモジュール１１０の計測日時と、センサモジュール１１０の計測値とが関連付けられて記憶されている。

[0050] （２－１－６）パケット生成部

パケット生成部１６０は、ホスト機器２００に送信するための計測データＤを含むパケットを生成する。特に、パケット生成部１６０は、記憶部１５０に記憶されている計測データＤを記憶部１５０に記憶されている暗号鍵Ｋで暗号化し、暗号化した計測データＤを含むパケットを生成する。なお、パケット生成部１６０の暗号鍵Ｋを用いた暗号化には、既知の暗号化アルゴリズム（例えば、ＡＥＳ暗号化等）が用いられればよい。

[0051] パケット生成部１６０は、暗号化した計測データＤを含むアドバタイズパケットをパケットとして生成する。パケット生成部１６０により生成されたパケットは、前述のように、送信部１４０によりブロードキャストで送信される。

[0052] 本実施形態では、記憶部１５０に記憶され、暗号化される計測データＤは、センサモジュール１１０の計測データそのものである。ただし、これに限定されるものではなく、暗号化される計測データＤは、センサモジュール１１０が複数回計測した計測データの平均値や中央値等、センサモジュール１１０の計測値に基づいて算出される値であってもよい。

[0053] パケット生成部１６０は、計測データＤに加え、識別文字列Ｃを含むパケットを生成することが好ましい。具体的には、パケット生成部１６０は、記

憶部１５０に記憶されている計測データＤ及び識別文字列Ｃを暗号鍵Ｋで暗号化し、暗号化された計測データＤ及び識別文字列Ｃを含むパケットを生成することが好ましい。

[0054] （２－２）ホスト機器

ホスト機器２００は、例えばコンピュータにより実現される。ホスト機器２００は、図示しない制御演算装置及び記憶装置を含む。制御演算装置には、ＣＰＵやＧＰＵ等のプロセッサを使用できる。制御演算装置は、記憶装置に記憶されているプログラムを読み出して実行し、所定の処理を行う。また、制御演算装置は、プログラムに従って、演算結果を記憶装置に書き込み、記憶装置に記憶されている情報を読み出す。

[0055] ホスト機器２００は、制御演算装置が記憶装置に記憶されているプログラムを実行することで、図２のように、受信部２１０、送信部２２０、記憶部２３０，暗号鍵生成部２４０、復号部２５０、第１判断部２６０、第２判断部２７０、及び書込部２８０として機能する。

[0056] （２－２－１）受信部

受信部２１０は、センサ機器１００からネットワーク２０を介して送信されてくる各種信号を受信する。

[0057] 受信部２１０は、例えば、センサ機器１００から計測データＤを受信する。要するに、受信部２１０は、計測データ受信部の一例である。具体的には、受信部２１０は、センサ機器１００の送信部１４０がブロードキャストで送信してくる、暗号鍵Ｋで暗号化された計測データＤを含むパケットを受信する。より具体的には、受信部２１０は、センサ機器１００の送信部１４０がブロードキャストで送信してくる、暗号鍵Ｋで暗号化された計測データＤを含むアドバタイズパケットを受信する。特に、本実施形態のデータ収集システム１では、受信部２１０は、センサ機器１００の送信部１４０が送信してくる、暗号鍵Ｋで暗号化された計測データＤ及び識別文字列Ｃを含むパケットを受信する。

[0058] （２－２－２）送信部

送信部２２０は、ネットワーク２０を介してセンサ機器１００に各種信号を送信する。送信部２２０は、例えば、ネットワーク２０を介して、暗号鍵生成部２４０の生成したセンサ機器１００に固有の暗号鍵Ｋを、公開鍵暗号基盤を用いてセンサ機器１００に送信する。具体的には、送信部２２０は、ホスト機器２００とセンサ機器１００とのペアリング時に、公開鍵暗号基盤を用いてセンサ機器１００に固有の暗号鍵Ｋをセンサ機器１００に送信する。なお、暗号鍵生成部２４０は、センサ機器１００ａ～１００ｎのそれぞれに対して異なる暗号鍵を生成する。そのため、送信部２２０は、センサ機器１００ａ～１００ｎのそれぞれに対して異なる暗号鍵を、公開鍵暗号基盤を用いてセンサ機器１００に送信する。

[0059] （２－２－３）記憶部

記憶部２３０は、ホスト側記憶部の一例である。記憶部２３０は、各種情報を記憶する。記憶部２３０に記憶される情報には、暗号鍵Ｋと、識別文字列Ｃと、計測データＤと、を含む。

[0060] 暗号鍵Ｋは、暗号鍵生成部２４０が、センサ機器１００ａ～１００ｎのそれぞれに対して個別に生成する、各センサ機器１００ａ～１００ｎの固有の暗号鍵である。記憶部２３０には、センサ機器１００ａ～１００ｎの識別情報と、各センサ機器１００ａ～１００ｎの暗号鍵とが関連付けて記憶される。

[0061] 識別文字列Ｃは、ホスト機器２００の記憶部２３０に予め記憶されている情報である。センサ機器１００の記憶部１５０にも、同一の、言い換えれば共通の識別文字列Ｃが、記憶されている。

[0062] 計測データＤは、センサ機器１００の計測データＤである。なお、ここでは、以下の２つの条件が成立したときに、後述する書込部２８０が、後述する復号部２５０が復号化した計測データＤを記憶部２３０に記憶する。以下の２つの条件の両方を満たさない場合には、受信部２１０が受信したパケットは破棄される。

条件１：受信部２１０が受信したパケットに含まれ、後述する復号部２５０

の復号化した計測データが有効なデータであること。言い換えれば、受信部２１０が受信したパケットにおいて暗号化に用いられている暗号鍵が、記憶部２３０に記憶されている暗号鍵Ｋであること。

条件２：受信部２１０が受信したパケットに含まれ、後述する復号部２５０の復号化した識別文字列Ｃが、記憶部２３０に記憶されている識別文字列Ｃと一致すること。言い換えれば、後述する第１判断部２６０が、受信部２１０が受信したパケットを、データ収集の対象のセンサ機器１００の送信した計測データではないと判断しないこと。

[0063] （２－２－４）暗号鍵生成部

暗号鍵生成部２４０は、センサ機器１００に固有の暗号鍵Ｋを生成する。言い換えれば、暗号鍵生成部２４０は、センサ機器１００ａ～１００ｎのそれぞれに対して、互いに異なる暗号鍵を生成する。

[0064] （２－２－５）復号部

復号部２５０は、受信部２１０が受信したパケットに含まれる暗号化された計測データＤを、記憶部２３０に記憶されている暗号鍵Ｋを用いて復号する。特に本実施形態のデータ収集システム１では、復号部２５０は、受信部２１０が受信したパケットに含まれる暗号鍵Ｋで暗号化された計測データＤ及び識別文字列Ｃを含むパケットを復号する。

[0065] なお、仮に、受信部２１０が受信したパケットに含まれるデータが、暗号鍵Ｋを用いて暗号化されていない場合、復号化されたデータは有効なデータとならない。復号化されたデータが有効なデータではない場合、受信部２１０が受信したパケットのデータは、無効なデータとして破棄される。具体的には、復号化されたデータが有効なデータではない場合、後述する書込部２８０は、受信部２１０が受信したパケットのデータを記憶部２３０に記憶しない。

[0066] （２－２－６）第１判断部

第１判断部２６０は、復号部２５０により復号された識別文字列Ｃを、記憶部２３０に記憶されている識別文字列Ｃと比較し、両者が一致するか否か

を判断する。

[0067] 第１判断部２６０は、復号部２５０により復号された識別文字列Ｃと、記憶部２３０に記憶されている識別文字列Ｃとが一致しない場合には、受信部２１０が受信したパケットを、データ収集の対象外の機器の送信したパケットと判断する。例えば、センサ機器１００になりすましてデータを送信してくる機器（偽装デバイス）である。第１判断部２６０が、受信部２１０が受信したパケットをデータ収集の対象外の機器の送信したパケットと判断した場合、受信部２１０が受信したパケットのデータは、無効なデータとして破棄される。具体的には、第１判断部２６０が、受信部２１０が受信したパケットをデータ収集の対象外の機器の送信したパケットと判断した場合、後述する書込部２８０は、受信部２１０が受信したパケットのデータを記憶部２３０に記憶しない。

[0068] （２－２－７）第２判断部

第２判断部２７０は、受信部２１０が受信する計測データＤの時間変化に基づき、受信した計測データＤがデータ収集の対象外の機器の送信したデータであるか否かを判断する。具体的には、第２判断部２７０は、受信部２１０が受信したパケットに含まれ、復号部２５０により復号された計測データＤの時間変化に基づき、受信した計測データＤがデータ収集の対象外の機器の送信したデータであるか否かを判断する。より具体的には、第２判断部２７０は、受信部２１０が受信し記憶部２３０に記憶されている計測データＤの温度が、長期間変化しない場合には、受信した計測データＤが、データ収集の対象外の機器の送信したデータであると判断する。

[0069] （２－２－８）書込部

書込部２８０は、受信部２１０がパケットを受信した際、復号部２５０の復号化したデータが有効なデータであり、かつ、第１判断部２６０が、受信部２１０が受信したパケットを、データ収集の対象のセンサ機器１００の送信した計測データではないと判断しない場合、復号部２５０の復号化した計測データを、計測データＤとして記憶部２３０に記憶する。

[0070] （３）データ収集システムの動作

データ収集システム１の動作について、図３～図５を参照しながら説明する。図３は、データ収集システム１で行われるホスト機器２００とセンサ機器１００とのデータのやりとりを主に説明するためのシーケンスチャートである。なお、図３のシーケンスチャートでは、センサ機器１００以外のデータ収集対象外の機器（例えばなりすまし機器（偽装デバイス））からパケットが送信される場合を想定して描画されていない。図４は、データ収集システム１で行われるセンサ機器１００への暗号鍵送信のフローチャートである。図５は、データ収集システム１で行われるセンサ機器１００の計測データの収集に関する処理のフローチャートである。

