(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
2024年1月11日(11.01.2024)

WIPO | PCT

(10) 国際公開番号
WO 2024/009355 A1

(51) 国際特許分類:
G06F 21/44 (2013.01)

(21) 国際出願番号： PCT/JP2022/026598

(22) 国際出願日： 2022年7月4日(04.07.2022)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(71) 出願人: 日本電信電話株式会社 (**NIPPON TELEGRAPH AND TELEPHONE CORPORATION**) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目５番１号 Tokyo (JP).

(72) 発明者: 工藤 史堯(**KUDO, Fumiaki**); 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP). 永井 彰(**NAGAI, Akira**); 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP). 飯島 悠介(**IIJIMA, Yusuke**); 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP).

(74) 代理人: 中尾 直樹, 外 (**NAKAO, Naoki** et al.); 〒1600022 東京都新宿区新宿三丁目１番２２号 新宿ＮＳＯビル６階 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, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH,

WO 2024/009355 A1

(54) **Title:** AUTHENTICATION SYSTEM, AUTHENTICATION METHOD, AND PROGRAM

(54) 発明の名称： 認証システム、認証方法、プログラム

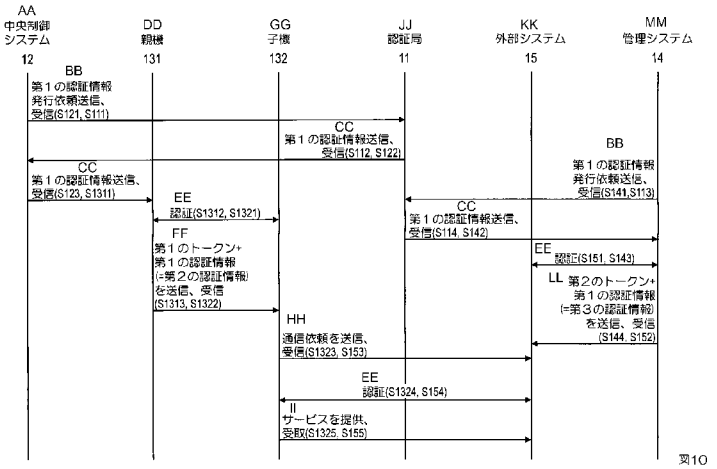


図10

AA Central control system
BB Transmit/receive first authentication information issuance request
CC Transmit/receive first authentication information
DD Parent device
EE Execute authentication
FF Transmit/receive first token + first authentication information (= second authentication information)
GG Child device
HH Transmit/receive communication request
II Provide/receive service
JJ Certificate authority
KK External system
LL Transmit/receive second token + first authentication information (= third authentication information)
MM Management system

(57) **Abstract:** This authentication system comprises a certificate authority, a central control system, a group including a drone serving as a parent device and a drone serving as a child device, a management system, and an external system. The central control system includes a first authentication information transmission unit for transmitting first authentication information received from the certificate authority to the parent device; the parent device includes an authentication unit for executing authentication with the child device belonging to the same group and a second authentication information

［続葉有］

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, 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, SC, 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)）

transmission unit for transmitting second authentication information, including a first token with an expiration time and the first authentication information, to the authenticated child device; the management system includes an authentication unit for executing authentication with the external system and a third authentication information transmission unit for transmitting third authentication information, including a second token and the first authentication information received from the certificate authority, to the authenticated external system; and the child device and the external system include an authentication unit for executing authentication on the basis of the second authentication information and the third authentication information.

(57) 要約：認証局と、中央制御システムと、親機である無人機と子機である無人機を含むグループと、管理システムと、外部システムを含む認証システムであって、前記中央制御システムは、前記認証局から受信した第１の認証情報を前記親機に送信する第１認証情報送信部を含み、前記親機は、同じグループに属する前記子機との認証を実行する認証部と、認証された前記子機に有効期限付きの第１のトークンと前記第１の認証情報を含む第２の認証情報を送信する第２認証情報送信部を含み、前記管理システムは、前記外部システムとの認証を実行する認証部と、認証された前記外部システムに第２のトークンと前記認証局から受信した前記第１の認証情報を含む第３の認証情報を送信する第３認証情報送信部を含み、前記子機と前記外部システムは、前記第２の認証情報と前記第３の認証情報に基づいて認証を実行する認証部を含む。

明　細　書

発明の名称 ： 認証システム、認証方法、プログラム

技術分野

[0001] 本発明は、無人機を認証する認証システム、認証方法、プログラムに関する。

背景技術

[0002] 無人機（人が搭乗しない乗り物または輸送機械）を使ったサービスでは、無人機がグループを組んでサービスを提供することも検討されており、今後膨大な数の無人機をセキュアに管理する必要性が出てくると想定される。

[0003] 無人機の管理にあたっては、無人機のグループが状況に応じて親機同士で子機を融通し合うなど、柔軟性の高い管理方法が求められる。

[0004] ＩｏＴデバイスや無人機の認証を実現する方法として、中央システム側からＩｏＴデバイスや無人機に対して電子証明書及び秘密鍵を配布するシステム（非特許文献１）が開示されている。

先行技術文献

非特許文献

[0005] 非特許文献1：Prodrone Co., Ltd., “ドローンの通信セキュリティ強化のための実証実験を開始 ～GMOグローバルサインのセキュリティ技術で「空」もセキュアに～”、［online］、令和 3 年 5 月 14 日、Prodrone Co., Ltd.,［令和 4 年 6 月 20日検索］、インターネット〈URL：https://www.prodrone.com/jp/release/7589/〉

発明の概要

発明が解決しようとする課題

[0006] 図１に今後実現される可能性がある無人機によるサービス提供システムの構成例を示す。同図に示すようにこの構成例では、中央制御システム９２と、親機９３１と子機９３２を含むグループ９３をＮ個（９３－１，…，９３－ｎ，…，９３－Ｎ、Ｎは１以上の整数）含む。ｎ番目のグループに属する

親機９３１は親機９３１－ｎと表記される。

[0007] 同図においては便宜上各グループの子機９３２の台数は全てＭ台（Ｍは１以上の整数）としたが、子機９３２の台数はグループごとに異なっていてもよい。ｎ番目のグループに属し、グループ内でｍ台目に該当する子機９３２は子機９３２－ｎ－ｍと表記される。この表記方法は後述の実施例においても踏襲される。

[0008] 無人機が無人機同士もしくはその他システムとセキュアな通信を行うためには、無人機に、各個体を識別できる認証情報を配布する必要があるが、図１においてＮ，Ｍの値が大きい場合、すなわち無人機が膨大に存在する場合には、すべての個体の認証情報や権限を中央で管理するのは困難である。また、グループの組み換え時には、適切に認証情報や権限の制御が行われる必要があるが、グループの数が膨大にある場合は、中央で管理するのは困難である。

[0009] そこで本発明は、管理対象の無人機や無人機のグループが膨大にある場合であっても、これらの認証情報や権限を中央で管理することができる認証システムを提供することを目的とする。

課題を解決するための手段

[0010] 本発明の認証システムは、認証局と、中央制御システムと、親機である無人機と子機である無人機を含むグループと、管理システムと、外部システムを含む。

[0011] 中央制御システムは、認証局から受信した第１の認証情報を親機に送信する第１認証情報送信部を含む。

[0012] 親機は、同じグループに属する子機との認証を実行する認証部と、認証された子機に有効期限付きの第１のトークンと第１の認証情報を含む第２の認証情報を送信する第２認証情報送信部を含む。

[0013] 管理システムは、外部システムとの認証を実行する認証部と、認証された外部システムに第２のトークンと認証局から受信した第１の認証情報を含む第３の認証情報を送信する第３認証情報送信部を含む。

[0014] 子機と外部システムは、第２の認証情報と第３の認証情報に基づいて認証を実行する認証部を含む。

発明の効果

[0015] 本発明の認証システムによれば、管理対象の無人機や無人機のグループが膨大にある場合であっても、これらの認証情報や権限を中央で管理することができる。

図面の簡単な説明

[0016] [図1]今後実現される可能性がある無人機によるサービス提供システムの構成例を示す図。

[図2]実施例１の認証システムの機能構成を示すブロック図。

[図3]実施例１の認証局の機能構成を示すブロック図。

[図4]実施例１の中央制御システムの機能構成を示すブロック図。

[図5]実施例１の親機の機能構成を示すブロック図。

[図6]実施例１の子機の機能構成を示すブロック図。

[図7]実施例１の管理システムの機能構成を示すブロック図。

[図8]実施例１の外部システムの機能構成を示すブロック図。

[図9]実施例１の認証システムの動作の概略を示す図。

[図10]実施例１の認証システムの動作を示すシーケンス図。

[図11]実施例２の認証システムの機能構成を示すブロック図。

[図12]実施例２の認証局の機能構成を示すブロック図。

[図13]実施例２の中央制御システムの機能構成を示すブロック図。

[図14]実施例２の親機の機能構成を示すブロック図。

[図15]実施例２の子機の機能構成を示すブロック図。

[図16]実施例２の管理システムの機能構成を示すブロック図。

[図17]実施例２の外部システムの機能構成を示すブロック図。

[図18]実施例２の認証システムの動作を示すシーケンス図。

[図19]実施例３の認証システムの機能構成を示すブロック図。

[図20]コンピュータの機能構成例を示す図。

発明を実施するための形態

[0017] 以下、本発明の実施の形態について、詳細に説明する。なお、同じ機能を有する構成部には同じ番号を付し、重複説明を省略する。

実施例 1

[0018] 以下、図２を参照して実施例１の認証システム１の構成を説明する。同図に示すように本実施例の認証システム１は、認証局１１と、中央制御システム１２と、親機１３１と、子機１３２と、管理システム１４と、外部システム１５を含む構成である。親機１３１、子機１３２、外部システム１５は、ＴＥＥやＳＥなどのセキュア環境内に配置されており、セキュア環境内に配置されている状態を示すために各ブロックをカギ括弧で囲んで示した。

[0019] なお、本システムは、１台の親機１３１とM台の子機１３２を含むグループ１３をＮ個（グループ１３－１，…，グループ１３－ｎ，…，グループ１３－Ｎ、Ｎは１以上の整数）含む。親機１３１は１つのグループ内に複数台属していてもよい。子機１３２の台数はグループごとに異なっていてもよい。

[0020] ｎ番目のグループに属する親機１３１は親機１３１－ｎと表記され、ｎ番目のグループに属し、グループ内でｍ台目に該当する子機１３２は子機１３２－ｎ－ｍと表記される。枝番を付さずに、親機１３１、子機１３２と表現する場合は、任意の親機、子機を指すものとする。

[0021] 以下、図３を参照して、認証局１１の機能構成を説明する。認証局１１は、第１認証情報発行依頼受信部１１１と、第１認証情報送信部１１２と、第１認証情報発行依頼受信部１１３と、第１認証情報送信部１３４を含む。

