(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
2020年3月5日(05.03.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/044624 A1

(51) 国際特許分類:
H04L 9/32 (2006.01)　*G06F 21/44* (2013.01)

(21) 国際出願番号：　PCT/JP2019/009533

(22) 国際出願日：　2019年3月8日(08.03.2019)

(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 2018-159771　2018年8月28日(28.08.2018)　JP

(71) 出願人: アルプスアルパイン株式会社(**ALPS ALPINE CO., LTD.**) [JP/JP]; 〒1458501 東京都大田区雪谷大塚町１番７号 Tokyo (JP).

(72) 発明者: 村田 眞司(**MURATA, Shinji**); 〒1458501 東京都大田区雪谷大塚町１番７号 アルプスアルパイン株式会社内 Tokyo (JP). 桝田屋 秀樹(**MASUDAYA, Hideki**); 〒1458501 東京都大田区雪谷大塚町１番７号 アルプスアルパイン株式会社内 Tokyo (JP).

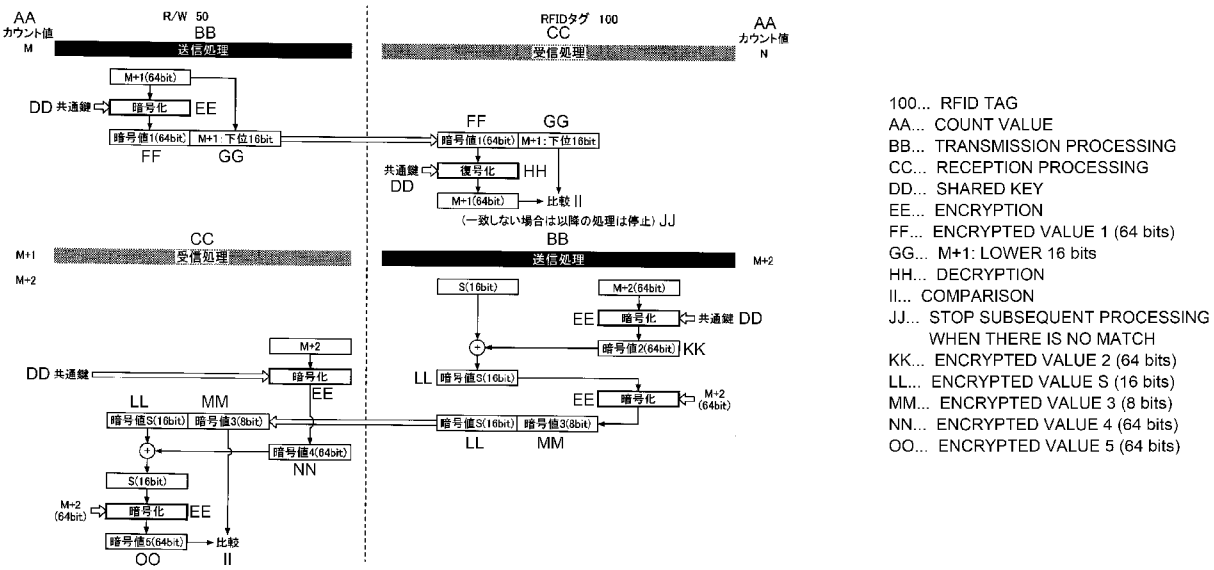
(74) 代理人: 伊東 忠重，外(**ITOH, Tadashige** et al.); 〒1000005 東京都千代田区丸の内二丁目１番１号 丸の内ＭＹ ＰＬＡＺＡ（明治安田生命ビル）１６階 Tokyo (JP).

(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, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,

(54) **Title:** MUTUAL AUTHENTICATION METHOD AND COMMUNICATION SYSTEM

(54) 発明の名称： 相互認証方法及び通信システム

[図2]



(57) **Abstract:** Provided are a mutual authentication method and a communication system capable of performing authentication within a short time. This mutual authentication method is used for a communication system including a first communication device and a second communication device having a shared key, where the first communication device and the second communication device each hold a first count value and a second count value representing the number of communications. The first communication device generates a first encrypted value by encrypting the first count value with the shared key, and transmits the first encrypted value and a first numerical value including at least a portion of the first count value to the second communication device. When the second communication device receives the first encrypted

WO 2020/044624 A1

［続葉有］

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))

value and the first numerical value, the second communication device decrypts the first encrypted value with the shared key, determines whether there is a match between a first decrypted value obtained through the decryption and the first numerical value, and, when there is a match, determines that the first communication device is authenticated if the first decrypted value is equal to the second count value or is more advanced than the second count value.

(57) 要約:認証を短時間で行うことができる相互認証方法及び通信システムを提供する。相互認証方法は、共通鍵を有する第1通信機と第2通信機とを含み、前記第1通信機及び前記第2通信機が通信回数を表す第1カウント値及び第2カウント値をそれぞれ保持する通信システムにおける相互認証方法であって、前記第1通信機は、前記共通鍵で前記第1カウント値を暗号化して第1暗号値を生成し、前記第1暗号値と、前記第1カウント値の少なくとも一部分を含む第1数値とを前記第2通信機に送信し、前記第2通信機は、前記第1暗号値及び前記第1数値を受信すると、前記共通鍵で前記第1暗号値を復号化し、前記復号化で得る第1復号値と前記第1数値との一致性を判定し、前記一致性が成立する場合に、前記第1復号値が前記第2カウント値と等しいか、又は、前記第2カウント値よりも進んでいれば、第1通信機の認証が成立したと判定する。