[0071] （３－１）センサ機器とホスト機器との間のデータのやり取り

図３を参照しながら、センサ機器１００とホスト機器２００との間のデータのやり取りについて説明する。

[0072] まず、センサ機器１００の電源が初めてＯＮになると、センサ機器１００は、送信部１４０からネットワーク２０を介してブロードキャストでペアリング要求と共に認証プロファイルを送信する。これに対し、ホスト機器２００は、ペアリング処理を行い、ホスト機器２００とセンサ機器１００とはペアリングを開始する。その後、ホスト機器２００では、暗号鍵生成部２４０がセンサ機器１００に固有の暗号鍵Ｋを生成し、記憶部２３０に記憶する。また、ホスト機器２００の送信部２２０は、公開鍵暗号基盤を用いて、暗号鍵生成部２４０が生成した暗号鍵Ｋを、ネットワーク２０を介して、センサ機器１００に送信する。センサ機器１００は、受信部１３０が受信した暗号鍵Ｋを、記憶部１５０に記憶する。以上が、ホスト機器２００からセンサ機器１００への暗号鍵Ｋの送信処理における、ホスト機器２００とセンサ機器１００との間のデータのやり取りの流れである。

[0073] センサ機器１００が暗号鍵Ｋを受信した後、センサ機器１００のセンサモジュール１１０は、所定のタイミングで計測データＤを取得し、取得した計測データＤを記憶部１５０に記憶する。そして、パケット生成部１６０が、

記憶部１５０に記憶されている計測データＤ及び識別文字列Ｃを暗号鍵Ｋで暗号化し、暗号化された計測データＤ及び識別文字列Ｃを含むアドバタイズパケットを生成する。そして、送信部１４０は、アドバタイズパケットをブロードキャストで送信する。ホスト機器２００は、受信部２１０がアドバタイズパケットを受信すると、アドバタイズパケットに含まれる暗号化された計測データＤを、アドバタイズパケットの送信元のセンサ機器１００用の暗号鍵Ｋで復号し、計測データを記憶部２３０に記憶する。なお、ホスト機器２００がアドバタイズパケットを受信した際に行う各種処理については、後ほど説明する。

[0074] （３－２）センサ機器への暗号鍵の送信

データ収集システム１で行われる、センサ機器１００への暗号鍵送信までの処理の流れについて、図４を参照しながら再度説明する。なお、ここで説明するフローチャートは一例に過ぎず、矛盾の無い範囲で適宜変更されてもよい。

[0075] まず、センサ機器１００の電源が初めてＯＮになると、センサ機器１００は、送信部１４０からネットワーク２０を介してブロードキャストでペアリング要求と共に認証プロファイルを送信する（ステップＳ１）。

[0076] ホスト機器２００は、ペアリング要求及び認証プロファイルを受信部２１０が受信すると、ペアリング処理を行う。その結果、ホスト機器２００とセンサ機器１００との間のペアリングが開始される（ステップＳ２）。

[0077] 次に、ホスト機器２００の暗号鍵生成部２４０は、センサ機器１００に固有の暗号鍵Ｋを生成する（ステップＳ３）。

[0078] 次に、ホスト機器２００は、暗号鍵生成部２４０の生成した暗号鍵Ｋを、センサ機器１００を識別する情報と関連付けて記憶部２３０に記憶する（ステップＳ４）。

[0079] 次に、ホスト機器２００の送信部２２０は、公開鍵暗号基盤を用いて、ネットワーク２０を介して、暗号鍵生成部２４０の生成した暗号鍵Ｋをセンサ機器１００に送信する（ステップＳ５）。

[0080] センサ機器１００の受信部１３０は、ホスト機器２００が送信した暗号鍵Ｋを受信する（ステップＳ６）。そして、センサ機器１００は、受信部１３０が受信する暗号鍵Ｋを記憶部１５０に記憶する（ステップＳ７）。

[0081] そして、センサ機器１００とホスト機器２００との間のペアリングが終了する（ステップＳ８）。

[0082] なお、以上で説明した暗号鍵Ｋの生成及び送信の処理は、センサ機器１００の設置時だけではなく、定期的に実行されてもよい。定期的に暗号鍵Ｋが更新されることで、通信の安全性を高めることができる。

[0083] （３－３）データ収集システムにおけるセンサ機器の計測データの収集

データ収集システム１で行われる、センサ機器１００の計測データの収集に関する処理について、図５を参照しながら再度説明する。なお、ここで説明するフローチャートは一例に過ぎず、矛盾の無い範囲で適宜変更されてもよい。

[0084] 前提として、センサ機器１００のセンサモジュール１１０（ここでは温度センサモジュール）は、所定のタイミングで温度の計測を行い、記憶部１５０には計測データＤが記憶されているものとする。

[0085] センサ機器１００のパケット生成部１６０は、所定のタイミングで、記憶部１５０に記憶されている暗号鍵Ｋで、記憶部１５０に記憶されている計測データＤを暗号化する。より具体的には、パケット生成部１６０は、記憶部１５０に記憶されている暗号鍵Ｋで、記憶部１５０に記憶されている計測データＤ及び識別文字列Ｃを暗号化する（ステップＳ１１）。

[0086] そして、パケット生成部１６０は、暗号化した計測データＤを含むパケットを生成する。より具体的には、パケット生成部１６０は、暗号化した計測データＤ及び識別文字列Ｃを含むアドバタイズパケットを生成する（ステップＳ１２）。

[0087] 次に、ステップＳ１３では、送信部１４０は、パケット生成部１６０の生成するパケットをブロードキャストで送信する。具体的には、送信部１４０は、パケット生成部１６０の生成するアドバタイズパケットをブロードキャ

ストで送信する。

[0088] 次に、ステップＳ１４では、ホスト機器２００の受信部２１０が、センサ機器１００から計測データＤを受信する。より具体的には、受信部２１０は、センサ機器１００から送信されてくるアドバタイズパケットを受信する。

[0089] 次に、ステップＳ１５では、ホスト機器２００の復号部２５０は、パケットの送信元のセンサ機器１００に対応する暗号鍵Ｋを用いて、受信部２１０が受信したパケットに含まれる、暗号化された計測データＤ及び識別文字列Ｃを復号する。

[0090] 次に、ステップＳ１６では、センサ機器１００では、復号化された計測データＤ及び識別文字列Ｃが有効なデータであるか否かが判断される。復号化された計測データＤ及び識別文字列Ｃが有効なデータであればステップＳ１７に進み、復号化された計測データＤ及び識別文字列Ｃが有効なデータでなければステップＳ２２に進む。

[0091] 次に、ステップＳ１７では、第１判断部２６０は、復号部２５０により復号された識別文字列Ｃと、記憶部２３０に記憶されている識別文字列Ｃとが一致するか否かを判断する。そして、第１判断部２６０は、復号部２５０により復号された識別文字列Ｃと、記憶部２３０に記憶されている識別文字列Ｃとが一致しないと判断した場合、ステップＳ１４で受信部２１０が受信したパケットを、データ収集の対象外の機器の送信したパケットと判断する。

[0092] ステップＳ１７で、第１判断部２６０が、復号部２５０により復号された識別文字列Ｃと、記憶部２３０に記憶されている識別文字列Ｃとが一致すると判断すると、ステップＳ１８に進む。一方で、ステップＳ１７で、第１判断部２６０が、復号部２５０により復号された識別文字列Ｃと、記憶部２３０に記憶されている識別文字列Ｃとが一致しないと判断すると、ステップＳ２２に進む。

[0093] ステップＳ１８では、ホスト機器２００の書込部２８０は、ステップＳ１５において復号された計測データＤを記憶部２３０に記憶する。

[0094] ステップＳ１９では、第２判断部２７０は、受信部２１０が受信する計測

データＤの時間変化を分析する。具体的には、第２判断部２７０は、直近に記憶された計測データＤを含む、記憶部２３０に記憶された過去の計測データＤの時間変化を分析する。

[0095] 次にステップＳ２０では、第２判断部２７０は、過去の計測データＤが所定の長時間一定の値であるか否かを判断する。第２判断部２７０は、過去の計測データＤが長時間一定である場合には、受信した計測データＤがデータ収集の対象外の機器の送信した計測データであると判断し、一連の処理を終了する（ステップＳ２１）。なお、第２判断部２７０が記憶部２３０に記憶されているセンサ機器１００の計測データＤをデータ収集の対象外の機器の送信した計測データであると判断した場合、ホスト機器２００は、計測データＤを利用する各種処理において、記憶部２３０にセンサ機器１００の計測データＤとして記憶されているデータを、無効なデータとして無視してもよい。

[0096] 一方、第２判断部２７０は、ステップＳ２０において、過去の計測データＤに変化がある場合には（ステップＳ２０でＮｏ）、受信した計測データＤがセンサ機器１００の送信した計測データであると判断し、一連の処理を終了する

ステップＳ１６及びステップＳ１７からステップＳ２２に進んだ場合には、ホスト機器２００は、データを破棄する。具体的には、ホスト機器２００の書込部２８０は、ステップＳ１５において復号された計測データＤを記憶部２３０に記憶することなく、一連の処理を終了する。

[0097] （４）特徴

（４－１）

本実施形態のデータ収集システム１は、ホスト機器２００と、センサ機器１００と、を備える。センサ機器１００は、ホスト機器２００とネットワーク２０を介して接続される。センサ機器１００は、ホスト機器２００に計測データＤを送信する。センサ機器１００は、電池１２０を有し、電池１２０が供給する電力で駆動される。ホスト機器２００は、暗号鍵生成部２４０と