[0022] 以下、図４を参照して、中央制御システム１２の機能構成を説明する。中央制御システム１２は、第１認証情報発行依頼送信部１２１と、第１認証情報受信部１２２と、第１認証情報送信部１２３を含む。中央制御システム１２を複数の装置で構成する場合、各構成要件（１２１～１２３）のそれぞれを別の装置としてもよい。また構成要件のうち２つの機能を備える装置と、構成要件のうち１つの機能を備える装置により構成されていてもよい。

[0023] 以下、図５を参照して、親機１３１の機能構成を説明する。親機１３１は、第１認証情報受信部１３１１と、認証部１３１２と、第２認証情報送信部１３１３を含む。

[0024] 以下、図６を参照して、子機１３２の機能構成を説明する。子機１３２は、認証部１３２１と、第２認証情報受信部１３２２と、通信依頼送信部１３２３と、認証部１３２４と、サービス提供部１３２５を含む。

[0025] 以下、図７を参照して、管理システム１４の機能構成を説明する。管理システム１４は、第１認証情報発行依頼送信部１４１と、第１認証情報受信部１４２と、認証部１４３と、第３認証情報送信部１４４を含む。管理システム１４を複数の装置で構成する場合、各構成要件（１４１～１４４）のそれぞれを別の装置としてもよい。また構成要件のうち２つ以上の機能を備える装置と、その他の構成要件として機能する装置により構成されていてもよい。

[0026] 以下、図８を参照して、外部システム１５の機能構成を説明する。外部システム１５は、認証部１５１と、第３認証情報受信部１５２と、通信依頼受信部１５３と、認証部１５４と、サービス受取部１５５を含む。外部システム１５を複数の装置で構成する場合、各構成要件（１５１～１５５）のそれぞれを別の装置としてもよい。また構成要件のうち２つ以上の機能を備える装置と、その他の構成要件として機能する装置により構成されていてもよい。

[0027] 図９に示すように、本実施例の認証システム１は、権限管理を階層構造にし、中央制御システム１２は親機１３１の認証情報（第１の認証情報５、同図）のみを管理することを特徴とする。第１の認証情報として任意の認証情報を用いることができるが、例えばシステムをＩＤベース暗号方式で組む場合、第１の認証情報＝秘密鍵となる（詳細は実施例２を参照）。

[0028] 親機１３１はＳＥ（Secure Element）やＴＥＥ(Trusted Execution Environment)などのセキュア環境を搭載し、子機１３２の認証情報（第２の認証情報６、同図）の管理・配布を行う。

[0029] 子機１３２には親機１３１と子機１３２の間で互いに正規の端末であることを確認可能な認証情報（第４の認証情報７、同図）のみ事前に配布しておく。第４の認証情報７として、例えば事前共有鍵や物理的な特徴を使った画像認識などが挙げられる。例えば同図に例示するように、グループ１３－１に属していた子機１３２－１－Ｍが、グループ１３－ｎに配属変更となった場合、グループ１３－ｎの親機１３１－ｎは、新しく配属された子機１３２－１－Ｍに対して、第４の認証情報７を事前に配布し、互いに正規の端末であることを確認可能な状態にしておく。

[0030] また、管理システム１４は外部システム１５との認証に用いる認証情報（第５の認証情報Ａ、同図）を事前に配布しておくものとする。

[0031] 以下、図１０のシーケンスに基づいて、本実施例の認証システム１の各装置の動作を構成要件ごとに説明する。

[0032] ＜中央制御システム１２－第１認証情報発行依頼送信部１２１＞

まず、中央制御システム１２の第１認証情報発行依頼送信部１２１は、認証局１１に第１の認証情報発行依頼を送信する（Ｓ１２１）。

[0033] ＜認証局１１－第１認証情報発行依頼受信部１１１＞

認証局１１の第１認証情報発行依頼受信部１１１は、中央制御システム１２から第１の認証情報発行依頼を受信する（Ｓ１１１）。

[0034] ＜認証局１１－第１認証情報送信部１１２＞

認証局１１の第１認証情報送信部１１２は第１の認証情報を発行し、中央制御システム１２に送信する（Ｓ１１２）。

[0035] ＜中央制御システム１２－第１認証情報受信部１２２＞

中央制御システム１２の第１認証情報受信部１２２は、認証局１１から第１の認証情報を受信する（Ｓ１２２）。

[0036] ＜中央制御システム１２－第１認証情報送信部１２３＞

中央制御システム１２の第１認証情報送信部１２３は、認証局１１から受信した第１の認証情報を親機１３１に送信する（Ｓ１２３）。

[0037] ＜親機１３１－第１認証情報受信部１３１１＞

親機１３１の第１認証情報送信部１３１１は、中央制御システム１２から第１の認証情報を受信する（Ｓ１３１１）。

[0038] ＜親機１３１－認証部１３１２＞

親機１３１の認証部１３１２は、同じグループに属する子機１３２との認証を実行する（Ｓ１３１２）。認証には前述した第４の認証情報７（図９）が用いられる。親機１３１は近接通信（Bluetooth（登録商標），NFCなど）を用いて子機１３２との認証を実行すれば好適である。

[0039] 本システムは、従来の認証システムには無い特徴である無人機である親機１３１が中間認証局として機能するという特徴を備えているため、無人機である中間認証局自身が移動（航行、走行、飛行）して、子機１３２に近接して近接通信を確立することができるため、なりすましや運用ミスなどが発生するリスクを低減でき、従来の認証システムに無い方法でセキュアな通信を確立することができる。

[0040] ＜子機１３２－認証部１３２１＞

子機１３２の認証部１３２１は、同じグループに属する親機１３１との認証を実行する（Ｓ１３２１）。認証には前述した第４の認証情報７（図９）が用いられる。子機１３２は近接通信を用いて親機１３１との認証を実行すれば好適である。

[0041] ＜親機１３１－第２認証情報送信部１３１３＞

親機１３１の第２認証情報送信部１３１３は、ステップＳ１３１２，Ｓ１３２１で認証済みの子機１３２に有効期限付きの第１のトークンと第１の認証情報を含む第２の認証情報を送信する（Ｓ１３１３）。親機１３１の第２認証情報送信部１３１３は、近接通信を用いて子機１３２に第２の認証情報を送信すれば好適である。

[0042] 第１のトークンは、親機１３１が子機１３２に払い出すワンタイムトークンとすれば好適である。ワンタイムトークンには、認証・権限情報と有効期限が書き込まれ、外部システム１５が正当な相手であることが確認できるようにしておく。例えばシステムをＩＤベース暗号方式で組む場合、第１のト

ークン＝子機１３２のＩＤとすればよい。

[0043] ＜子機１３２－第２認証情報受信部１３２２＞

ステップＳ１３１２，Ｓ１３２１で認証済みの子機１３２の第２認証情報受信部１３２２は、親機１３１から第２の認証情報を受信する（Ｓ１３２２）。第２認証情報受信部１３２２は、近接通信を用いて第２の認証情報を受信すれば好適である。

[0044] ＜管理システム１４－第１認証情報発行依頼送信部１４１＞

管理システム１４の第１認証情報発行依頼送信部１４１は、認証局１１に第１の認証情報発行依頼を送信する（Ｓ１４１）。

[0045] ＜認証局１１－第１認証情報発行依頼受信部１１３＞

認証局１１の第１認証情報発行依頼受信部１１３は、管理システム１４から第１の認証情報発行依頼を受信する（Ｓ１１３）。

[0046] ＜認証局１１－第１認証情報送信部１１４＞

認証局１１の第１認証情報送信部１１４は第１の認証情報を発行し、管理システム１４に送信する（Ｓ１１４）。

[0047] ＜管理システム１４－第１認証情報受信部１４２＞

管理システム１４の第１認証情報受信部１４２は、認証局１１から第１の認証情報を受信する（Ｓ１４２）。

[0048] ＜外部システム１５－認証部１５１＞

外部システム１５の認証部１５１は、管理システム１４との認証を実行する（Ｓ１５１）。認証には前述した第５の認証情報Ａ（図９）が用いられる。

[0049] ＜管理システム１４－認証部１４３＞

管理システム１４の認証部１４３は、外部システム１５との認証を実行する（Ｓ１４３）。認証には前述した第５の認証情報Ａ（図９）が用いられる。

[0050] ＜管理システム１４－第３認証情報送信部１４４＞

管理システム１４の第３認証情報送信部１４４は、認証済みの外部システ

ム１５に第２のトークンと認証局１１から受信した第１の認証情報を含む第３の認証情報を送信する（Ｓ１４４）。例えばシステムをＩＤベース暗号方式で組む場合、第２のトークン＝外部システム１５のＩＤとすればよい。

[0051] ＜外部システム１５－第３認証情報受信部１５２＞

外部システム１５の第３認証情報受信部１５２は、管理システム１４から第３の認証情報を受信する（Ｓ１５２）。

[0052] ＜子機１３２－通信依頼送信部１３２３＞

子機１３２の通信依頼送信部１３２３は、外部システム１５に通信依頼を送信する（Ｓ１３２３）。

[0053] ＜外部システム１５－通信依頼受信部１５３＞

外部システム１５の通信依頼受信部１５３は、子機１３２から通信依頼を受信する（Ｓ１５３）。

[0054] ＜外部システム１５－認証部１５４＞

外部システム１５の認証部１５４は、第２の認証情報と第３の認証情報に基づいて、通信依頼の送信元である子機１３２との認証を実行する（Ｓ１５４）。例えばシステムをＩＤベース暗号方式で組む場合、子機１３２のＩＤ、外部システム１５のＩＤ、秘密鍵を用いて、参考特許文献１に記載の方法で認証を実行することができる。

[0055] （参考特許文献１：特開２０２１－０１９２２３号公報）

＜子機１３２－認証部１３２４＞

子機１３２の認証部１３２４は、第２の認証情報と第３の認証情報に基づいて、通信依頼の送信先である外部システム１５との認証を実行する（Ｓ１３２４）。ステップＳ１５４と同様、システムをＩＤベース暗号方式で組む場合、参考特許文献１に記載の方法で認証を実行することができる。

[0056] ＜子機１３２－サービス提供部１３２５＞

認証済みの子機１３２のサービス提供部１３２５は、認証済みの外部システムに対して、サービスを提供する（Ｓ１３２５）。サービスの典型例として、物流サービスなどがある。外部システム１５の具体例として荷物を預か

るシステムなどが考えられる。

[0057] ＜外部システム１５－サービス受取部１５５＞

認証済みの外部システム１５のサービス受取部１５５は、認証済みの子機１３２からサービスを受け取る（Ｓ１５５）。物流サービスであればこの動作は荷物の受け取りに該当する。

実施例 2

[0058] 以下、図１１を参照して実施例１の認証システム１をＩＤベース暗号方式で構成した実施例２の認証システム２の機能構成を説明する。同図に示すように本実施例の認証システム１は、認証局２１と、中央制御システム２２と、親機２３１と、子機２３２と、管理システム２４と、外部システム２５を含む構成である。