明　細　書

発明の名称 ： 相互認証方法及び通信システム

技術分野

[0001] 本発明は、相互認証方法及び通信システムに関する。

背景技術

[0002] 従来より、通信路で接続された第１機器と第２機器とからなる通信システムにおいて相手が正当な機器であることを認証するための機器認証システムであって、前記第１機器は、前記第２機器の正当性を検証するための複数の検証関数を予め記憶している検証関数記憶手段と、第１チャレンジデータを生成し第２機器に送信する第１チャレンジデータ送信手段と、前記第１チャレンジデータに対応する第１レスポンスデータを前記第２機器から受信する第１レスポンスデータ受信手段と、前記第１チャレンジデータと前記第１レスポンスデータとが前記複数の検証関数のいずれかによって関連づけられるか否かを検証する第１検証手段と、前記第１検証手段が肯定的に検証した場合に前記第２機器の正当性を認証する第１認証手段とを備え、第２機器は、前記複数の検証関数それぞれに対応する複数の証明関数であって、自己の正当性を証明するためのものを予め記憶している証明関数記憶手段と、前記第１機器が送信した第１チャレンジデータを受信する第１チャレンジデータ受信手段と、前記複数の証明関数から１つを選択する証明関数選択手段と、前記証明関数選択手段が選択した証明関数に基づいて、前記第１チャレンジデータから第１レスポンスデータを生成し第１機器に送信する第１レスポンスデータ送信手段とを備えることを特徴とする機器認証システムがある。第２機器が第２機器の正当性を検証するには、上述とは逆の動作を行う（例えば、特許文献１参照）。

先行技術文献

特許文献

[0003] 特許文献1：特開平１０－２２４３４３号公報

発明の概要

発明が解決しようとする課題

[0004] ところで、従来の機器認証システムにおける正当性の検証方法(認証方法)では、第１機器と第２機器が互いに認証するには二往復のデータ通信が必要であるため、認証にかかる通信時間が長いという課題がある。

[0005] そこで、認証を短時間で行うことができる相互認証方法及び通信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

[0006] 本発明の実施の形態の相互認証方法は、共通鍵を有する第１通信機と第２通信機とを含み、前記第１通信機及び前記第２通信機が通信回数を表す第１カウント値及び第２カウント値をそれぞれ保持する通信システムにおける相互認証方法であって、前記第１通信機は、前記共通鍵で前記第１カウント値を暗号化して第１暗号値を生成し、前記第１暗号値と、前記第１カウント値の少なくとも一部分を含む第１数値とを前記第２通信機に送信し、前記第２通信機は、前記第１暗号値及び前記第１数値を受信すると、前記共通鍵で前記第１暗号値を復号化し、前記復号化で得る第１復号値と前記第１数値との一致性を判定し、前記一致性が成立する場合に、前記第１復号値が前記第２カウント値と等しいか、又は、前記第２カウント値よりも進んでいれば、第１通信機の認証が成立したと判定する。

発明の効果

[0007] 認証を短時間で行うことができる相互認証方法及び通信システムを提供することができる。

図面の簡単な説明

[0008] [図1]相互認証方法を実行する通信システム１０を示す図である。

[図2]Ｒ／Ｗ５０及びＲＦＩＤタグ１００が行う認証処理を示すタスク図である。

[図3]Ｒ／Ｗ５０が実行する相互認証処理を表すフローチャートを示す図であ

る。

[図4]ＲＦＩＤタグ１００が実行する相互認証処理を表すフローチャートを示す図である。

[図5]変形例におけるＲ／Ｗ５０及びＲＦＩＤタグ１００が行う認証処理を示すタスク図である。

[図6]変形例におけるＲ／Ｗ５０及びＲＦＩＤタグ１００が行う認証処理を示すタスク図である。

[図7]変形例におけるＲ／Ｗ５０及びＲＦＩＤタグ１００が行う認証処理を示すタスク図である。

発明を実施するための形態

[0009] 以下、本発明の相互認証方法及び通信システムを適用した実施の形態について説明する。

[0010] ＜実施の形態＞

図１は、相互認証方法を実行する通信システム１０を示す図である。通信システム１０は、Ｒ／Ｗ（リーダライタ）５０とＲＦＩＤタグ１００を含む。Ｒ／Ｗ５０は、第１通信機の一例であり、ＲＦＩＤタグ１００は、第２通信機の一例である。ＲＦＩＤタグ１００には、センサ３０が接続されている。

[0011] 以下では、Ｒ／Ｗ５０とＲＦＩＤタグ１００が１個ずつ存在する形態について説明するが、１個のＲ／Ｗ５０が複数のＲＦＩＤタグ１００と通信を行う形態であってよい。

[0012] また、一例として、センサ３０が応力センサである場合には、ＲＦＩＤタグ１００は、橋梁や斜面等に設置され、センサ３０が検出する応力を表すデータを暗号化してＲ／Ｗ５０に送信する。Ｒ／Ｗ５０は、センサ３０の検出値を取得することができる。なお、このような用途は一例であり、様々な種類のセンサをセンサ３０として用いることにより、ＲＦＩＤタグ１００を介してＲ／Ｗ５０で様々な検出値を取得することができる。

[0013] Ｒ／Ｗ５０は、制御装置６０、アンテナ７０、及びメモリ８０を有する。

[0014] 制御装置６０は、ＣＰＵ(Central Processing Unit)、ＲＡＭ(Random Access Memory)、ＲＯＭ(Read Only Memory)、ＨＤＤ(Hard Disk Drive)、入出力インターフェース、及び内部バス等を含むコンピュータによって実現される。

[0015] 制御装置６０は、主制御部６１、暗号部６２、認証部６４、論理演算部６５、及び通信部６６を有する。制御部６１、暗号部６２、認証部６４、論理演算部６５、及び通信部６６は、制御装置６０が実行するプログラムの機能（ファンクション）を機能ブロックとして示したものである。また、メモリ８０は、制御装置６０のメモリを機能的に表したものである。

[0016] 主制御部６１は、制御装置６０の処理を統括する制御部であり、暗号部６２、認証部６４、論理演算部６５、及び通信部６６が行う処理以外の処理を実行する。主制御部６１は、例えば、カウンタの機能を有し、Ｒ／Ｗ５０が通信を行う度に、通信回数を表すカウント値をインクリメントする。また、主制御部６１は、ＲＦＩＤタグ１００にカウント値や暗号等のデータを送信する処理を通信部６６に行わせる。また、主制御部６１は、ＲＦＩＤタグ１００からカウント値や暗号等のデータを受信する処理を通信部６６に行わせ、受信したデータを暗号部６２に伝送する。主制御部６１がカウントするカウント値は、第１カウント値の一例である。