、ホスト側記憶部の一例としての記憶部２３０と、暗号鍵送信部の一例としての送信部２２０と、計測データ受信部の一例としての受信部２１０と、を有する。暗号鍵生成部２４０は、センサ機器１００に固有の暗号鍵Ｋを生成する。記憶部２３０は、暗号鍵生成部２４０が生成した暗号鍵Ｋを記憶する。送信部２２０は、公開鍵暗号基盤を用いて、ネットワーク２０を介して、センサ機器１００に暗号鍵Ｋを送信する。受信部２１０は、センサ機器１００から計測データＤを受信する。センサ機器１００は、暗号鍵受信部の一例としての受信部１３０と、センサ側記憶部の一例としての記憶部１５０と、パケット生成部１６０と、パケット送信部の一例としての送信部１４０と、を有する。受信部１３０は、ホスト機器２００が送信する暗号鍵Ｋを受信する。記憶部１５０は、受信部１３０が受信する暗号鍵Ｋを記憶する。パケット生成部１６０は、記憶部１５０に記憶されている暗号鍵Ｋで計測データＤを暗号化し、暗号化した計測データＤを含むパケットを生成する。送信部１４０は、パケット生成部１６０の生成するパケットをブロードキャストで送信する。

[0098] データ収集システム１では、ホスト機器２００が公開鍵暗号基盤を用いてセキュアな環境でセンサ機器１００に暗号鍵Ｋを送信し、センサ機器１００はこの暗号鍵Ｋを用いて暗号化した計測データＤを、消費電力の比較的少ないブロードキャストで送信する。このため、データ収集システム１では、ホスト機器２００とセンサ機器１００との間のセキュアな通信環境と、センサ機器１００の省電力化とを両立できる。

[0099] また、本データ収集システム１では、ブロードキャストを利用するため、１台のホスト機器２００で、理論上台数制限なく、多数のセンサ機器１００から計測データＤを収集できる。

[0100] （４－２）

本実施形態のデータ収集システム１では、ホスト機器２００とセンサ機器１００とはＢｌｕｅｔｏｏｔｈ（登録商標）規格を用いて通信を行う。送信部２２０は、ホスト機器２００とセンサ機器１００とのペアリング時にセン

サ機器１００に暗号鍵Ｋを送信する。パケット生成部１６０は、暗号化した計測データＤを含むアドバタイズパケットをパケットとして生成する。

[0101] 本データ収集システム１では、Ｂｌｕｅｔｏｏｔｈ（登録商標）規格を用いて、セキュアな通信環境と、センサ機器１００の省電力化と、を両立できる。

[0102] （４－３）

本実施形態のデータ収集システム１では、ホスト機器２００の記憶部２３０及びセンサ機器１００の記憶部１５０は、共通の識別文字列Ｃを記憶する。パケット生成部１６０は、暗号化した計測データＤ及び識別文字列Ｃを含むパケットを生成する。

[0103] 本データ収集システム１では、パケットにホスト機器２００及びセンサ機器１００が記憶する共通の識別文字列Ｃが含まれるので、セキュアなシステムが実現されやすい。

[0104] （４－４）

本実施形態のデータ収集システム１では、ホスト機器２００は、復号部２５０と、第１判断部２６０と、を備える。復号部２５０は、暗号鍵Ｋを用いて、受信したパケットに含まれる、暗号化された計測データＤ及び識別文字列Ｃを復号する。第１判断部２６０は、復号部２５０により復号された識別文字列Ｃと、記憶部２３０に記憶されている識別文字列Ｃとが一致するか否かを判断する。

[0105] 本データ収集システム１では、不適切な計測データが誤って収集される事態の発生を抑制できる。

[0106] （４－５）

本実施形態のデータ収集システム１では、第１判断部２６０は、復号部２５０により復号された識別文字列Ｃと、ホスト機器２００の記憶部２３０に記憶されている識別文字列Ｃとが一致しないと判断した場合に、受信したパケットを、データ収集の対象外の機器の送信したパケットと判断する。

[0107] 本データ収集システム１では、識別文字列Ｃの不一致に基づきデータ収集

の対象外の機器が判断されるため、セキュアなシステムを実現できる。

[0108] （４－６）

本実施形態のデータ収集システム１では、ホスト機器２００は、第２判断部２７０を備える。第２判断部２７０は、受信部２１０が受信する計測データＤの時間変化に基づき、受信した計測データＤがデータ収集の対象外の機器の送信した計測データであるか否かを判断する。

[0109] 本データ収集システム１では、計測データＤの時間変化に基づいて、計測データＤが、偽装デバイス等のデータ収集の対象外の機器の送信した計測データであることを判断できる。

[0110] （４－７）

本実施形態のデータ収集方法は、センサ機器１００が送信する計測データを、センサ機器１００とネットワーク２０を介して接続されるホスト機器２００で収集するデータ収集方法である。センサ機器１００は、電池１２０を有し、電池１２０の電力で駆動される。データ収集方法は、暗号鍵生成ステップと、第１記憶ステップと、暗号鍵送信ステップと、暗号鍵受信ステップと、第２記憶ステップと、パケット生成ステップと、パケット送信ステップと、を備える。暗号鍵生成ステップでは、ホスト機器２００が、センサ機器１００に固有の暗号鍵Ｋを生成する。第１記憶ステップでは、ホスト機器２００が、ホスト側記憶部の一例である記憶部２３０に、生成されたセンサ機器１００に固有の暗号鍵Ｋを記憶する。暗号鍵送信ステップでは、ホスト機器２００が、公開鍵暗号基盤を用いて、ネットワーク２０を介して、センサ機器１００に暗号鍵Ｋを送信する。暗号鍵受信ステップでは、センサ機器１００が、ホスト機器２００が送信した暗号鍵Ｋを受信する。第２記憶ステップでは、センサ機器１００が、受信した暗号鍵Ｋをセンサ側記憶部の一例である記憶部１５０に記憶する。パケット生成ステップでは、センサ機器１００が、記憶部１５０に記憶されている暗号鍵Ｋで計測データＤを暗号化し、暗号化した計測データＤを含むパケットを生成する。パケット送信ステップは、センサ機器１００が、生成されたパケットをブロードキャストで送信す

る。

[0111] ＜第２実施形態＞

第２実施形態のデータ収集システム１Ａについて、図６及び図７を参照しながら説明する。図６は、データ収集システム１Ａの概略ブロック図である。なお、図６中で、図２と同一の参照符号を用いて表した機能部は、データ収集システム１の同一の参照符号を付して説明した機能部と概ね同一の機能を有する。図７は、データ収集システム１Ａで行われるホスト機器２００Ａとセンサ機器１００Ａとのデータのやりとりを主に説明するためのシーケンスチャートである。

[0112] データ収集システム１Ａと第１実施形態のデータ収集システム１との主な相違点は、図６のブロック図に示すように、ホスト機器２００Ａは暗号鍵生成部２４０を有さない一方で、センサ機器１００Ａが暗号鍵生成部１７０を有する点である。他の点については、データ収集システム１Ａとデータ収集システム１とは同様である。

[0113] データ収集システム１とデータ収集システム１Ａとの処理は、概ね以下の点で異なる。

[0114] データ収集システム１では、ホスト機器２００が暗号鍵Ｋを生成し、生成された暗号鍵Ｋがセンサ機器１００に送信され、センサ機器１００に記憶される。

[0115] これに対し、第２実施形態のデータ収集システム１Ａでは、センサ機器１００Ａの暗号鍵生成部１７０が暗号鍵Ｋを生成し、生成した暗号鍵Ｋを記憶部１５０に記憶する（図７参照）。また、第２実施形態のデータ収集システム１Ａでは、センサ機器１００Ａの送信部１４０が、暗号鍵生成部１７０の生成した暗号鍵Ｋを、公開鍵暗号基盤を用いて、ネットワーク２０を介してホスト機器２００に送信する（図７参照）。そして、ホスト機器２００では、受信部２１０が暗号鍵Ｋを受信し、受信した暗号鍵Ｋを記憶部２３０に記憶する（図７参照）。

[0116] なお、その他の点は、データ収集システム１Ａと第１実施形態のデータ収

集システム１とは同様である。例えば、データ収集システム１Ａにおける、ホスト機器２００Ａに対するセンサ機器１００Ａの計測データＤの送信処理は、データ収集システム１における処理と同様である。したがって、ここではこれ以上の説明を省略する。

[0117] （１）特徴

本実施形態のデータ収集システム１Ａは以下の特徴を有する。また、データ収集システム１Ａは、第１実施形態のデータ収集システム１の（４－２）－（４－６）と同様の特徴を有する。

[0118] （１－１）

本実施形態のデータ収集システム１Ａは、ホスト機器２００Ａと、センサ機器１００Ａと、を備える。センサ機器１００Ａは、ホスト機器２００Ａとネットワーク２０を介して接続される。センサ機器１００Ａは、ホスト機器２００Ａに計測データＤを送信する。センサ機器１００Ａは、電池１２０を有し、電池１２０が供給する電力で駆動される。センサ機器１００Ａは、暗号鍵生成部１７０と、センサ側記憶部の一例としての記憶部１５０と、暗号側送信部及びパケット送信部の一例としての送信部１４０と、パケット生成部１６０と、を有する。暗号鍵生成部１７０は、センサ機器１００Ａに固有の暗号鍵Ｋを生成する。記憶部１５０は、暗号鍵生成部１７０が生成する暗号鍵Ｋを記憶する。送信部１４０は、公開鍵暗号基盤を用いて、ネットワーク２０を介して、ホスト機器２００Ａに暗号鍵Ｋを送信する。パケット生成部１６０は、記憶部１５０に記憶されている暗号鍵で計測データＤを暗号化し、暗号化した計測データＤを含むパケットを生成する。送信部１４０は、パケット生成部１６０の生成するパケットをブロードキャストで送信する。ホスト機器２００Ａは、暗号鍵受信部及び計測データ受信部の一例としての受信部２１０と、ホスト側記憶部の一例としての記憶部２３０と、を有する。受信部２１０は、センサ機器１００Ａが送信する暗号鍵Ｋを受信する。記憶部２３０は、受信部２１０が受信する暗号鍵Ｋを記憶する。受信部２１０は、センサ機器１００Ａの送信する計測データＤを受信する。