[0059] 本実施例において、無人機（親機２３１、子機２３２）はドローンであり、管理システム２４はスマートロッカー管理システムであり、外部システム２５はスマートロッカーである。また、第１の認証情報は秘密鍵であり、第１のトークンは、子機のＩＤであり、第２のトークンは、外部システムのＩＤであり、子機２３２と外部システム２５は、子機２３２のＩＤと、外部システム２５のＩＤと、秘密鍵に基づいて、ＩＤベース暗号方式により認証を実行することを特徴とする。

[0060] 図１２～図１７に各装置、システムの機能構成を示す。各装置、システムの構成要件の名称は実施例１と同じであり、符号の一部が変更されている。

[0061] より詳細には、認証局２１は、第１認証情報発行依頼受信部２１１と、第１認証情報送信部２１２と、第１認証情報発行依頼受信部２１３と、第１認証情報送信部２３４を含み、中央制御システム２２は、第１認証情報発行依頼送信部２２１と、第１認証情報受信部２２２と、第１認証情報送信部２２３を含み、親機２３１は、第１認証情報受信部２３１１と、認証部２３１２と、第２認証情報送信部２３１３を含み、子機２３２は、認証部２３２１と、第２認証情報受信部２３２２と、通信依頼送信部２３２３と、認証部２３２４と、サービス提供部２３２５を含み、管理システム２４は、第１認証情

報発行依頼送信部２４１と、第１認証情報受信部２４２と、認証部２４３と、第３認証情報送信部２４４を含み、外部システム２５は、認証部２５１と、第３認証情報受信部２５２と、通信依頼受信部２５３と、認証部２５４と、サービス受取部２５５を含む。

[0062] 親機２３１、子機２３２、外部システム２５は、ＴＥＥやＳＥなどのセキュア環境内に配置されており、セキュア環境内に配置されている状態を示すために各ブロックをカギ括弧で囲んで示した。本実施例では、ルート鍵発行局（ＫＧＣ）である認証局２１配下の中間鍵発行局（中間ＫＧＣ）を、親機２３１のセキュア環境内、および管理システム２４に配置する。

[0063] 以下、図１８のシーケンスに基づいて、本実施例の認証システム２の各装置の動作を説明する。

[0064] ＜ステップＳ２２１，Ｓ２１１，Ｓ２１２，Ｓ２２２，Ｓ２２３，Ｓ２３１１＞

実施例１のステップＳ１２１，Ｓ１１１，Ｓ１１２，Ｓ１２２，Ｓ１２３，Ｓ１３１１において、第１の認証情報→秘密鍵と読み替えた動作が、同名の構成要件によりそれぞれ実行される。

[0065] ＜ステップＳ２３１２，Ｓ２３２１＞

実施例１のステップＳ１３１２，Ｓ１３２１と同じ動作が、同名の構成要件によりそれぞれ実行される。

[0066] ＜ステップＳ２３１３，Ｓ２３２２＞

実施例１のステップＳ１３１３，Ｓ１３２２において、第１のトークン→配送主情報、権限有効期限を組み込んだ子機２３２のＩＤ（公開鍵）、第１の認証情報→秘密鍵と読み替えた動作が、同名の構成要件によりそれぞれ実行される。

[0067] ＜ステップＳ２４１，Ｓ２１３，Ｓ２１４，Ｓ２４２＞

実施例１のステップＳ１４１，Ｓ１１３，Ｓ１１４，Ｓ１４２において、第１の認証情報→秘密鍵と読み替えた動作が、同名の構成要件によりそれぞれ実行される。

[0068] ＜ステップＳ２５１，Ｓ２４３＞

実施例１のステップＳ１５１，Ｓ１４３と同じ動作が、同名の構成要件によりそれぞれ実行される。

[0069] ＜ステップＳ２４４，Ｓ２５２＞

実施例１のステップＳ１４４，Ｓ１５２において、第２のトークン→外部システム２５（スマートロッカー）のＩＤ、第１の認証情報→秘密鍵と読み替えた動作が、同名の構成要件によりそれぞれ実行される。

[0070] ＜ステップＳ２３２３，Ｓ２５３＞

実施例１のステップＳ１３２３，Ｓ１５３と同じ動作が、同名の構成要件によりそれぞれ実行される。

[0071] ＜ステップＳ２３２４、Ｓ２５４＞

ステップＳ２３２４、Ｓ２５４については、子機２３２のＩＤ、外部システム２５（スマートロッカー）のＩＤ、秘密鍵を用いて、参考特許文献１に記載の方法で認証を実行することができる。

[0072] ＜ステップＳ２３２５，Ｓ２５５＞

実施例１のステップＳ１３２５，Ｓ１５５と同じ動作が、同名の構成要件によりそれぞれ実行される。本実施例では、ドローン編隊による荷物の配送をサービスの内容としているため、配送物の引渡、受取に該当する。

[0073] 実施例１、２の認証システム１、２によれば、管理対象の無人機や無人機のグループが膨大にある場合であっても、個体管理コストを低くすることができるため、これらの認証情報や権限を中央で管理することができる。また、無人機グループの配属変更を任意のタイミングで行うことができる。

実施例 3

[0074] 図１９に示すように、実施例１、２に登場した無人機（親機及び子機）は自律的に移動を行う無人機でなく、固定的に設置されたＩｏＴデバイス３３１、３３２に置き換えてもよい。同図に示すように、実施例３の認証システム３は、実施例１における無人機（親機、子機）をＩＯＴデバイス（親機３３１、子機３３２）に代替して構成されている。

[0075] ＜変形例＞

実施例１～３の認証システム１～３は、階層型ＩＤベース暗号に限らず、例えば失効機能付き階層型ＩＤベース暗号を含む、他の認証手段を用意する形態でも良い。例えば、公開鍵基盤を活用し、親機に中間ＣＡを配置するような構成でも良いし、親機が認証情報を発行可能な独自の認証方法によって実現されても良い。

[0076] ＜補記＞

本発明の装置は、例えば単一のハードウェアエンティティとして、キーボードなどが接続可能な入力部、液晶ディスプレイなどが接続可能な出力部、ハードウェアエンティティの外部に通信可能な通信装置（例えば通信ケーブル）が接続可能な通信部、ＣＰＵ（Central Processing Unit、キャッシュメモリやレジスタなどを備えていてもよい）、メモリであるＲＡＭやＲＯＭ、ハードディスクである外部記憶装置並びにこれらの入力部、出力部、通信部、ＣＰＵ、ＲＡＭ、ＲＯＭ、外部記憶装置の間のデータのやり取りが可能なように接続するバスを有している。また必要に応じて、ハードウェアエンティティに、ＣＤ－ＲＯＭなどの記録媒体を読み書きできる装置（ドライブ）などを設けることとしてもよい。このようなハードウェア資源を備えた物理的実体としては、汎用コンピュータなどがある。

[0077] ハードウェアエンティティの外部記憶装置には、上述の機能を実現するために必要となるプログラムおよびこのプログラムの処理において必要となるデータなどが記憶されている（外部記憶装置に限らず、例えばプログラムを読み出し専用記憶装置であるＲＯＭに記憶させておくこととしてもよい）。また、これらのプログラムの処理によって得られるデータなどは、ＲＡＭや外部記憶装置などに適宜に記憶される。

[0078] ハードウェアエンティティでは、外部記憶装置（あるいはＲＯＭなど）に記憶された各プログラムとこの各プログラムの処理に必要なデータが必要に応じてメモリに読み込まれて、適宜にＣＰＵで解釈実行・処理される。その結果、ＣＰＵが所定の機能（上記、…部、…手段などと表した各構成要件）

を実現する。

[0079] 本発明は上述の実施形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲で適宜変更が可能である。また、上記実施形態において説明した処理は、記載の順に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されるとしてもよい。

[0080] 既述のように、上記実施形態において説明したハードウェアエンティティ（本発明の装置）における処理機能をコンピュータによって実現する場合、ハードウェアエンティティが有すべき機能の処理内容はプログラムによって記述される。そして、このプログラムをコンピュータで実行することにより、上記ハードウェアエンティティにおける処理機能がコンピュータ上で実現される。

[0081] 上述の各種の処理は、図２０に示すコンピュータの記録部１００２０に、上記方法の各ステップを実行させるプログラムを読み込ませ、制御部１００１０、入力部１００３０、出力部１００４０などに動作させることで実施できる。

[0082] この処理内容を記述したプログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。コンピュータで読み取り可能な記録媒体としては、例えば、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリ等どのようなものでもよい。具体的には、例えば、磁気記録装置として、ハードディスク装置、フレキシブルディスク、磁気テープ等を、光ディスクとして、ＤＶＤ（Digital Versatile Disc）、ＤＶＤ－ＲＡＭ（Random Access Memory）、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory）、ＣＤ－Ｒ（Recordable）／ＲＷ（ReWritable）等を、光磁気記録媒体として、ＭＯ（Magneto-Optical disc）等を、半導体メモリとしてＥＥＰ－ＲＯＭ（Electrically Erasable and Programmable-Read Only Memory）等を用いることができる。

[0083] また、このプログラムの流通は、例えば、そのプログラムを記録したＤＶ

Ｄ、ＣＤ－ＲＯＭ等の可搬型記録媒体を販売、譲渡、貸与等することによって行う。さらに、このプログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータから他のコンピュータにそのプログラムを転送することにより、このプログラムを流通させる構成としてもよい。

[0084] このようなプログラムを実行するコンピュータは、例えば、まず、可搬型記録媒体に記録されたプログラムもしくはサーバコンピュータから転送されたプログラムを、一旦、自己の記憶装置に格納する。そして、処理の実行時、このコンピュータは、自己の記録媒体に格納されたプログラムを読み取り、読み取ったプログラムに従った処理を実行する。また、このプログラムの別の実行形態として、コンピュータが可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することとしてもよく、さらに、このコンピュータにサーバコンピュータからプログラムが転送されるたびに、逐次、受け取ったプログラムに従った処理を実行することとしてもよい。また、サーバコンピュータから、このコンピュータへのプログラムの転送は行わず、その実行指示と結果取得のみによって処理機能を実現する、いわゆるＡＳＰ（Application Service Provider）型のサービスによって、上述の処理を実行する構成としてもよい。なお、本形態におけるプログラムには、電子計算機による処理の用に供する情報であってプログラムに準ずるもの（コンピュータに対する直接の指令ではないがコンピュータの処理を規定する性質を有するデータ等）を含むものとする。

[0085] また、この形態では、コンピュータ上で所定のプログラムを実行させることにより、ハードウェアエンティティを構成することとしたが、これらの処理内容の少なくとも一部をハードウェア的に実現することとしてもよい。