[0017] 暗号部６２は、ＲＦＩＤタグ１００に送信するデータ等を暗号化する。暗号部６２は、一例として、Present 80 Encryption によるデータの暗号化処理を行う。Present 80 Encryptionは、共通鍵を使った暗号化手法である。

[0018] 認証部６４は、ＲＦＩＤタグ１００から受信する暗号やカウント値等に基づいて、ＲＦＩＤタグ１００の認証処理を行う。認証処理の詳細については、図２を用いて後述する。

[0019] 論理演算部６５は、ＲＦＩＤタグ１００から受信する暗号値と、暗号部６２が生成する暗号値との排他的論理和（ＥＸＯＲ）を演算する。この処理の詳細については図２を用いて後述する。

[0020] 通信部６６は、ＲＦＩＤタグ１００との通信用のアンテナ７０が接続され

ている。通信部６６は、主制御部６１からの指令に従って、ＲＦＩＤタグ１００にデータを送信する処理と、ＲＦＩＤタグ１００からデータを受信する処理とを行う。

[0021] アンテナ７０は、ＲＦＩＤタグ１００と無線通信を行えるアンテナであればよい。アンテナ７０は、通信部６６に接続されており、ＲＦＩＤタグ１００に送信するデータ等を含む信号を放射し、ＲＦＩＤタグ１００から返信されるデータ等を含む信号を受信する。

[0022] メモリ８０は、Ｒ／Ｗ５０が認証処理を行うために必要なプログラムやデータ等を格納する。また、メモリ８０は、主制御部６１がカウントするカウント値を一時的に保持する。また、メモリ８０は、Ｒ／Ｗ５０及びＲＦＩＤタグ１００が暗号化や複合化等に用いる共通鍵を格納する。

[0023] ＲＦＩＤタグ１００は、制御装置１１０、アンテナ１２０、及びメモリ１３０を有する。ＲＦＩＤタグ１００は、一例として、Ｒ／Ｗ５０から送信される信号をアンテナ１２０で受信すると、受信した電力で作動し、演算処理等を行って、Ｒ／Ｗ５０にデータを送信（返信）する。

[0024] 制御装置１１０は、ＩＣ(Integrated Circuit)チップによって実現される。

[0025] 制御装置１１０は、主制御部１１１、暗号部１１２、復号部１１３、認証部１１４、論理演算部１１５、及び通信部１１６を有する。主制御部１１１、暗号部１１２、復号部１１３、認証部１１４、論理演算部１１５、及び通信部１１６は、制御装置１１０が実行するプログラムの機能（ファンクション）を機能ブロックとして示したものである。また、メモリ１３０は、制御装置１１０のメモリを機能的に表したものである。

[0026] 主制御部１１１は、制御装置１１０の処理を統括する制御部であり、暗号部１１２、復号部１１３、認証部１１４、論理演算部１１５、及び通信部１１６が行う処理以外の処理を実行する。主制御部１１１は、例えば、カウンタの機能を有し、ＲＦＩＤタグ１００が通信を行う度に、通信回数を表すカウント値をインクリメントする。また、主制御部１１１は、Ｒ／Ｗ５０にカ

ウント値や暗号等のデータを送信する処理を通信部１１６に行わせる。また、主制御部１１１は、Ｒ／Ｗ５０からカウント値や暗号等のデータを受信する処理を通信部１１６に行わせ、受信したデータを暗号部１１２、復号部１１３に伝送する。主制御部１１１がカウントするカウント値は、第１カウント値の一例である。

[0027] 暗号部１１２は、Ｒ／Ｗ５０に送信するデータ等を暗号化する。暗号部１１２は、一例として、Present 80 Encryption によるデータの暗号化処理を行う。

[0028] 復号部１１３は、Ｒ／Ｗ５０から受信するデータ等を復号化する。復号部１１３は、一例として、Present 80 Decryption によるデータの復号化処理を行う。Present 80 Decryptionは、共通鍵を使った復号化手法である。

[0029] 認証部１１４は、Ｒ／Ｗ５０から受信する暗号やカウント値等に基づいて、Ｒ／Ｗ５０の認証処理を行う。認証処理の詳細については、図２を用いて後述する。

[0030] 論理演算部１１５は、センサ３０の検出値と、暗号部１１２が生成する暗号値との排他的論理和（ＥＸＯＲ）を演算する。この処理の詳細については図２を用いて後述する。

[0031] 通信部１１６は、Ｒ／Ｗ５０との通信用のアンテナ１２０が接続されている。通信部１１６は、主制御部１１１からの指令に従って、Ｒ／Ｗ５０にデータを送信する処理と、Ｒ／Ｗ５０からデータを受信する処理とを行う。

[0032] アンテナ１２０は、Ｒ／Ｗ５０と無線通信を行えるアンテナであればよい。アンテナ１２０は、通信部１１６に接続されており、Ｒ／Ｗ５０から送信されるデータ等を含む信号を受信し、Ｒ／Ｗ５０に返信するデータ等を含む信号を放射する。

[0033] メモリ１３０は、ＲＦＩＤタグ１００が認証処理を行うために必要なプログラムやデータ等を格納する。また、メモリ１３０は、主制御部１１１がカウントするカウント値を一時的に保持する。また、メモリ１３０は、Ｒ／Ｗ５０及びＲＦＩＤタグ１００が暗号化や複合化等に用いる共通鍵を格納する

。

[0034] ここで、Ｒ／Ｗ５０のカウント値は、ＲＦＩＤタグ１００のカウント値以上である。Ｒ／Ｗ５０及びＲＦＩＤタグ１００は、Ｒ／Ｗ５０及びＲＦＩＤタグ１００の間で通信を行う度に、カウント値をインクリメントする。このため、Ｒ／Ｗ５０及びＲＦＩＤタグ１００の間の通信が異常がなく、Ｒ／Ｗ５０及びＲＦＩＤタグ１００が送信／受信を毎回正常に行えている場合には、Ｒ／Ｗ５０及びＲＦＩＤタグ１００のカウント値は等しくなる。異常とは、例えば、Ｒ／Ｗ５０が信号を送信しても、ノイズ等によってＲＦＩＤタグ１００が受信できないような状態である。