[0119] 本実施形態のデータ収集システム１Ａでは、センサ機器１００Ａが公開鍵暗号基盤を用いてセキュアな環境でホスト機器２００Ａに暗号鍵を送信し、センサ機器１００Ａは自ら作成した暗号鍵Ｋを用いて暗号化した計測データＤを、消費電力の比較的少ないブロードキャストで送信する。このため、本データ収集システム１Ａでは、ホスト機器２００Ａとセンサ機器１００Ａとの間のセキュアな通信環境と、センサ機器１００Ａの省電力化と、を両立できる。

[0120] また、本実施形態のデータ収集システム１Ａでは、ブロードキャストを利用するため、１台のホスト機器２００Ａで、理論上台数制限なく、多数のセンサ機器１００Ａから計測データを収集できる。

[0121] ただし、センサ機器１００Ａが暗号鍵Ｋを生成する場合、第三者が自分のＰＣとペアリングして暗号鍵Ｋを盗み見する等のリスクも考えられる。そのため、好ましくは、第１実施形態のデータ収集システム１のように、ホスト機器２００側で暗号鍵Ｋが生成される。

[0122] （１－２）

本実施形態のデータ収集方法は、センサ機器１００Ａが送信する計測データＤを、センサ機器１００Ａとネットワーク２０を介して接続されるホスト機器２００Ａで収集するデータ収集方法である。センサ機器１００Ａは、電池１２０を有し、電池１２０の電力で駆動される。データ収集方法は、暗号鍵生成ステップと、第１記憶ステップと、暗号鍵送信ステップと、暗号鍵受信ステップと、第２記憶ステップと、パケット生成ステップと、パケット送信ステップと、を備える。暗号鍵生成ステップでは、センサ機器１００Ａが、センサ機器１００Ａに固有の暗号鍵Ｋを生成する。第１記憶ステップでは、センサ機器１００Ａが、センサ機器１００Ａの記憶部１５０に、生成されたセンサ機器１００Ａに固有の暗号鍵Ｋを記憶する。暗号鍵送信ステップでは、センサ機器１００Ａが、公開鍵暗号基盤を用いて、ネットワーク２０を介して、ホスト機器２００Ａに暗号鍵Ｋを送信する。暗号鍵受信ステップでは、ホスト機器２００Ａが、センサ機器１００Ａが送信した暗号鍵Ｋを受信

する。第２記憶ステップでは、ホスト機器２００Ａが、受信した暗号鍵Ｋをホスト機器２００Ａの記憶部２３０に記憶する。パケット生成ステップでは、センサ機器１００Ａが、記憶部１５０に記憶されている暗号鍵Ｋで計測データＤを暗号化し、暗号化した計測データＤを含むパケットを生成する。パケット送信ステップでは、センサ機器１００Ａが、生成されたパケットをブロードキャストで送信する。

[0123] ＜変形例＞

以下に上記実施形態の変形例を示す。なお、変形例は、矛盾しない範囲で互いに適宜組み合わされてもよい。

[0124] （１）変形例Ａ

上記第１実施形態のセンサ機器１００は、図８のように、電池１２０に代えて（又は電池１２０に加えて）環境発電素子１２２を有し、環境発電素子１２２が発電する電力で駆動されてもよい。なお、センサ機器１００は、電力系統には接続されていない。

[0125] ここでの、環境発電素子１２２は、太陽光、照明光、振動、電磁波、廃熱等のエネルギーを利用して発電を行う素子である。環境発電素子１２２で得られる電力は一般に限定的であるため、センサ機器１００は省電力化が図られることが好ましい。

[0126] なお、ここでは図示及び説明を省略するが、第２実施形態のセンサ機器１００Ａも、電池１２０に代えて（又は加えて）環境発電素子１２２を有してもよい。

[0127] （２）変形例Ｂ

第１実施形態のデータ収集システム１では、ホスト機器２００の記憶部２３０に、センサ機器１００の計測データＤが記憶される。ただし、これに限定されるものではなく、ホスト機器２００の受信したセンサ機器１００の計測データＤは、例えばインターネット等のネットワーク３０を介して接続されているサーバ３００の記憶部３１０に記憶されてもよい。ここでは図示及び説明を省略するが、第２実施形態のデータ収集システム１Ａについて同様

に構成されてもよい。

[0128] ＜付記＞

以上、本開示の実施形態を説明したが、特許請求の範囲に記載された本開示の趣旨及び範囲から逸脱することなく、形態や詳細の多様な変更が可能なことが理解されるであろう。

産業上の利用可能性

[0129] 本開示は、ホスト機器と、ネットワークを介してホスト機器に計測データを送信するセンサ機器と、を備えたデータ収集システム、及び、データ収集方法に広く適用でき有用である。

符号の説明

[0130]

１，１Ａ	データ収集システム
２０	ネットワーク
１００，１００Ａ	センサ機器
１２０	電池
１２２	環境発電素子
１３０	受信部（暗号鍵受信部）
１４０	送信部（パケット送信部、暗号鍵送信部）
１５０	記憶部（センサ側記憶部）
１６０	パケット生成部
１７０	暗号鍵生成部
２００，２００Ａ	ホスト機器
２１０	受信部（計測データ受信部、暗号鍵受信部）
２２０	送信部（暗号鍵送信部）
２３０	記憶部（ホスト側記憶部）
２４０	暗号鍵生成部
２５０	復号部
２６０	第１判断部
２７０	第２判断部

C 識別文字列

D 計測データ

K 暗号鍵

先行技術文献

特許文献

[0131] 特許文献1：特開２００５－１８２４４１号公報

請求の範囲

[請求項1] ホスト機器（２００）と、前記ホスト機器とネットワークを介して接続され、前記ホスト機器に計測データ（Ｄ）を送信するセンサ機器（１００）と、を備えたデータ収集システムであって、

前記センサ機器は、電池（１２０）又は環境発電素子（１２２）を有し、前記電池が供給する電力又は前記環境発電素子が発電する電力で駆動され、

前記ホスト機器は、

前記センサ機器に固有の暗号鍵（Ｋ）を生成する暗号鍵生成部（２４０）と、

前記暗号鍵生成部が生成した前記暗号鍵を記憶するホスト側記憶部（２３０）と、

公開鍵暗号基盤を用いて、前記ネットワークを介して、前記センサ機器に前記暗号鍵を送信する暗号鍵送信部（２２０）と、

前記センサ機器から前記計測データを受信する計測データ受信部（２１０）と、

を有し、

前記センサ機器は、

前記ホスト機器が送信する前記暗号鍵を受信する暗号鍵受信部（１３０）と、

前記暗号鍵受信部が受信する前記暗号鍵を記憶するセンサ側記憶部（１５０）と、

前記センサ側記憶部に記憶されている前記暗号鍵で前記計測データを暗号化し、暗号化した前記計測データを含むパケットを生成するパケット生成部（１６０）と、

前記パケット生成部の生成する前記パケットをブロードキャストで送信するパケット送信部（１４０）と、

を有する、

データ収集システム（１）。

[請求項2] 前記ホスト機器と前記センサ機器とはＢｌｕｅｔｏｏｔｈ（登録商標）規格を用いて通信を行い、

前記暗号鍵送信部は、前記ホスト機器と前記センサ機器とのペアリング時に前記センサ機器に前記暗号鍵を送信し、

前記パケット生成部は、暗号化した前記計測データを含むアドバタイズパケットを前記パケットとして生成する、

請求項１に記載のデータ収集システム。

[請求項3] 前記ホスト側記憶部及び前記センサ側記憶部は、共通の識別文字列（Ｃ）を記憶し、

前記パケット生成部は、暗号化した前記計測データ及び前記識別文字列を含む前記パケットを生成する、

請求項１又は２に記載のデータ収集システム。

[請求項4] 前記ホスト機器は、

前記暗号鍵を用いて、受信した前記パケットに含まれる、暗号化された前記計測データ及び前記識別文字列を復号する復号部（２５０）と、

前記復号部により復号された前記識別文字列と、前記ホスト側記憶部に記憶されている前記識別文字列とが一致するか否かを判断する第１判断部（２６０）と、

を更に備える、

請求項３に記載のデータ収集システム。

[請求項5] 前記第１判断部は、前記復号部により復号された前記識別文字列と前記ホスト側記憶部に記憶されている前記識別文字列とが一致しないと判断した場合に、受信した前記パケットを、データ収集の対象外の機器の送信したパケットと判断する、

請求項４に記載のデータ収集システム。

[請求項6] 前記ホスト機器は、前記計測データ受信部が受信する前記計測デー

タの時間変化に基づき、受信した前記計測データがデータ収集の対象外の機器の送信した計測データであるか否かを判断する第２判断部（２７０）、を更に備える、

請求項１から５のいずれか１項に記載のデータ収集システム。

[請求項7] ホスト機器（２００Ａ）と、前記ホスト機器とネットワーク（２０）を介して接続され、前記ホスト機器に計測データ（Ｄ）を送信するセンサ機器（１００Ａ）と、を備えたデータ収集システムであって、

前記センサ機器は、電池（１２０）又は環境発電素子（１２２）を有し、前記電池が供給する電力又は前記環境発電素子が発電する電力で駆動され、

前記センサ機器は、

前記センサ機器に固有の暗号鍵（Ｋ）を生成する暗号鍵生成部（１７０）と、

前記暗号鍵生成部が生成する前記暗号鍵を記憶するセンサ側記憶部（１５０）と、

公開鍵暗号基盤を用いて、前記ネットワークを介して、前記ホスト機器に前記暗号鍵を送信する暗号鍵送信部（１４０）と、

前記センサ側記憶部に記憶されている前記暗号鍵で前記計測データを暗号化し、暗号化した前記計測データを含むパケットを生成するパケット生成部（１６０）と、

前記パケット生成部の生成する前記パケットをブロードキャストで送信するパケット送信部（１４０）と、

を有し、

前記ホスト機器は、

前記センサ機器が送信する前記暗号鍵を受信する暗号鍵受信部（２１０）と、

前記暗号鍵受信部が受信する前記暗号鍵を記憶するホスト側記憶部（２３０）と、

前記センサ機器の送信する前記計測データを受信する計測データ受信部（２１０）と、

を有する、

データ収集システム（１Ａ）。

[請求項8] 電池（１２０）又は環境発電素子（１２２）を有し、前記電池の電力又は前記環境発電素子が発電する電力で駆動されるセンサ機器（１００）が送信する計測データ（Ｄ）を、前記センサ機器とネットワーク（２０）を介して接続されるホスト機器（２００）で収集するデータ収集方法であって、