請求の範囲

[請求項1] 認証局と、中央制御システムと、親機である無人機と子機である無人機を含むグループと、管理システムと、外部システムを含む認証システムであって、

前記中央制御システムは、

前記認証局から受信した第１の認証情報を前記親機に送信する第１認証情報送信部を含み、

前記親機は、

同じグループに属する前記子機との認証を実行する認証部と、

認証された前記子機に有効期限付きの第１のトークンと前記第１の認証情報を含む第２の認証情報を送信する第２認証情報送信部を含み、

前記管理システムは、

前記外部システムとの認証を実行する認証部と、

認証された前記外部システムに第２のトークンと前記認証局から受信した前記第１の認証情報を含む第３の認証情報を送信する第３認証情報送信部を含み、

前記子機と前記外部システムは、

前記第２の認証情報と前記第３の認証情報に基づいて認証を実行する認証部を含む

認証システム。

[請求項2] 請求項１に記載の認証システムであって、

前記親機の前記認証部は、

近接通信を用いて前記子機との認証を実行する

認証システム。

[請求項3] 請求項１に記載の認証システムであって、

前記親機の前記第２認証情報送信部は、

近接通信を用いて前記子機に前記第２の認証情報を送信する

認証システム。

[請求項4] 請求項２または３に記載の認証システムであって、

前記無人機はドローンであり、

前記外部システムはスマートロッカーである

認証システム。

[請求項5] 請求項１から３の何れかに記載の認証システムであって、

前記第１の認証情報は秘密鍵であり、

前記第１のトークンは、前記子機のＩＤであり、

前記第２のトークンは、前記外部システムのＩＤであり、

前記子機と前記外部システムは、

前記子機のＩＤと、前記外部システムのＩＤと、前記秘密鍵に基づいて、ＩＤベース暗号方式により認証を実行する

認証システム。

[請求項6] 認証局と、中央制御システムと、親機である無人機と、子機である無人機と、管理システムと、外部システムが実行する認証方法であって、

前記中央制御システムは、

前記認証局から受信した第１の認証情報を前記親機に送信するステップを実行し、

前記親機は、

同じグループに属する前記子機との認証を実行するステップと、

認証された前記子機に有効期限付きの第１のトークンと前記第１の認証情報を含む第２の認証情報を送信するステップを実行し、

前記管理システムは、

前記外部システムとの認証を実行するステップと、

認証された前記外部システムに第２のトークンと前記認証局から受信した前記第１の認証情報を含む第３の認証情報を送信するステップを実行し、

前記子機と前記外部システムは、

前記第２の認証情報と前記第３の認証情報に基づいて認証を実行するステップを実行する

認証方法。

[請求項7] コンピュータを請求項１に記載の中央制御システムとして機能させるプログラム。

[請求項8] 無人機を請求項１に記載の親機、または子機として機能させるプログラム。

[図1]

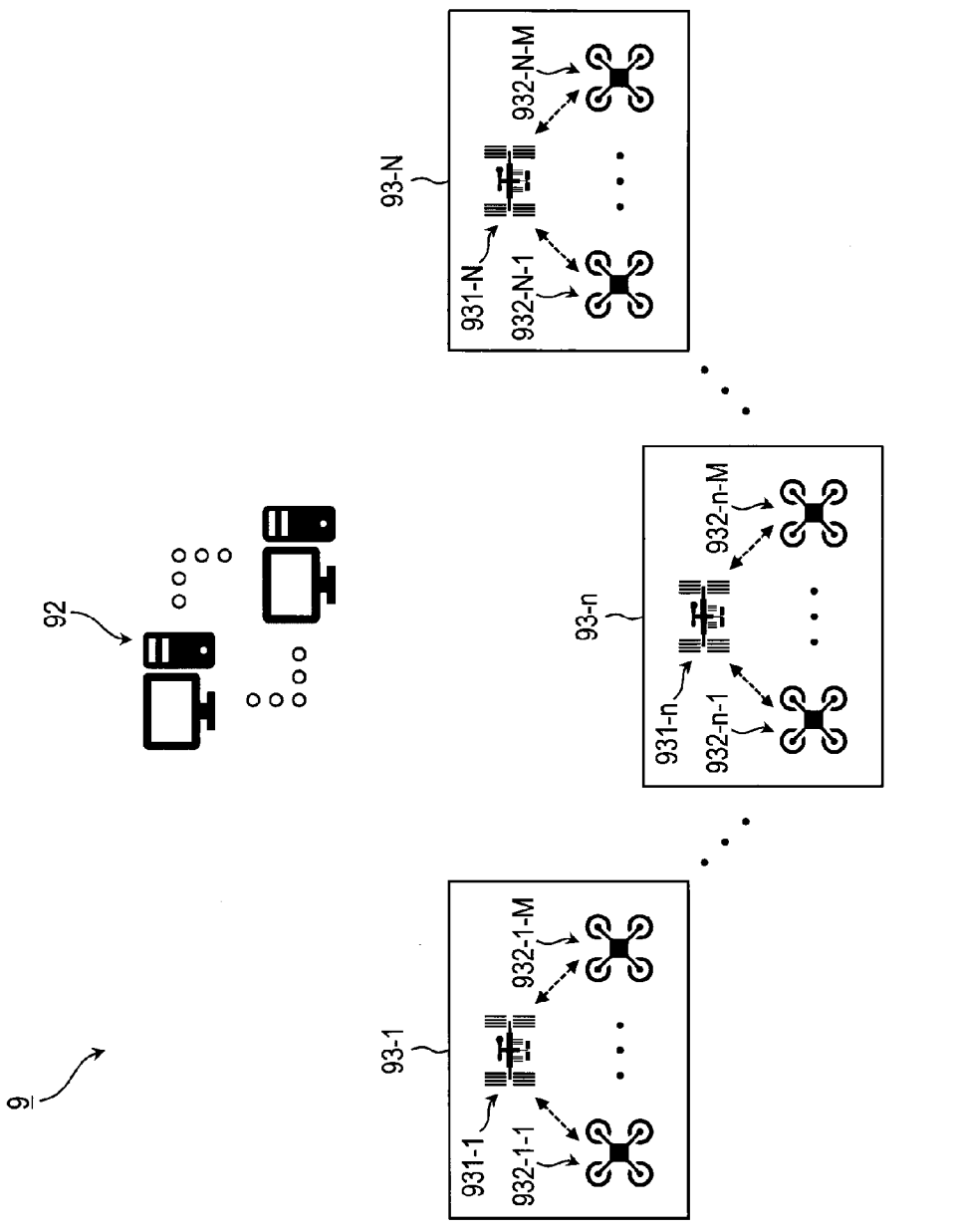

9
92
93-1
931-1
932-1-1
932-1-M
93-n
931-n
932-n-1
932-n-M
93-N
931-N
932-N-1
932-N-M

図1

[図2]

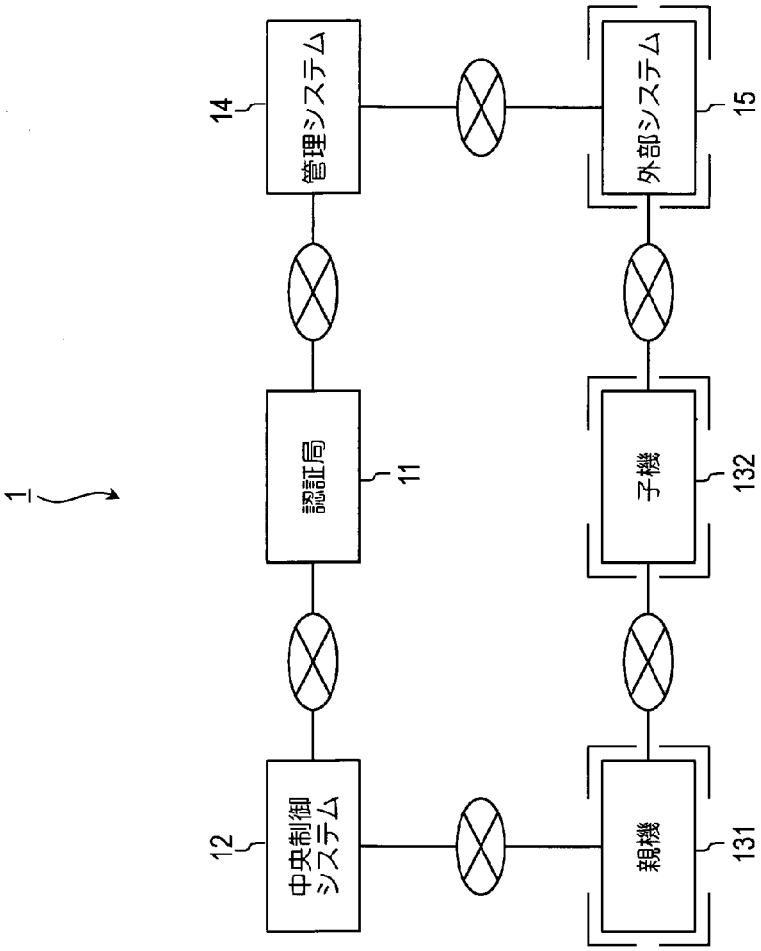


図2

[図3]

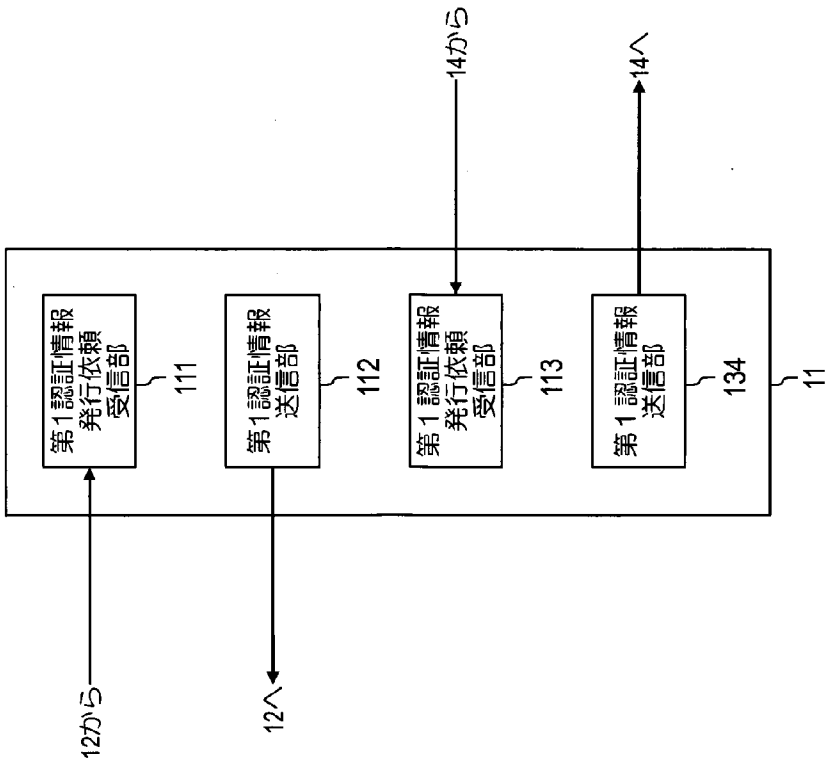
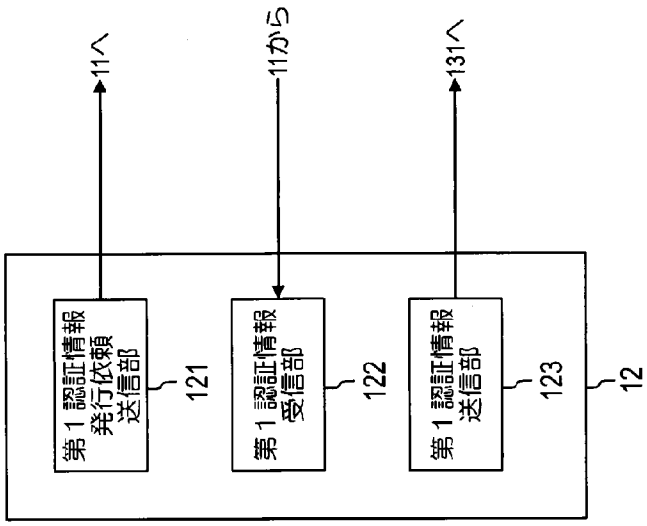