[0035] ところで、通信に異常が生じると、ＲＦＩＤタグ１００はＲ／Ｗ５０から送信された信号がＲ／Ｗ５０から送信されたことを認識できない状況が生じる。

[0036] この場合には、Ｒ／Ｗ５０のカウント値はインクリメントされるが、ＲＦＩＤタグ１００のカウント値はインクリメントされない。このため、Ｒ／Ｗ５０のカウント値は、ＲＦＩＤタグ１００のカウント値よりも進む（多くなる）ことが有り得る。

[0037] 通信システム１０では、Ｒ／Ｗ５０及びＲＦＩＤタグ１００のカウント値を認証に利用する。ＲＦＩＤタグ１００がＲ／Ｗ５０を認証する際に、Ｒ／Ｗ５０のカウント値がＲＦＩＤタグ１００のカウント値以上であることが認証成立の１つの条件である。

[0038] ただし、Ｒ／Ｗ５０のカウント値がＲＦＩＤタグ１００のカウント値よりもあまりにも多い場合には、正常に完了しなかった通信の回数が多いことになる。

[0039] このため、Ｒ／Ｗ５０のカウント値がＲＦＩＤタグ１００のカウント値よりも進んでいる場合には、Ｒ／Ｗ５０のカウント値と、ＲＦＩＤタグ１００のカウント値との差が所定値以下である場合に、認証を成立させることとする。なお、所定値は、一例として５０である。

[0040] なお、ＲＦＩＤタグ１００が、本来信号を受信する対象ではないリーダラ

イタ（Ｒ／Ｗ５０とは別の同様のリーダライタ）が送信した信号を受信すると、本来信号を受信する対象であるＲ／Ｗ５０のカウント値よりもＲＦＩＤタグ１００のカウント値が進む場合が有り得る。このため、ＲＦＩＤタグ１００のカウント値がＲ／Ｗ５０のカウント値よりも進んでいる場合には、認証は不成立となる。

[0041] 図２は、Ｒ／Ｗ５０及びＲＦＩＤタグ１００が行う認証処理を示すタスク図である。

[0042] まず、初期状態において、Ｒ／Ｗ５０のカウント値が６４ビットのＭ（６４ｂｉｔ）であることとする。Ｒ／Ｗ５０の制御部６１はカウント値をインクリメントしＭ＋１（６４ｂｉｔ）とする。Ｒ／Ｗ５０の暗号部６２は、共通鍵を用いてインクリメントしたカウント値Ｍ＋１（６４ｂｉｔ）を暗号化して、暗号値１（６４ｂｉｔ）を生成する。

[0043] そして、Ｒ／Ｗ５０は、暗号値１（６４ｂｉｔ）と、カウント値Ｍ＋１（６４ｂｉｔ）のうちの下位１６ビットであるカウント値Ｍ＋１（下位１６ｂｉｔ）とをＲＦＩＤタグ１００に送信する。

[0044] なお、暗号値１（６４ｂｉｔ）は、第１暗号値の一例であり、カウント値Ｍ＋１（下位１６ｂｉｔ）は、第１数値の一例である。また、カウント値Ｍ＋１（６４ｂｉｔ）のうちの下位１６ビット（カウント値Ｍ＋１（下位１６ｂｉｔ））のみをＲＦＩＤタグ１００に送信することにより、通信データ容量を小さくすることができる。

[0045] ＲＦＩＤタグ１００が暗号値１（６４ｂｉｔ）及びカウント値Ｍ＋１（下位１６ｂｉｔ）を受信すると、復号部１１３は、共通鍵で暗号値１（６４ｂｉｔ）を復号化し、認証部１１４は、復号化で得るカウント値Ｍ＋１（６４ｂｉｔ）の下位１６ビットと、受信したカウント値Ｍ＋１（下位１６ｂｉｔ）とを比較し、一致性を判定する。ここで、復号化で得るカウント値Ｍ＋１（６４ｂｉｔ）は、第１復号値の一例である。

[0046] 復号化で得るカウント値Ｍ＋１（６４ｂｉｔ）のすべてのビット（６４ビット）を比較しなくても、下位１６ビット同士の比較で十分であるため、下

位１６ビット同士のみを比較するようにしている。また、これにより、通信データ容量を小さくすることができる。

[0047] ここで、一致性を判定し、一致することは、一致性が成立することである。ここでは、下位１６ビット同士のように一部の連続するビット同士が一致する場合に、一致性が成立することになる。なお、一致性の判定は、全ビット同士で行ってもよく、この場合には、全ビット同士が一致する場合に、一致性が成立することになる。

[0048] 認証部１１４は、下位１６ビット同士の値が一致する場合に、復号化で得るカウント値Ｍ＋１（６４ｂｉｔ）が、ＲＦＩＤタグ１００の６４ビットのカウント値Ｎと等しいか、又は、カウント値Ｎよりも進んでおり、かつ、カウント値の差が所定値以下であれば、Ｒ／Ｗ５０の認証が成立したと判定する。

[0049] Ｒ／Ｗ５０のカウント値は、ＲＦＩＤタグ１００のカウント値以上である。このため、Ｒ／Ｗ５０のカウント値（復号化で得るカウント値Ｍ＋１（６４ｂｉｔ））と、ＲＦＩＤタグ１００のカウント値Ｎとが等しい場合には、Ｒ／Ｗ５０及びＲＦＩＤタグ１００のカウント値は正常であり、Ｒ／Ｗ５０の認証が成立したこととする。

[0050] また、Ｒ／Ｗ５０のカウント値（復号化で得るカウント値Ｍ＋１（６４ｂｉｔ））がＲＦＩＤタグ１００のカウント値Ｎよりも多い場合に、その差が所定値以下である場合にも、Ｒ／Ｗ５０及びＲＦＩＤタグ１００のカウント値は正常であり、Ｒ／Ｗ５０の認証が成立したこととする。なお、所定値は、一例として５０である。

[0051] ＲＦＩＤタグ１００の主制御部１１１は、認証が成立すると、自己のカウント値Ｎを、復号化で得るカウント値Ｍ＋１（６４ｂｉｔ）に設定する。これにより、ＲＦＩＤタグ１００のカウント値は、復号化で得るカウント値Ｍ＋１（６４ｂｉｔ）になる。