前記ホスト機器が、前記センサ機器に固有の暗号鍵（Ｋ）を生成する暗号鍵生成ステップと、

前記ホスト機器が、前記ホスト機器のホスト側記憶部（２３０）に、生成された前記センサ機器に固有の暗号鍵を記憶する第１記憶ステップと、

前記ホスト機器が、公開鍵暗号基盤を用いて、前記ネットワークを介して、前記センサ機器に前記暗号鍵を送信する暗号鍵送信ステップと、

前記センサ機器が、前記ホスト機器が送信した前記暗号鍵を受信する暗号鍵受信ステップと、

前記センサ機器が、受信した前記暗号鍵を前記センサ機器のセンサ側記憶部（１５０）に記憶する第２記憶ステップと、

前記センサ機器が、前記センサ側記憶部に記憶されている前記暗号鍵で前記計測データを暗号化し、暗号化した前記計測データを含むパケットを生成するパケット生成ステップと、

前記センサ機器が、生成された前記パケットをブロードキャストで送信するパケット送信ステップと、

を備える、データ収集方法。

[請求項9] 電池（１２０）又は環境発電素子（１２２）を有し、前記電池の電

力又は前記環境発電素子が発電する電力で駆動されるセンサ機器（１００Ａ）が送信する計測データ（Ｄ）を、前記センサ機器とネットワーク（２０）を介して接続されるホスト機器（２００Ａ）で収集するデータ収集方法であって、

前記センサ機器が、前記センサ機器に固有の暗号鍵（Ｋ）を生成する暗号鍵生成ステップと、

前記センサ機器が、前記センサ機器のセンサ側記憶部（１５０）に、生成された前記センサ機器に固有の暗号鍵を記憶する第１記憶ステップと、

前記センサ機器が、公開鍵暗号基盤を用いて、前記ネットワークを介して、前記ホスト機器に前記暗号鍵を送信する暗号鍵送信ステップと、

前記ホスト機器が、前記センサ機器が送信した前記暗号鍵を受信する暗号鍵受信ステップと、

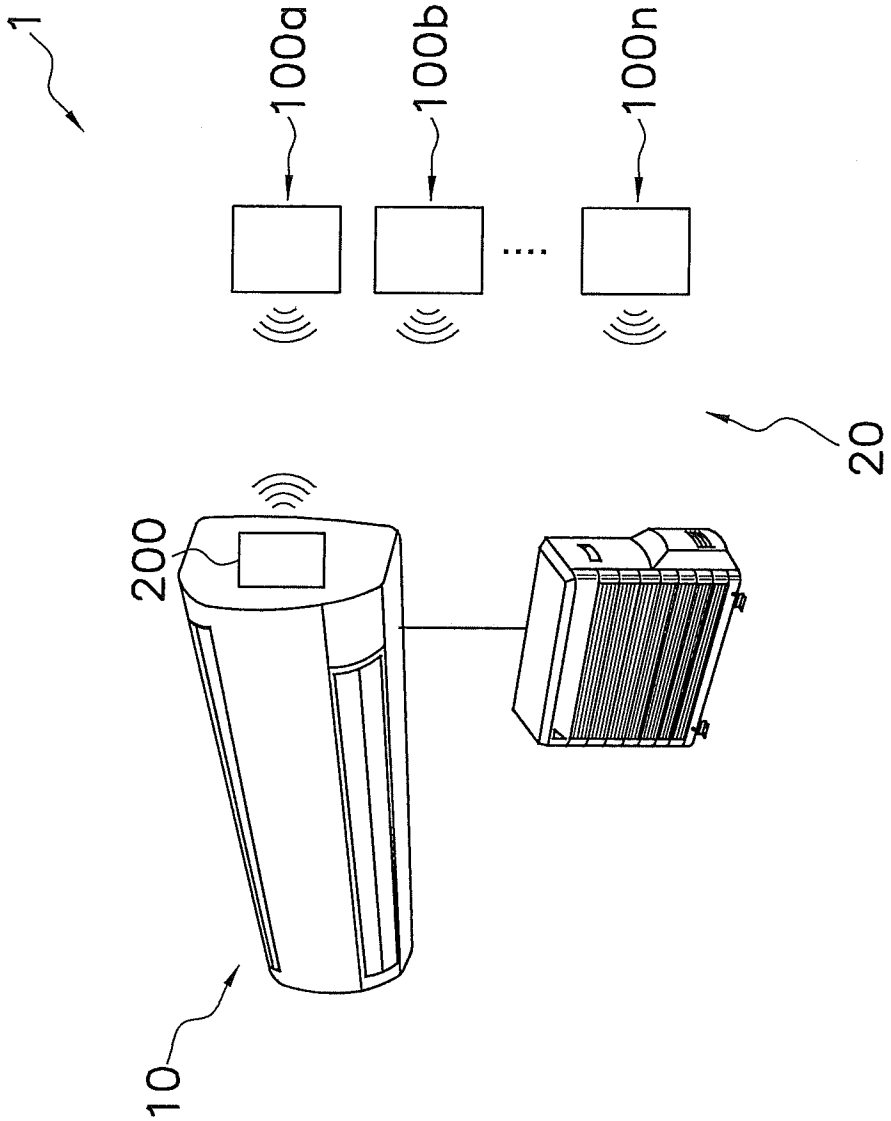
前記ホスト機器が、受信した前記暗号鍵を前記ホスト機器のホスト側記憶部（２３０）に記憶する第２記憶ステップと、

前記センサ機器が、前記センサ側記憶部に記憶されている前記暗号鍵で前記計測データを暗号化し、暗号化した前記計測データを含むパケットを生成するパケット生成ステップと、

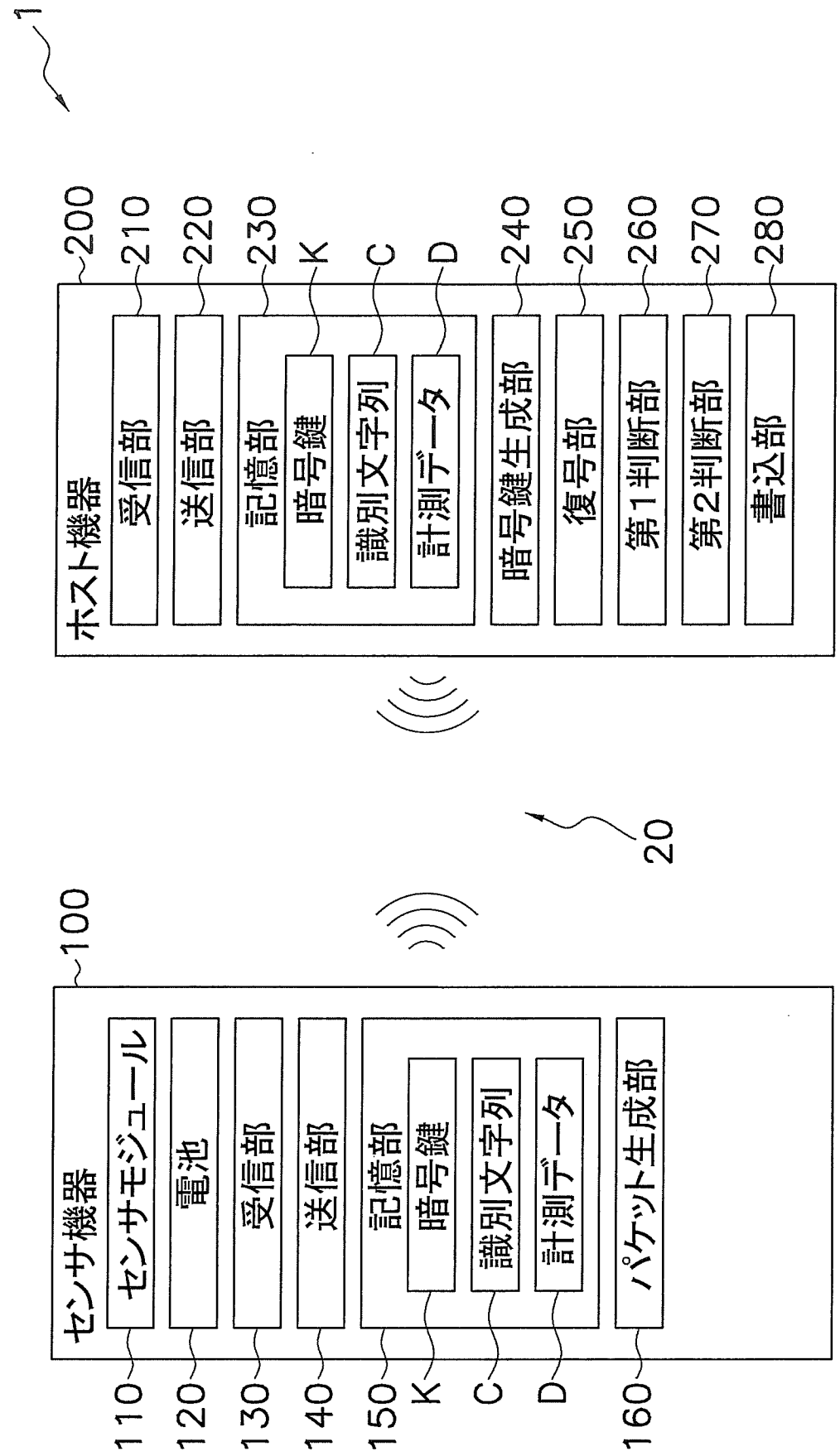
前記センサ機器が、生成された前記パケットをブロードキャストで送信するパケット送信ステップと、