第１認証情報発行依頼受信部
111
第１認証情報送信部
112
第１認証情報発行依頼受信部
113
第１認証情報送信部
134
11
12から
12へ
14から
14へ

図3

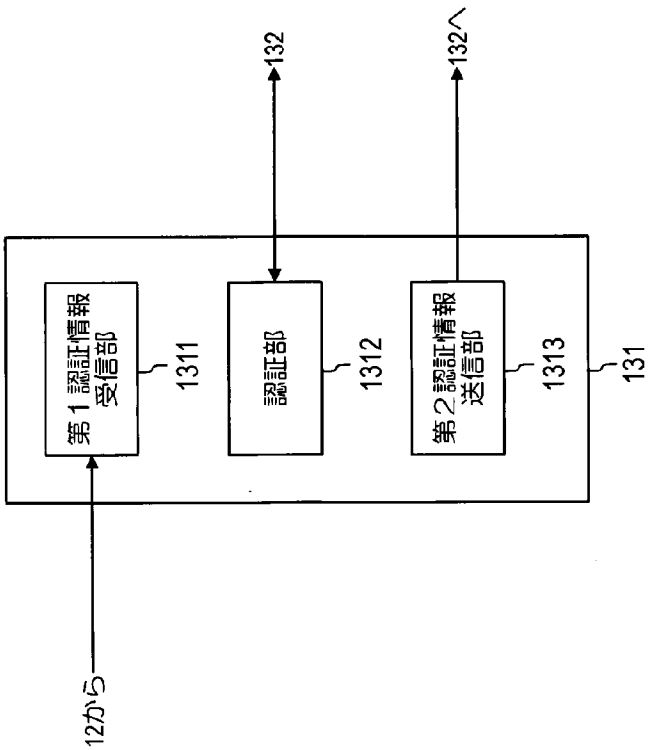
[図4]

図4


11へ
11から
131へ
第1認証情報
発行依頼
送信部
121
第1認証情報
受信部
122
第1認証情報
送信部
123
12

[図5]

図5



[図6]

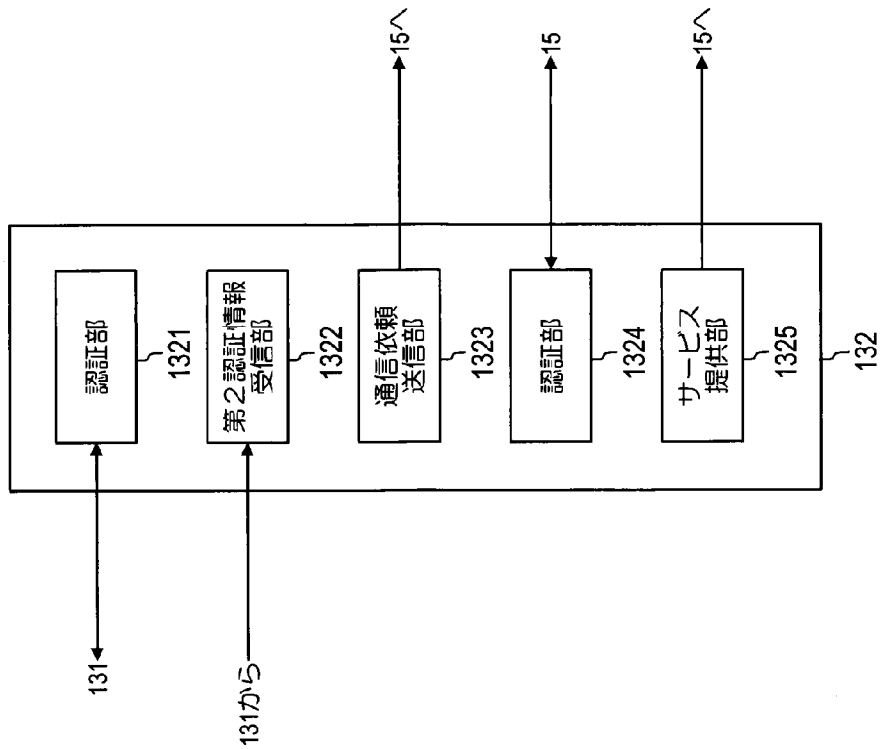

認証部
1321
第２認証情報受信部
1322
通信依頼送信部
1323
認証部
1324
サービス提供部
1325
132
131
131から
15へ
15
15へ

図6

[図7]

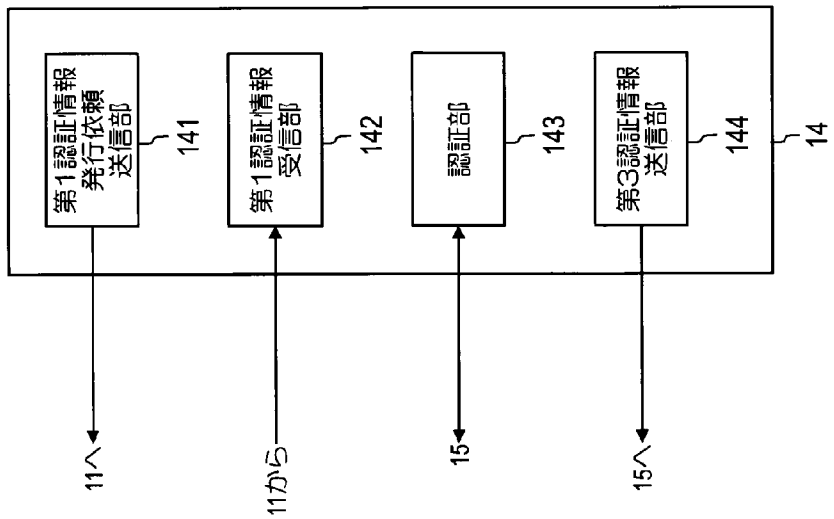

第1認証情報
発行依頼
送信部
141
第1認証情報
受信部
142
認証部
143
第3認証情報
送信部
144
14
11へ
11から
15
15へ

図7

[図8]

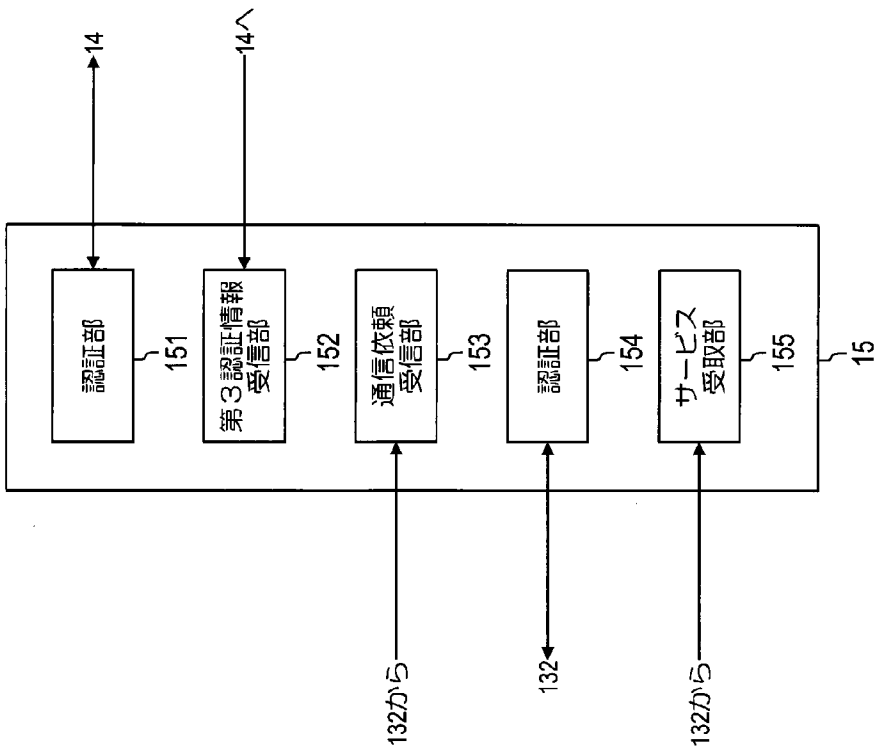

14
14へ
認証部
151
第3認証情報受信部
152
通信依頼受信部
153
認証部
154
サービス受取部
155
15
132から
132
132から

図8

[図9]