[0052] 次に、ＲＦＩＤタグ１００の主制御部１１１は、センサ３０の検出値を取得する。検出値は、１６ビットのＳ（１６ｂｉｔ）である。

[0053] また、ＲＦＩＤタグ１００の主制御部１１１は、カウント値（Ｍ＋１（６４ｂｉｔ））をインクリメントし、Ｍ＋２（６４ｂｉｔ）にする。暗号部１１２は、カウント値Ｍ＋２（６４ｂｉｔ）を共通鍵で暗号化して、暗号値２（６４ｂｉｔ）を生成する。暗号値２（６４ｂｉｔ）は、第２暗号値の一例である。

[0054] 次に、論理演算部１１５は、センサ３０の検出値Ｓ（１６ｂｉｔ）と、暗号値２（６４ｂｉｔ）との排他的論理和を演算し、暗号値Ｓ（１６ｂｉｔ）を出力する。暗号値Ｓ（１６ｂｉｔ）は、暗号検出値の一例である。

[0055] 暗号部１１２は、暗号値Ｓ（１６ｂｉｔ）をカウント値Ｍ＋２（６４ｂｉｔ）で暗号化して、暗号値３（６４ｂｉｔ）を生成する。暗号値３（６４ｂｉｔ）は、第３暗号値の一例である。

[0056] そして、主制御部１１１は、暗号値Ｓ（１６ｂｉｔ）と、暗号値３（６４ｂｉｔ）の先頭（上位）８ビットである暗号値３（上位８ｂｉｔ）とを通信部１１６を介してＲ／Ｗ５０に送信する。

[0057] Ｒ／Ｗ５０は、受信モードになり、カウント値（Ｍ＋１）をインクリメントしてＭ＋２にする。

[0058] 暗号部６２は、インクリメントしたカウント値Ｍ＋２を共通鍵で暗号化し、６４ビットの暗号値４（６４ｂｉｔ）を生成する。暗号値４（６４ｂｉｔ）は、第４暗号値の一例である。暗号値４（６４ｂｉｔ）は、ＲＦＩＤタグ１００がＲ／Ｗ５０から貰ったカウント値Ｍ＋１をインクリメントしたＭ＋２を共通鍵で暗号化して生成した暗号値２（６４ｂｉｔ）と等しい。

[0059] Ｒ／Ｗ５０が暗号値Ｓ（１６ｂｉｔ）と、暗号値３（上位８ｂｉｔ）とを受信すると、論理演算部６５は、ＲＦＩＤタグ１００から受信した暗号値Ｓ（１６ｂｉｔ）と、暗号値４（６４ｂｉｔ）との排他的論理和を取ることによって暗号値Ｓ（１６ｂｉｔ）から検出値Ｓ（１６ｂｉｔ）を取り出す。

[0060] 暗号部６２は、論理演算部６５によって取り出された検出値Ｓ（１６ｂｉｔ）をカウント値Ｍ＋２で暗号化して暗号値５（６４ｂｉｔ）を生成する。暗号値５（６４ｂｉｔ）は、第５暗号値の一例である。

[0061] 認証部６４は、暗号部６２によって暗号化された暗号値５（６４ｂｉｔ）と、ＲＦＩＤタグ１００から受信した暗号値３（上位８ｂｉｔ）とを比較し、暗号値５（６４ｂｉｔ）の上位８ビットと一致すれば（一致性が成立すれば）、ＲＦＩＤタグ１００の認証が成立したと判定する。

[0062] 暗号値３（６４ｂｉｔ）は、ＲＦＩＤタグ１００の暗号部１１２が、暗号値Ｓ（１６ｂｉｔ）をカウント値Ｍ＋２（６４ｂｉｔ）で暗号化して生成した暗号値であり、暗号値５（６４ｂｉｔ）は、Ｒ／Ｗ５０の論理演算部６５によって取り出された検出値Ｓ（１６ｂｉｔ）を暗号部６２がカウント値Ｍ＋２で暗号化した暗号値であるため、上位８ビット同士が一致すれば、共通鍵とカウンタ値が一致するので正当な（正規の）ＲＦＩＤタグ１００であると考えられるからである。正当な（正規の）とは、自己の通信相手として通信システム１０において割り当てられていることをいう。

[0063] 主制御部６１は、検出値Ｓ（１６ｂｉｔ）をセンサ３０の検出値として採用し、上位機に伝送する。上位機は、センサ３０の検出値を収集するサーバ等である。

[0064] 図３は、Ｒ／Ｗ５０が実行する相互認証処理を表すフローチャートを示す図である。図４は、ＲＦＩＤタグ１００が実行する相互認証処理を表すフローチャートを示す図である。ここでは、図３及び図４をともに用いてＲ／Ｗ５０とＲＦＩＤタグ１００の処理を示す。

[0065] 処理がスタートすると、主制御部６１は、カウント値をインクリメントする（ステップＳ１）。これにより、Ｒ／Ｗ５０のカウント値は、６４ビットのＭ＋１（６４ｂｉｔ）になる。

[0066] 暗号部６２は、共通鍵でカウント値Ｍ＋１（６４ｂｉｔ）を暗号化して、暗号値１（６４ｂｉｔ）を生成する（ステップＳ２）。

[0067] 主制御部６１は、暗号値１（６４ｂｉｔ）と、カウント値Ｍ＋１（６４ｂｉｔ）のうちの下位１６ビットであるカウント値Ｍ＋１（下位１６ｂｉｔ）とをＲＦＩＤタグ１００に送信する（ステップＳ３）。