を備える、データ収集方法。

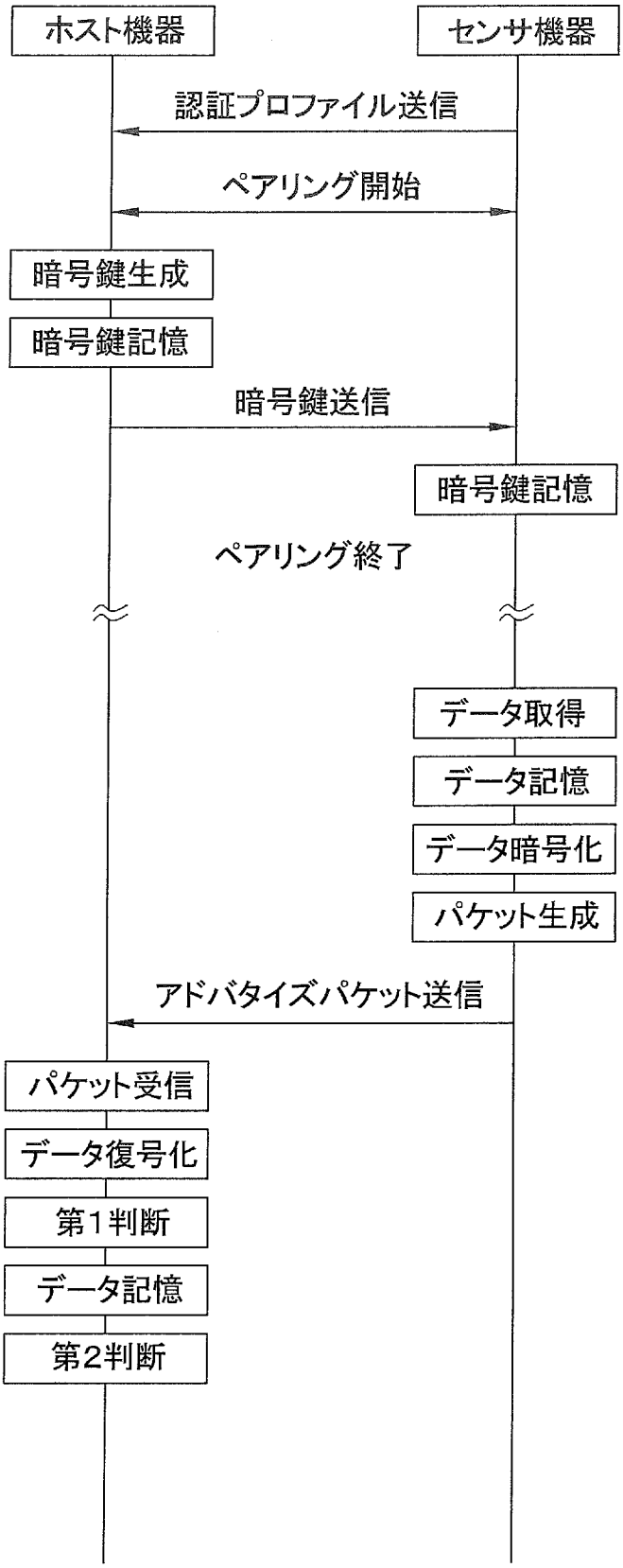
[図1]



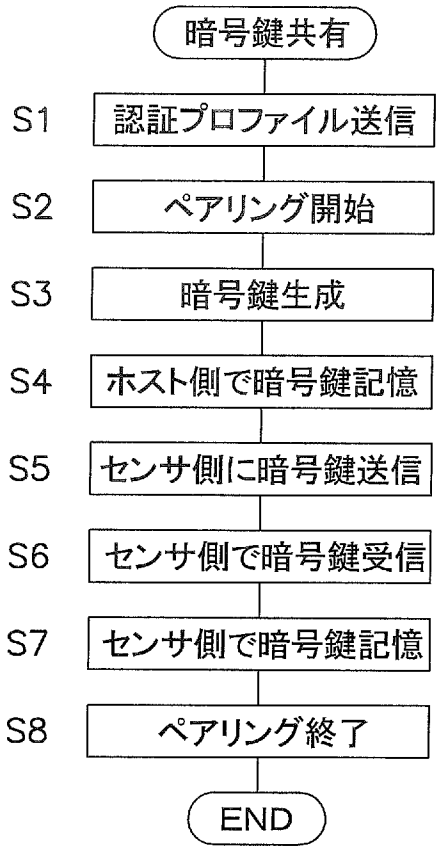
[図2]


1
200
ホスト機器
210
受信部
220
送信部
230
記憶部
K
暗号鍵
C
識別文字列
D
計測データ
240
暗号鍵生成部
250
復号部
260
第1判断部
270
第2判断部
280
書込部
20
100
センサ機器
センサモジュール
電池
受信部
送信部
記憶部
暗号鍵
識別文字列
計測データ
パケット生成部
110
120
130
140
150
K
C
D
160

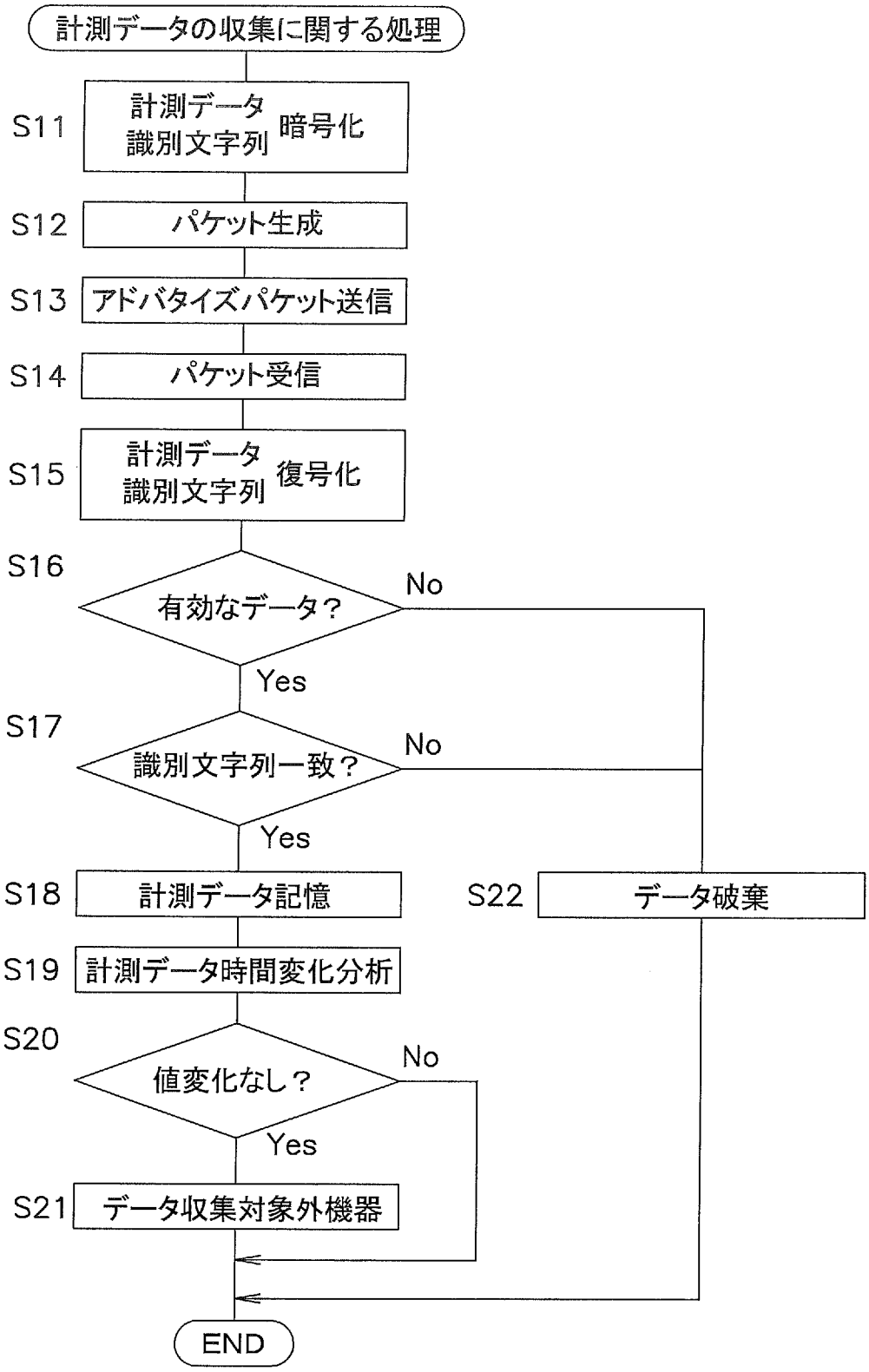
[図3]


ホスト機器
センサ機器
認証プロファイル送信
ペアリング開始
暗号鍵生成
暗号鍵記憶
暗号鍵送信
暗号鍵記憶
ペアリング終了
データ取得
データ記憶
データ暗号化
パケット生成
アドバタイズパケット送信
パケット受信
データ復号化
第1判断
データ記憶
第2判断