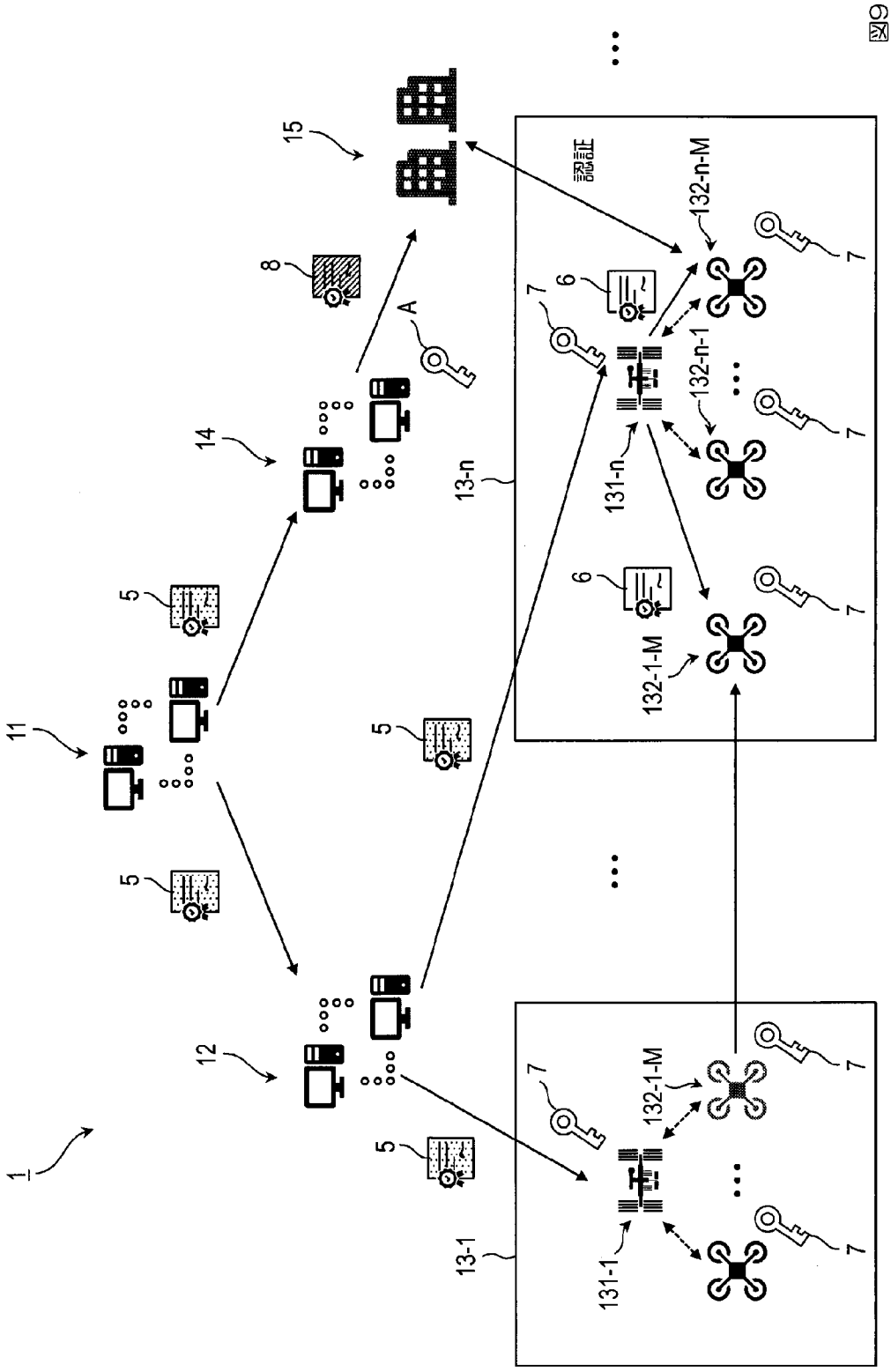


図9

[図10]

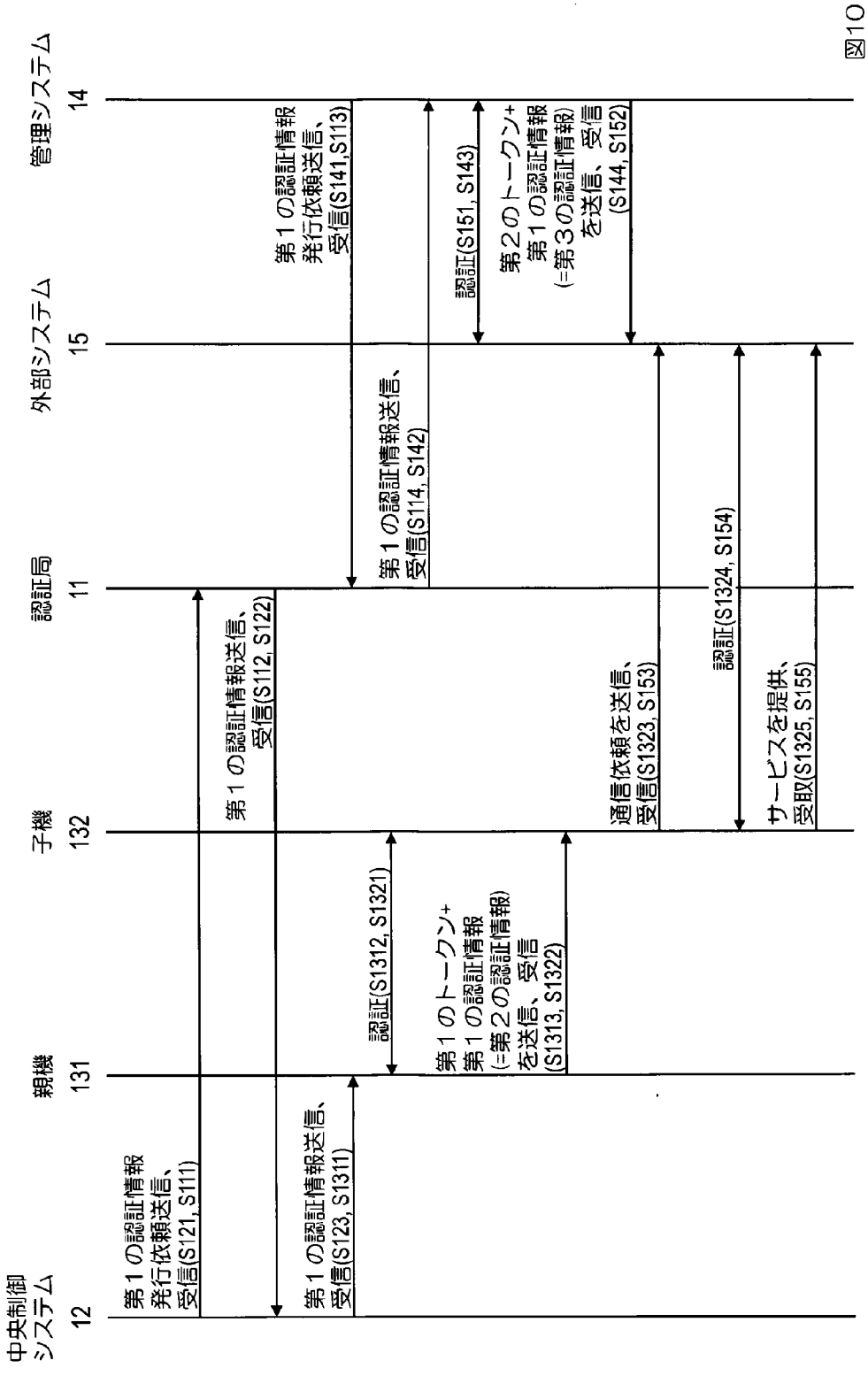

中央制御システム 12
親機 131
子機 132
認証局 11
外部システム 15
管理システム 14
第１の認証情報発行依頼送信、受信(S121, S111)
第１の認証情報送信、受信(S123, S1311)
第１の認証情報送信、受信(S112, S122)
認証(S1312, S1321)
第１のトークン+第１の認証情報(=第２の認証情報)を送信、受信(S1313, S1322)
第１の認証情報送信、受信(S114, S142)
第１の認証情報発行依頼送信、受信(S141,S113)
認証(S151, S143)
第２のトークン+第１の認証情報(=第３の認証情報)を送信、受信(S144, S152)
通信依頼を送信、受信(S1323, S153)
認証(S1324, S154)
サービスを提供、受取(S1325, S155)

図10

[図11]

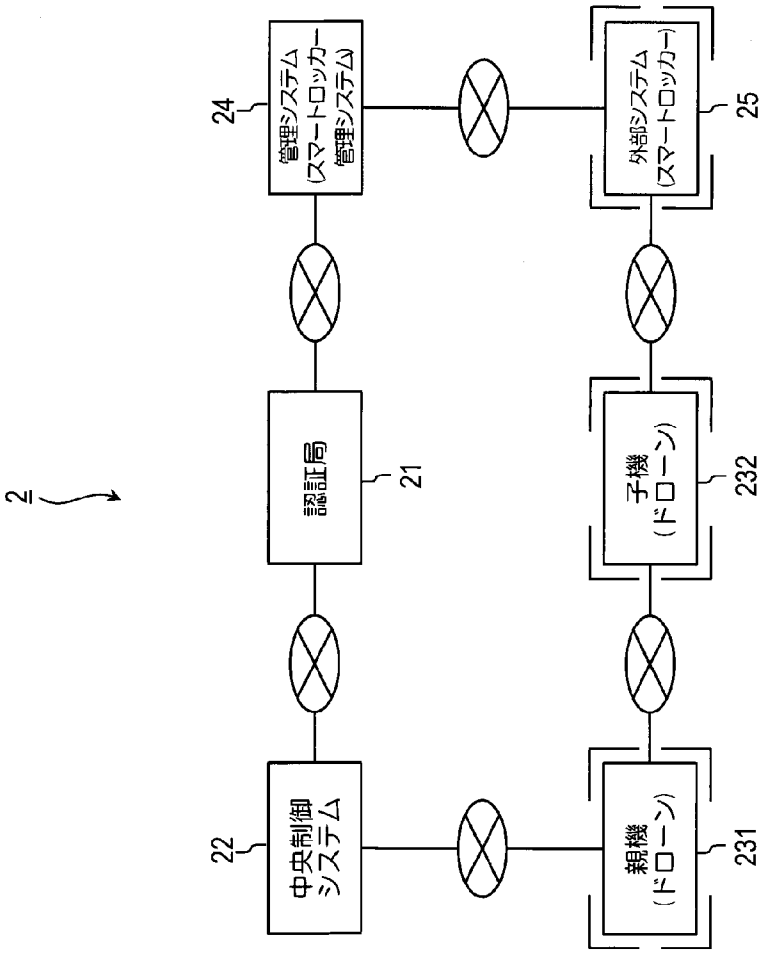

2
認証局
21
中央制御システム
22
管理システム（スマートロッカー管理システム）
24
外部システム（スマートロッカー）
25
親機（ドローン）
231
子機（ドローン）
232

図11

[図12]

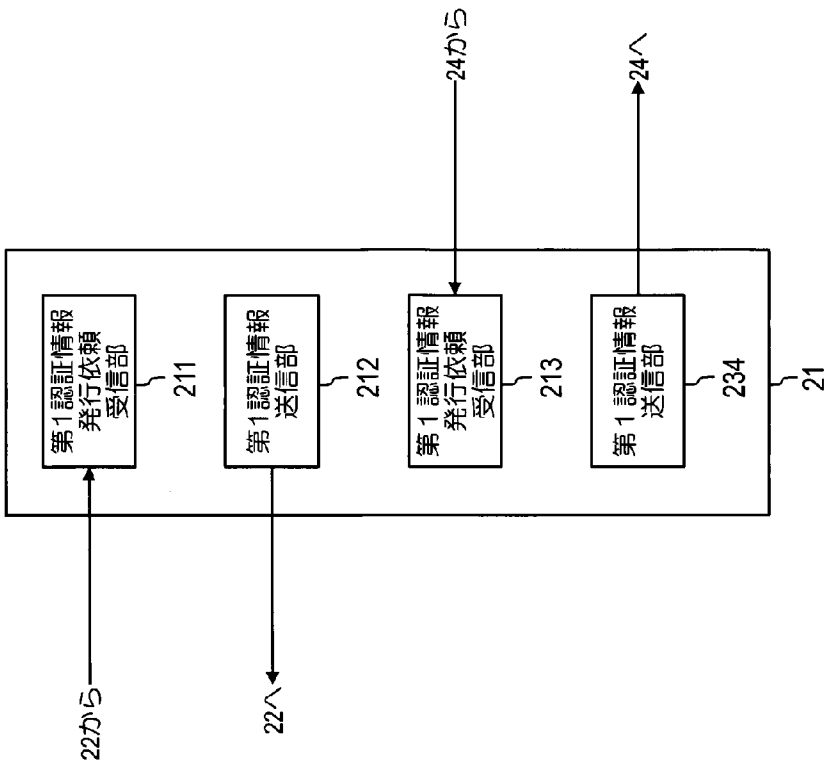
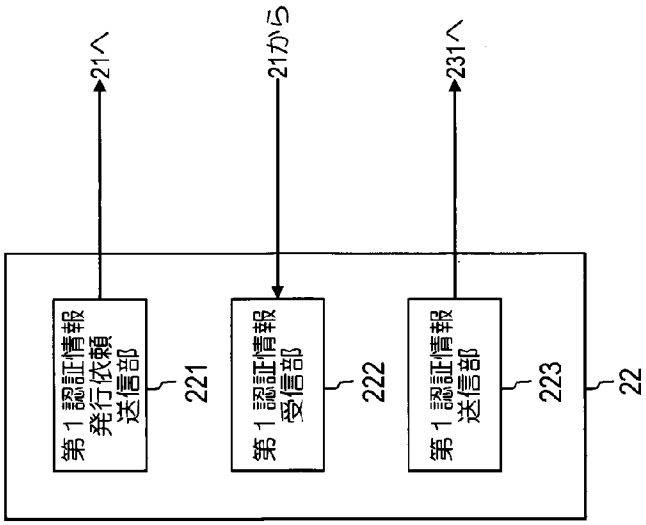