[0068] Ｒ／Ｗ５０は、受信モードになり、カウント値（Ｍ＋１）をインクリメン

トしてＭ＋２にする（ステップＳ４）。

[0069] 暗号部６２は、インクリメントしたカウント値Ｍ＋２を共通鍵で暗号化し、６４ビットの暗号値４（６４ｂｉｔ）を生成する（ステップＳ５）。

[0070] ＲＦＩＤタグ１００の主制御部１１１は、暗号値１（６４ｂｉｔ）及びカウント値Ｍ＋１（下位１６ｂｉｔ）を受信する（ステップＳ２１）。

[0071] 復号部１１３は、共通鍵で暗号値１（６４ｂｉｔ）を復号化し、カウント値Ｍ＋１（６４ｂｉｔ）を生成する（ステップＳ２２）。

[0072] 認証部１１４は、復号化で得るカウント値Ｍ＋１（６４ｂｉｔ）の下位１６ビットと、受信したカウント値Ｍ＋１（下位１６ｂｉｔ）とを比較し、一致性を判定する（ステップＳ２３）。

[0073] 認証部１１４は、下位１６ビット同士の値が一致する（一致性が成立する）（Ｓ２３：ＹＥＳ）場合に、Ｒ／Ｗ５０の認証が成立したかどうかを判定する（ステップＳ２４）。認証部１１４が認証が成立したと判定するのは、復号化で得るカウント値Ｍ＋１（６４ｂｉｔ）が、ＲＦＩＤタグ１００の６４ビットのカウント値Ｎと等しいか、又は、カウント値Ｎよりも進んでおり、かつ、カウント値の差が所定値以下である場合である。

[0074] 認証部１１４によってＲ／Ｗ５０の認証が成立した（Ｓ２４：ＹＥＳ）と判定されると、主制御部１１１は、カウント値Ｎを復号化で得るカウント値Ｍ＋１（６４ｂｉｔ）に設定し、さらにインクリメントする（ステップＳ２５）。これにより、ＲＦＩＤタグ１００のカウント値は、カウント値Ｍ＋２（６４ｂｉｔ）になる。

[0075] 暗号部１１２は、カウント値Ｍ＋２（６４ｂｉｔ）を共通鍵で暗号化して、暗号値２（６４ｂｉｔ）を生成する（ステップＳ２６）。

[0076] 次に、ＲＦＩＤタグ１００の主制御部１１１は、センサ３０の検出値Ｓ（１６ｂｉｔ）を取得する（ステップＳ２７）。

[0077] 次に、論理演算部１１５は、センサ３０の検出値Ｓ（１６ｂｉｔ）と、暗号値２（６４ｂｉｔ）との排他的論理和を演算し、暗号値Ｓ（１６ｂｉｔ）を出力する（ステップＳ２８）。

[0078] 暗号部１１２は、暗号値Ｓ（１６ｂｉｔ）をカウント値Ｍ＋２（６４ｂｉｔ）で暗号化して、暗号値３（６４ｂｉｔ）を生成する（ステップＳ２９）。

[0079] そして、主制御部１１１は、暗号値Ｓ（１６ｂｉｔ）と、暗号値３（６４ｂｉｔ）の先頭（上位）８ビットである暗号値３（上位８ｂｉｔ）とを通信部１１６を介してＲ／Ｗ５０に送信する（ステップＳ３０）。

[0080] Ｒ／Ｗ５０の主制御部６１は、通信部６６を介して暗号値Ｓ（１６ｂｉｔ）と、暗号値４（上位８ｂｉｔ）とを受信する（ステップＳ６）。

[0081] 論理演算部６５は、ＲＦＩＤタグ１００から受信した暗号値Ｓ（１６ｂｉｔ）と、暗号値４（６４ｂｉｔ）との排他的論理和を取ることによって暗号値Ｓ（１６ｂｉｔ）から検出値Ｓ（１６ｂｉｔ）を取り出す（ステップＳ７）。

[0082] 暗号部６２は、論理演算部６５によって取り出された検出値Ｓ（１６ｂｉｔ）をカウント値Ｍ＋２で暗号化して暗号値５（６４ｂｉｔ）を生成する（ステップＳ８）。

[0083] 認証部６４は、暗号部６２によって暗号化された暗号値５（６４ｂｉｔ）と、ＲＦＩＤタグ１００から受信した暗号値３（上位８ｂｉｔ）とを比較し、一致性を判定する（ステップＳ９）。

[0084] 認証部６４は、暗号値５（６４ｂｉｔ）の上位８ビットと一致すれば（一致性が成立すれば）、ＲＦＩＤタグ１００の認証が成立したと判定し、主制御部６１は、検出値Ｓ（１６ｂｉｔ）を上位機に伝送する（ステップＳ１０）。

[0085] 一方、認証部６４によって認証が不成立と判定されると、主制御部６１は、動作を停止させる（ステップＳ１１）。そして、主制御部６１は、フローをステップＳ１２に進行させる。

[0086] 主制御部６１は、ステップＳ１０又はＳ１１の処理が終了すると、一連の処理を終了するかどうかを判定する（ステップＳ１２）。一連の処理を終了するのは、例えばＲ／Ｗ５０の電源がオフにされたときである。

[0087] 主制御部６１は、一連の処理を終了しない（Ｓ１２：ＮＯ）と判定すると、フローをステップＳ１にリターンし、一連の処理を終了する（Ｓ１２：ＹＥＳ）と判定すると、一連の処理を終了する（エンド）。

[0088] 以上のように、実施の形態の通信システム１０及び相互認証方法では、Ｒ／Ｗ５０及びＲＦＩＤタグ１００で共通のカウント値を用いることにより、Ｒ／Ｗ５０からＲＦＩＤタグ１００への１回の通信に基づいてＲＦＩＤタグ１００がＲ／Ｗ５０の認証を行い、ＲＦＩＤタグ１００からＲ／Ｗ５０への１回の通信に基づいてＲ／Ｗ５０がＲＦＩＤタグ１００の認証を行うことができる。

[0089] したがって、認証を短時間で行うことができる相互認証方法及び通信システム１０を提供することができる。

[0090] また、認証処理に必要な通信回数が少ないので、Ｒ／Ｗ５０の消費電力を低減することができる。

[0091] なお、以上では、Ｒ／Ｗ５０がカウント値Ｍ＋１（６４ｂｉｔ）のうちの下位１６ビットであるとをＲＦＩＤタグ１００に送信する形態について説明したが、１６ビットに限られず、下位に限られず、６４ビットのうちの連続する複数のビットであればよい。また、６４ビットすべてを送信してもよい。