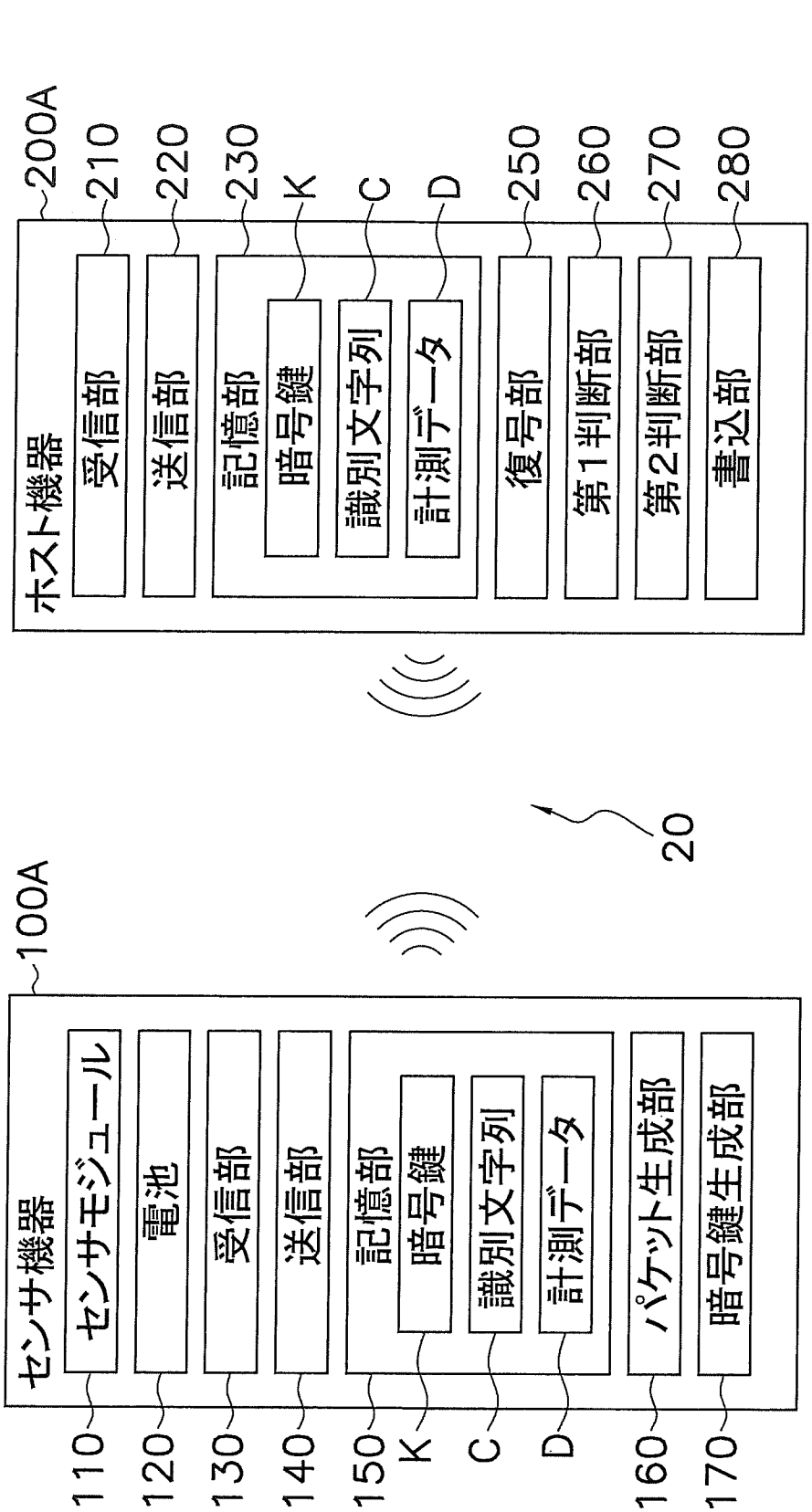
[図4]


暗号鍵共有
S1
認証プロファイル送信
S2
ペアリング開始
S3
暗号鍵生成
S4
ホスト側で暗号鍵記憶
S5
センサ側に暗号鍵送信
S6
センサ側で暗号鍵受信
S7
センサ側で暗号鍵記憶
S8
ペアリング終了
END

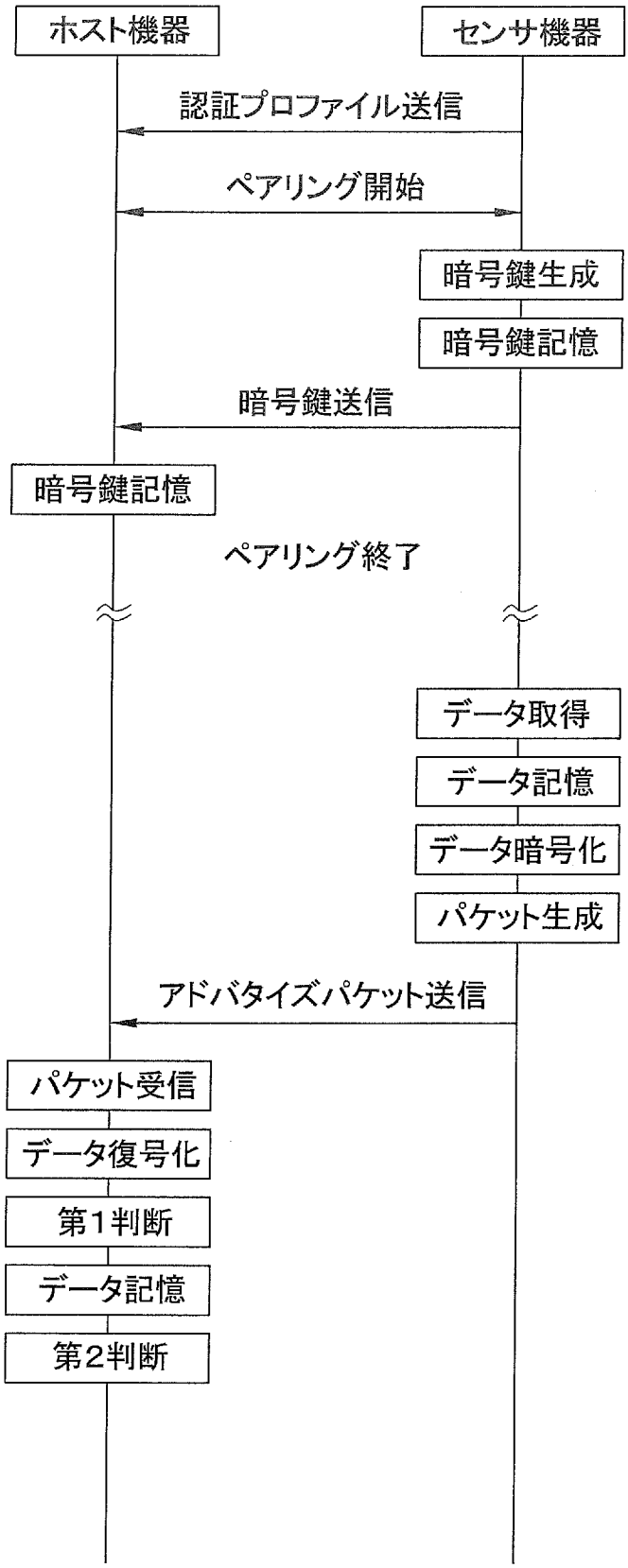
[図5]


計測データの収集に関する処理
S11
計測データ識別文字列 暗号化
S12
パケット生成
S13
アドバタイズパケット送信
S14
パケット受信
S15
計測データ識別文字列 復号化
S16
有効なデータ？
No
Yes
S17
識別文字列一致？
No
Yes
S18
計測データ記憶
S19
計測データ時間変化分析
S20
値変化なし？
No
Yes
S21
データ収集対象外機器
S22
データ破棄
END

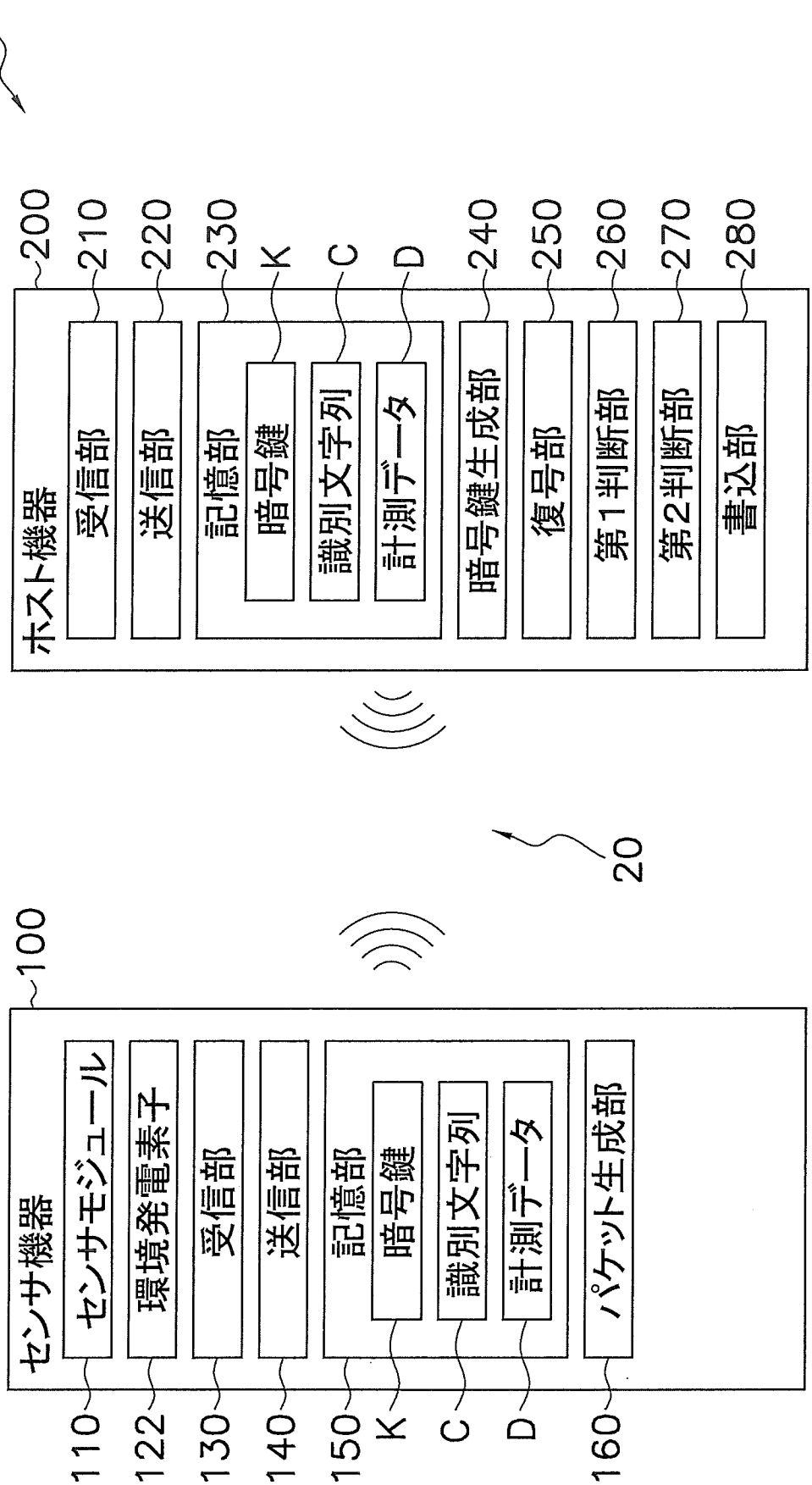
[図6]