第1認証情報発行依頼受信部
211
第1認証情報送信部
212
第1認証情報発行依頼受信部
213
第1認証情報送信部
234
21
22から
22へ
24から
24へ

図12

[図13]

図13


21へ
21から
231へ
第1認証情報
発行依頼
送信部
221
第1認証情報
受信部
222
第1認証情報
送信部
223
22

[図14]

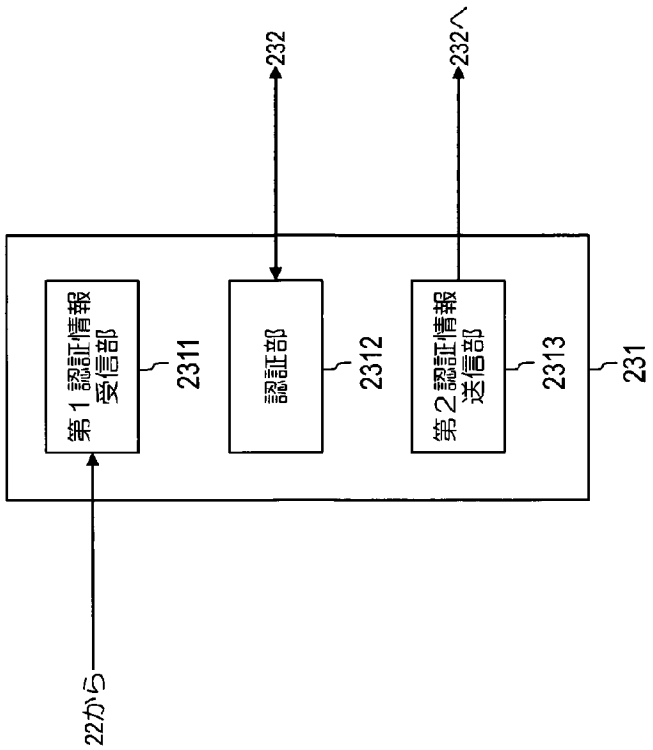


図１４

[図15]

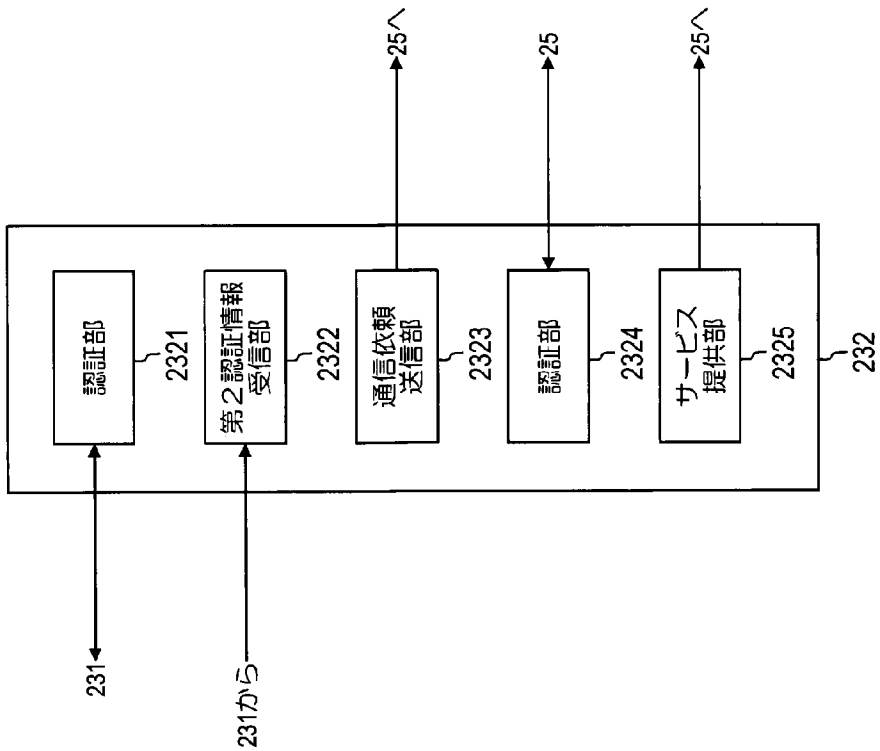

25へ
25
25へ
認証部
2321
第２認証情報受信部
2322
通信依頼送信部
2323
認証部
2324
サービス提供部
2325
232
231
231から

図15

[図16]

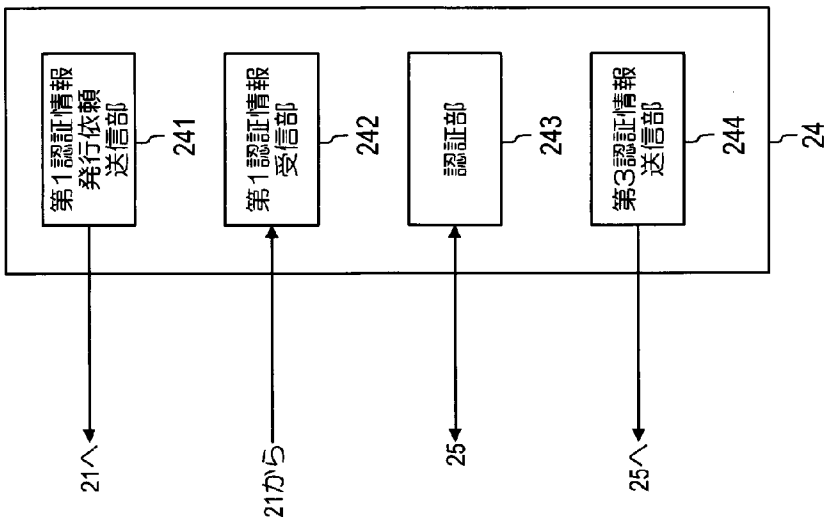

第1認証情報発行依頼送信部
241
第1認証情報受信部
242
認証部
243
第3認証情報送信部
244
24
21へ
21から
25
25へ

図16

[図17]

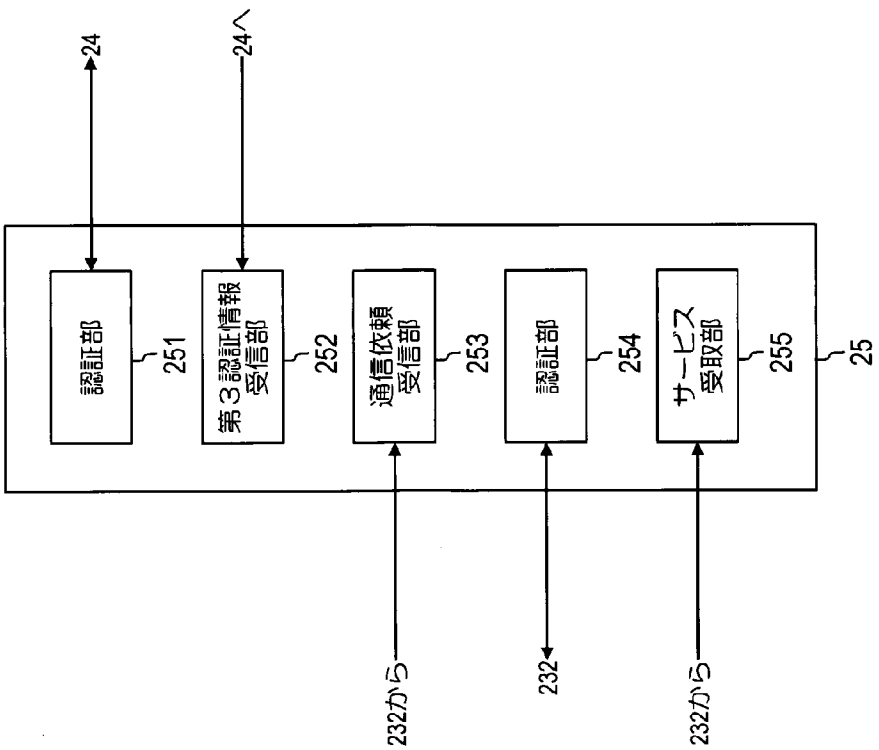

24
24へ
認証部
251
第３認証情報受信部
252
通信依頼受信部
253
認証部
254
サービス受取部
255
25
232から
232
232から

図17

[図18]