[0092] また、以上では、検出値Ｓが１６ビットである形態について説明したが、検出値のビット数は１６ビットに限られず、例えば８ビットでもよい。

[0093] また、以上では、ＲＦＩＤタグ１００が暗号値３（６４ｂｉｔ）のうちの上位８ビットをＲ／Ｗ５０に送信する形態について説明したが、８ビットに限られず、上位に限られず、６４ビットのうちの連続する複数のビットであればよい。また、６４ビットすべてを送信してもよい。

[0094] また、以上では、ＲＦＩＤタグ１００がＲ／Ｗ５０を認証する処理に際して、Ｒ／Ｗ５０が共通鍵でカウント値Ｍ＋１（６４ｂｉｔ）を暗号化した暗号値１（６４ｂｉｔ）をＲＦＩＤタグ１００が共通鍵で復号化する形態について説明したが、図５に示すように、Ｒ／Ｗ５０が共通鍵でカウント値Ｍ＋

１（６４ｂｉｔ）を復号化した暗号値１（６４ｂｉｔ）をＲＦＩＤタグ１００が共通鍵で暗号化するようにしてもよい。

[0095] 図５に示すＲ／Ｗ５０とＲＦＩＤタグ１００の処理は、上述のようにＲＦＩＤタグ１００がＲ／Ｗ５０を認証する処理について、暗号化と複合化を入れ替えたこと以外は、図２に示す処理と同様である。

[0096] このような構成でも、Ｒ／Ｗ５０からＲＦＩＤタグ１００への１回の通信に基づいてＲＦＩＤタグ１００がＲ／Ｗ５０の認証を行い、ＲＦＩＤタグ１００からＲ／Ｗ５０への１回の通信に基づいてＲ／Ｗ５０がＲＦＩＤタグ１００の認証を行うことができ、認証を短時間で行うことができる相互認証方法及び通信システム１０を提供することができる。

[0097] 図５に示すような処理を行う場合には、ＲＦＩＤタグ１００は、ＲＦＩＤタグ１００がＲ／Ｗ５０を認証する処理に際して暗号化を行い、Ｒ／Ｗ５０がＲＦＩＤタグ１００を認証する処理に際しても暗号化を行うことになる。

[0098] このため、ＲＦＩＤタグ１００の制御装置１１０は、復号部１１３を含まなくてよくなり、ＲＦＩＤタグ１００の制御装置１１０の簡易化を図ることができ、コストダウンを図ることができる。なお、Ｒ／Ｗ５０の制御装置６０は、復号処理を行うことになるため、復号部をさらに含む構成にすればよい。

[0099] また、ＲＦＩＤタグ１００にセンサ３０が接続されていない場合には、図６及び図７に示すように相互認証処理を簡易化することができる。

[0100] 図６では、ＲＦＩＤタグ１００がＲ／Ｗ５０を認証する処理は、図２と同様である。Ｒ／Ｗ５０がＲＦＩＤタグ１００を認証する処理では、ＲＦＩＤタグ１００に検出値が存在しないため、図２に示すような排他的論理和を演算する処理が不要になり、次のような処理を行えばよい。

[0101] ＲＦＩＤタグ１００は、ＲＦＩＤタグ１００の主制御部１１１は、カウント値（Ｍ＋１（６４ｂｉｔ））をインクリメントし、Ｍ＋２（６４ｂｉｔ）にし、暗号部１１２は、カウント値Ｍ＋２（６４ｂｉｔ）を共通鍵で暗号化して、暗号値２（６４ｂｉｔ）を生成する。

[0102] Ｒ／Ｗ５０は、受信モードになり、カウント値（Ｍ＋１）をインクリメントしてＭ＋２にする。Ｒ／Ｗ５０は、ＲＦＩＤタグ１００から受信する暗号値２（６４ｂｉｔ）を共通鍵で復号化して得るカウント値Ｍ＋２（６４ｂｉｔ）が、自己のカウント値Ｍ＋２（６４ｂｉｔ）と一致すれば、ＲＦＩＤタグ１００の認証成立と判定する。

[0103] このようにセンサ３０がＲＦＩＤタグ１００に接続されていない場合には、論理演算部６５、論理演算部１１５が不要になるため、システムの簡略化を図りつつ、認証を短時間で行うことができる相互認証方法及び通信システム１０を提供することができる。なお、Ｒ／Ｗ５０は、復号化処理を行うため、制御装置６０は、復号部を含む構成になる。

[0104] また、図７に示す相互認証処理は、図６に示す相互認証処理におけるＲＦＩＤタグ１００がＲ／Ｗ５０を認証する処理において、Ｒ／Ｗ５０が共通鍵でカウント値Ｍ＋１（６４ｂｉｔ）を復号化した暗号値１（６４ｂｉｔ）をＲＦＩＤタグ１００が共通鍵で暗号化するように変形した処理である。

[0105] すなわち、図７に示す相互認証処理と、図６に示す相互認証処理との関係は、図５に示す相互認証処理と、図２に示す相互認証処理との関係と同様であり、図７に示すＲ／Ｗ５０とＲＦＩＤタグ１００の処理は、ＲＦＩＤタグ１００がＲ／Ｗ５０を認証する処理について、暗号化と複合化を入れ替えたこと以外は、図６に示す処理と同様である。

[0106] このため、ＲＦＩＤタグ１００の制御装置１１０は、復号部１１３を含まなくてよくなり、ＲＦＩＤタグ１００の制御装置１１０の簡易化を図ることができ、コストダウンを図ることができる。なお、Ｒ／Ｗ５０の制御装置６０は、復号処理を行うことになるため、復号部をさらに含む構成にすればよい。

[0107] 以上、本発明の例示的な実施の形態の相互認証方法及び通信システムについて説明したが、本発明は、具体的に開示された実施の形態に限定されるものではなく、特許請求の範囲から逸脱することなく、種々の変形や変更が可能である。

[0108] なお、本国際出願は、２０１８年８月２８日に出願した日本国特許出願２０１８－１５９７７１に基づく優先権を主張するものであり、その全内容は本国際出願にここでの参照により援用されるものとする。