1A
200A
ホスト機器
受信部
210
送信部
220
記憶部
230
暗号鍵
K
識別文字列
C
計測データ
D
復号部
250
第1判断部
260
第2判断部
270
書込部
280
20
100A
センサ機器
センサモジュール
110
電池
120
受信部
130
送信部
140
記憶部
150
暗号鍵
K
識別文字列
C
計測データ
D
パケット生成部
160
暗号鍵生成部
170

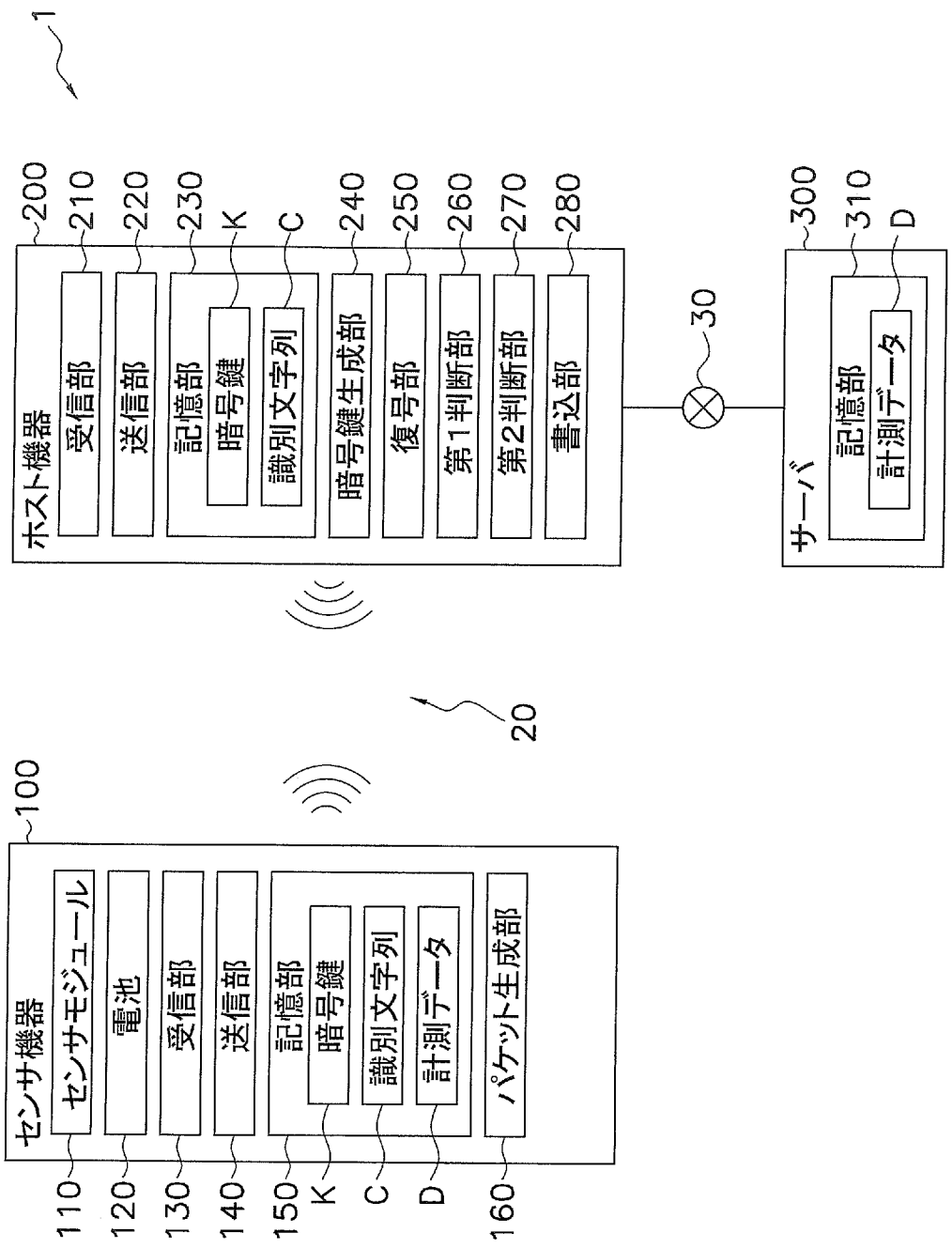
[図7]


ホスト機器
センサ機器
認証プロファイル送信
ペアリング開始
暗号鍵生成
暗号鍵記憶
暗号鍵送信
暗号鍵記憶
ペアリング終了
データ取得
データ記憶
データ暗号化
パケット生成
アドバタイズパケット送信
パケット受信
データ復号化
第1判断
データ記憶
第2判断

[図8]


1
ホスト機器
200
受信部
210
送信部
220
記憶部
230
暗号鍵
K
識別文字列
C
計測データ
D
暗号鍵生成部
240
復号部
250
第1判断部
260
第2判断部
270
書込部
280
20
センサ機器
100
センサモジュール
110
環境発電素子
122
受信部
130
送信部
140
記憶部
150
暗号鍵
K
識別文字列
C
計測データ
D
パケット生成部
160

[図9]


1
200
ホスト機器
210
受信部
220
送信部
230
記憶部
K
暗号鍵
C
識別文字列
240
暗号鍵生成部
250
復号部
260
第1判断部
270
第2判断部
280
書込部
30
300
サーバ
310
記憶部
D
計測データ
20
100
センサ機器
110
センサモジュール
120
電池
130
受信部
140
送信部
150
記憶部
K
暗号鍵
C
識別文字列
D
計測データ
160
パケット生成部

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/036470

A. CLASSIFICATION OF SUBJECT MATTER
H04L 9/08(2006.01)i; G06F 21/60(2013.01)i
FI: H04L9/00 601B; G06F21/60 360

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)
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	1971-2020
Registered utility model specifications of Japan	1996-2020
Published registered utility model applications of Japan	1994-2020

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	JP 2016-100757 A (PANASONIC IP MANAGEMENT CO., LTD.) 30 May 2016 (2016-05-30) in particular, paragraphs [0015]-[0017], [0031], [0037], [0042], [0051]-[0052], [0070], [0085], fig. 1	1-9
Y	WO 2015/105141 A1 (SUMITOMO ELECTRIC INDUSTRIES, LTD.) 16 July 2015 (2015-07-16) in particular, paragraph [0089]	1, 3-9
Y	in particular, paragraphs [0054], [0089]	2
Y	JP 2019-50511 A (BROTHER INDUSTRIES, LTD.) 28 March 2019 (2019-03-28) in particular, paragraphs [0074]-[0075]	1-9
Y	JP 2017-207904 A (NTT COMMUNICATIONS CORPORATION) 24 November 2017 (2017-11-24) in particular, paragraphs [0006], [0017]-[0022], [0085]-[0094]	6

☐ 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
09 December 2020 (09.12.2020)	22 December 2020 (22.12.2020)

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
Information on patent family members

International application No.
PCT/JP2020/036470

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2016-100757 A	30 May 2016	US 2016/0150404 A1 in particular, paragraphs [0020]-[0023], [0038], [0046], [0051], [0061]-[0062], [0080], [0095], fig. 1	
WO 2015/105141 A1	16 Jul. 2015	JP 2015-133581 A in particular, paragraphs [0054], [0089]	
JP 2019-50511 A	28 Mar. 2019	US 2019/0081801 A1 in particular, paragraphs [0082]-[0083]	
JP 2017-207904 A	24 Nov. 2017	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2020/036470

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

H04L 9/08(2006.01)i; G06F 21/60(2013.01)i
FI: H04L9/00 601B; G06F21/60 360

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））

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	１９７１－２０２０年
日本国実用新案登録公報	１９９６－２０２０年
日本国登録実用新案公報	１９９４－２０２０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	JP 2016-100757 A (パナソニックＩＰマネジメント株式会社) 30.05.2016 (2016-05-30) 特に段落0015-0017, 0031, 0037, 0042, 0051-0052, 0070, 0085, 図1	1-9
Y	WO 2015/105141 A1 (住友電気工業株式会社) 16.07.2015 (2015-07-16) 特に段落0089	1, 3-9
Y	特に段落0054, 0089	2
Y	JP 2019-50511 A (ブラザー工業株式会社) 28.03.2019 (2019-03-28) 特に段落0074-0075	1-9
Y	JP 2017-207904 A (エヌ・ティ・ティ・コミュニケーションズ株式会社) 24.11.2017 (2017-11-24) 特に段落0006, 0017-0022, 0085-0094	6

☐ 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抵触するものではなく、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
09.12.2020	22.12.2020

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
児玉　崇晶 5S 3651

電話番号 03-3581-1101 内線 3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2020/036470

引用文献	公表日	パテントファミリー文献	公表日
JP 2016-100757 A	30.05.2016	US 2016/0150404 A1 特に段落0020-0023, 0038, 0046, 0051, 0061-0062, 0080, 0095, FIG.1	
WO 2015/105141 A1	16.07.2015	JP 2015-133581 A 特に段落0054, 0089	
JP 2019-50511 A	28.03.2019	US 2019/0081801 A1 特に段落0082-0083	
JP 2017-207904 A	24.11.2017	（ファミリーなし）	