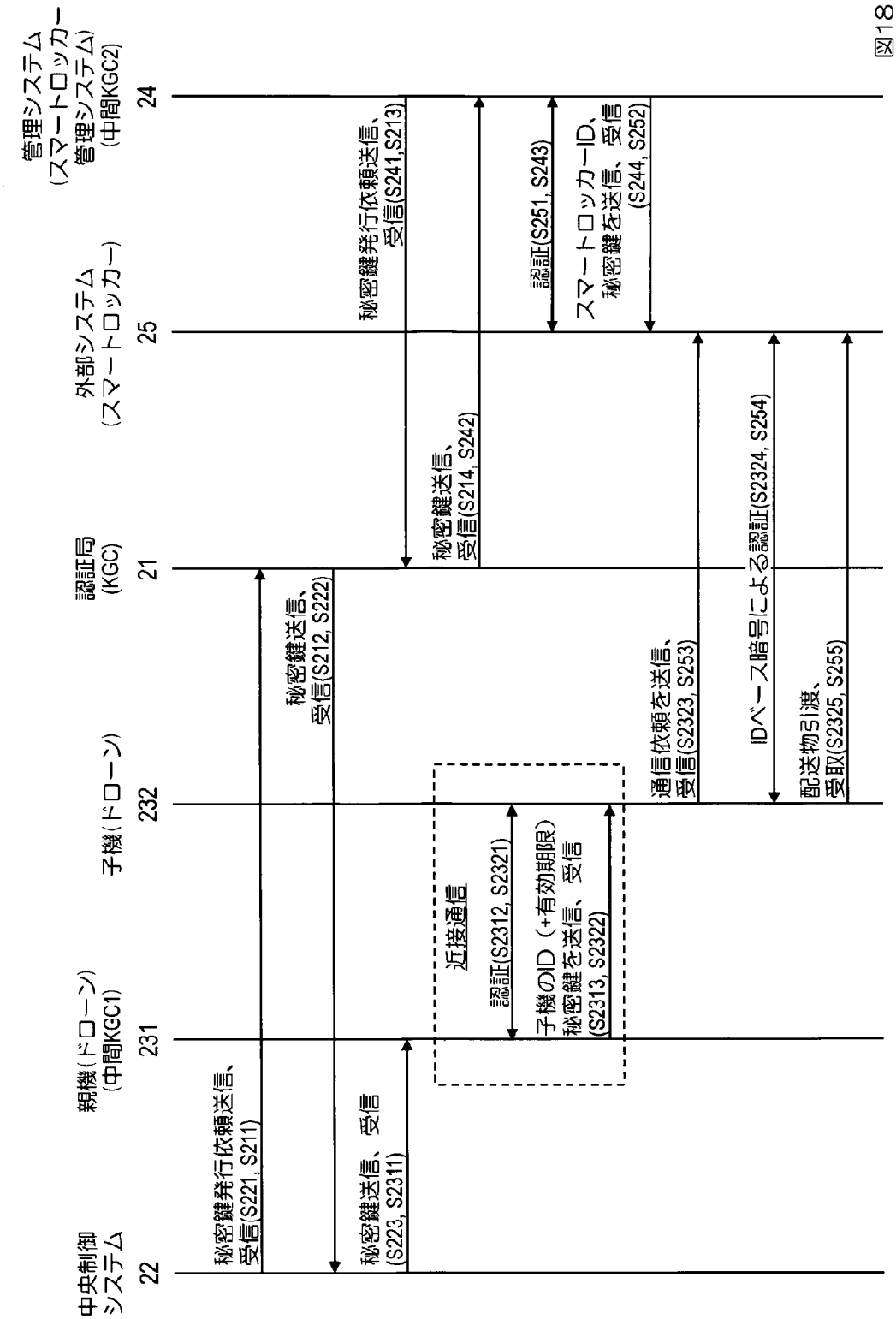

中央制御システム
22
親機(ドローン)(中間KGC1)
231
子機(ドローン)
232
認証局(KGC)
21
外部システム(スマートロッカー)
25
管理システム(スマートロッカー管理システム)(中間KGC2)
24
秘密鍵発行依頼送信、受信(S221, S211)
秘密鍵送信、受信(S223, S2311)
秘密鍵送信、受信(S212, S222)
近接通信
認証(S2312, S2321)
子機のID（+有効期限）秘密鍵を送信、受信(S2313, S2322)
秘密鍵送信、受信(S214, S242)
秘密鍵発行依頼送信、受信(S241,S213)
認証(S251, S243)
スマートロッカーID、秘密鍵を送信、受信(S244, S252)
通信依頼を送信、受信(S2323, S253)
IDベース暗号による認証(S2324, S254)
配送物引渡、受取(S2325, S255)

図18

[図19]

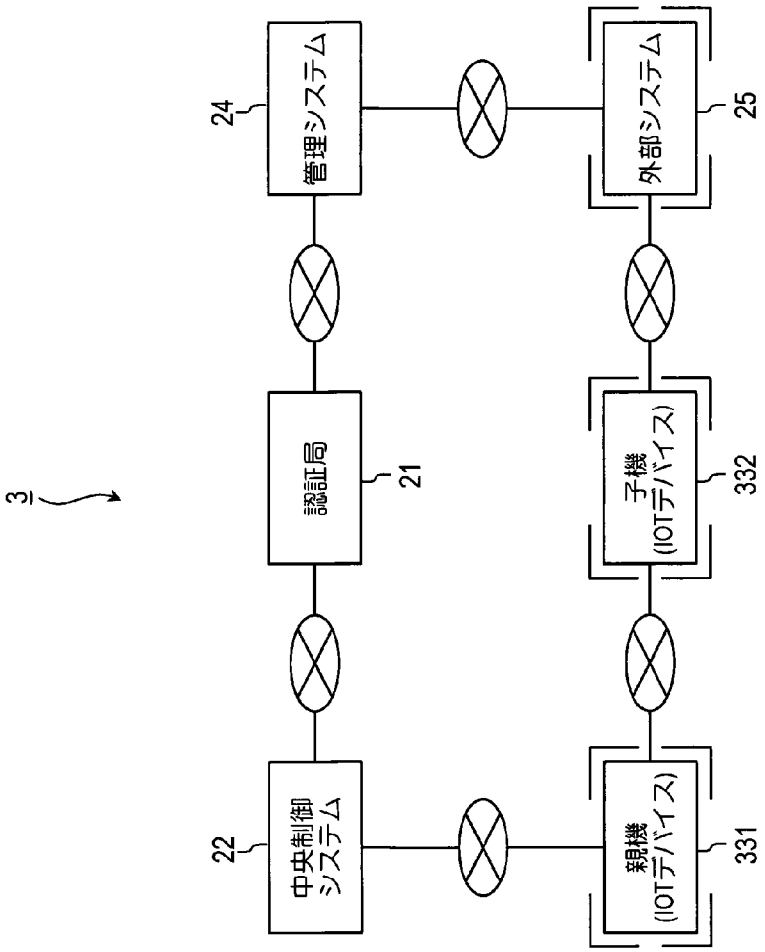
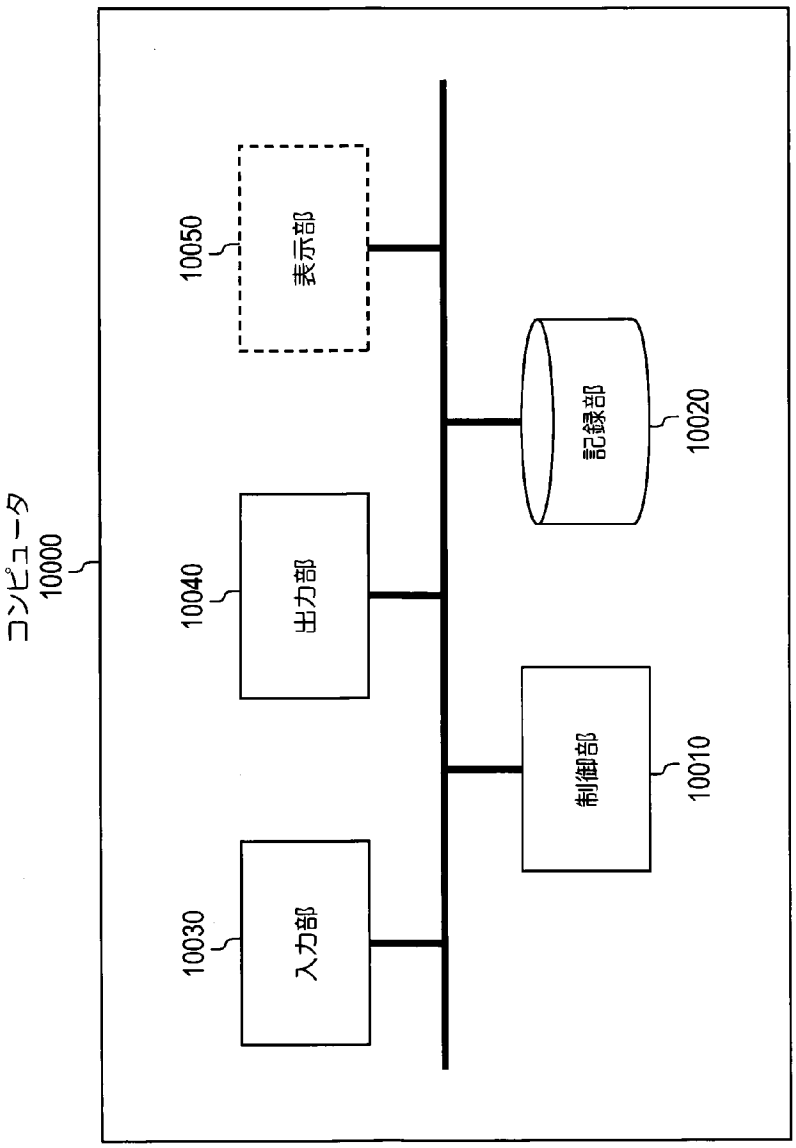

3
認証局
21
中央制御システム
22
管理システム
24
外部システム
25
親機(IOTデバイス)
331
子機(IOTデバイス)
332

図19

[図20]

図20


コンピュータ
10000
表示部
10050
記録部
10020
出力部
10040
制御部
10010
入力部
10030

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2022/026598

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/44(2013.01)i
FI: G06F21/44

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)

G06F21/44

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 1971-2022
Registered utility model specifications of Japan 1996-2022
Published registered utility model applications of Japan 1994-2022

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.
A	JP 2018-74253 A (NATIONAL INST. OF INFORMATION & COMMUNICATIONS TECHNOLOGY) 10 May 2018 (2018-05-10) entire text, all drawings	1-8
A	US 2018/0279105 A1 (AERYON LABS INC.) 27 September 2018 (2018-09-27) entire text, all drawings	1-8
A	US 2020/0007384 A1 (INTEL CORPORATION) 02 January 2020 (2020-01-02) entire text, all drawings	1-8

☐ 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
25 August 2022	**06 September 2022**
Name and mailing address of the ISA/JP **Japan Patent Office (ISA/JP)** **3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915** **Japan**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2022/026598

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP 2018-74253 A	10 May 2018	(Family: none)	
US 2018/0279105 A1	27 September 2018	WO 2016/026023 A1 entire text, all drawings	
US 2020/0007384 A1	02 January 2020	WO 2018/004681 A1 entire text, all drawings EP 3479626 A1	

国際調査報告

国際出願番号
PCT/JP2022/026598

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

G06F 21/44(2013.01)i
FI: G06F21/44

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））

G06F21/44

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	１９７１－２０２２年
日本国実用新案登録公報	１９９６－２０２２年
日本国登録実用新案公報	１９９４－２０２２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
A	JP 2018-74253 A (国立研究開発法人情報通信研究機構) 10.05.2018 (2018-05-10) 全文、全図	1-8
A	US 2018/0279105 A1 (AERYON LABS INC.) 27.09.2018 (2018-09-27) 全文、全図	1-8
A	US 2020/0007384 A1 (INTEL CORPORATION) 02.01.2020 (2020-01-02) 全文、全図	1-8

☐ 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
25.08.2022	06.09.2022

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）
松平　英 5S 3146

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/JP2022/026598

引用文献	公表日	パテントファミリー文献	公表日
JP 2018-74253 A	10.05.2018	（ファミリーなし）	
US 2018/0279105 A1	27.09.2018	WO 2016/026023 A1 全文、全図	
US 2020/0007384 A1	02.01.2020	WO 2018/004681 A1 全文、全図 EP 3479626 A1	