符号の説明

[0109] １０　通信システム

３０　センサ

５０　Ｒ／Ｗ

６０　制御装置

６２　暗号部

６４　認証部

６５　論理演算部

６６　通信部

１００　ＲＦＩＤタグ

１１０　制御装置

１１２　暗号部

１１３　復号部

１１４　認証部

１１５　論理演算部

１１６　通信部

請求の範囲

[請求項1] 共通鍵を有する第１通信機と第２通信機とを含み、前記第１通信機及び前記第２通信機が通信回数を表す第１カウント値及び第２カウント値をそれぞれ保持する通信システムにおける相互認証方法であって、

前記第１通信機は、

前記共通鍵で前記第１カウント値を暗号化して第１暗号値を生成し、

前記第１暗号値と、前記第１カウント値の少なくとも一部分を含む第１数値とを前記第２通信機に送信し、

前記第２通信機は、

前記第１暗号値及び前記第１数値を受信すると、前記共通鍵で前記第１暗号値を復号化し、

前記復号化で得る第１復号値と前記第１数値との一致性を判定し、

前記一致性が成立する場合に、前記第１復号値が前記第２カウント値と等しいか、又は、前記第２カウント値よりも進んでいれば、第１通信機の認証が成立したと判定する、相互認証方法。

[請求項2] 前記第２通信機は、前記第１復号値が前記第２カウント値と等しいか、又は、前記第２カウント値よりも進んでいて前記第２カウント値との差が所定数以下であれば、第１通信機の認証が成立したと判定する、請求項１記載の相互認証方法。

[請求項3] 前記第２通信機は、前記認証が成立すると、前記第１復号値を前記第２カウント値として設定する、請求項１又は２記載の相互認証方法。

[請求項4] 前記第２通信機は、

前記第２カウント値をインクリメントし、

前記インクリメントした第２カウント値を前記共通鍵で暗号化して第２暗号値を生成し、

前記第２暗号値を前記第１通信機に送信する、請求項３記載の相互認証方法。

[請求項5] 前記第１通信機は、

前記第２通信機から前記第２暗号値を受信すると前記第１カウント値をインクリメントし、

前記第１通信機から受信した第２暗号値を前記共通鍵で復号して得る復号値が前記インクリメントした第１カウント値と一致するか判定し、

一致する場合に、前記第２通信機の認証が成立したと判定する、請求項４記載の相互認証方法。

[請求項6] 共通鍵を有する第１通信機と第２通信機とを含み、前記第１通信機及び前記第２通信機が通信回数を表す第１カウント値及び第２カウント値をそれぞれ保持する通信システムにおける相互認証方法であって、

前記第１通信機は、

前記共通鍵で前記第１カウント値を復号化して第１復号値を生成し、

前記第１復号値と、前記第１カウント値の少なくとも一部分を含む第１数値とを前記第２通信機に送信し、

前記第２通信機は、

前記第１復号値及び前記第１数値を受信すると、前記共通鍵で前記第１復号値を暗号化し、

前記暗号化で得る第１暗号値と前記第１数値との一致性を判定し、

前記一致性が成立する場合に、前記第１暗号値が前記第２カウント値と等しいか、又は、前記第２カウント値よりも進んでいれば、第１通信機の認証が成立したと判定する、相互認証方法。

[請求項7] 前記第２通信機は、前記第１暗号値が前記第２カウント値と等しいか、又は、前記第２カウント値よりも進んでいて前記第２カウント値

との差が所定数以下であれば、第１通信機の認証が成立したと判定する、請求項６記載の相互認証方法。

[請求項8] 前記第２通信機は、前記認証が成立すると、前記第１暗号値を前記第２カウント値として設定する、請求項６又は７記載の相互認証方法。

[請求項9] 前記第２通信機は、

前記第２カウント値をインクリメントし、

前記インクリメントした第２カウント値を前記共通鍵で暗号化して第２暗号値を生成し、

前記第２暗号値を前記第１通信機に送信する、請求項８記載の相互認証方法。

[請求項10] 前記第１通信機は、

前記第２通信機から前記第２暗号値を受信すると前記第１カウント値をインクリメントし、

前記第１通信機から受信した第２暗号値を前記共通鍵で復号して得る復号値が前記インクリメントした第１カウント値と一致するか判定し、

一致する場合に、前記第２通信機の認証が成立したと判定する、請求項９記載の相互認証方法。

[請求項11] 前記第２通信機は、

センサをさらに有し、

前記第２カウント値をインクリメントし、

前記インクリメントした第２カウント値を前記共通鍵で暗号化して第２暗号値を生成し、

前記センサの検出値と前記第２暗号値との排他的論理和を表す暗号検出値を生成し、

前記暗号検出値を前記インクリメントした第２カウント値で暗号化して第３暗号値を生成し、

前記暗号検出値と、前記第３暗号値の少なくとも一部分を含む第３数値とを前記第１通信機に送信する、請求項３又は９記載の相互認証方法。

[請求項12] 前記第１通信機は、

前記第２通信機から前記暗号検出値と第３数値とを受信すると前記第１カウント値をインクリメントし、

前記第２通信機から受信した暗号検出値と、前記インクリメントした第１カウント値を前記共通鍵で暗号化した第４暗号値との排他的論理和を取ることによって前記暗号検出値から検出値を取り出し、

前記取り出した検出値を前記インクリメントした第１カウント値で暗号化して第５暗号値を生成し、

前記第２通信機から受信した第３数値と前記第５暗号値とが一致するか判定し、

一致する場合に、前記第２通信機の認証が成立したと判定する、請求項１１記載の相互認証方法。

[請求項13] 第１通信機と第２通信機とを含み、前記第１通信機及び前記第２通信機が共通鍵を有する通信システムであって、

前記第１通信機は、

通信回数を表す第１カウント値をカウントする第１カウンタと、

前記共通鍵で前記第１カウント値を暗号化して第１暗号値を生成する暗号部と、

前記第１暗号値と、前記第１カウント値の少なくとも一部分を含む第１数値とを前記第２通信機に送信する第１通信部と

を有し、

前記第２通信機は、

通信回数を表す第２カウント値をカウントする第２カウンタと、

前記第１暗号値及び前記第１数値を前記第１通信機から受信する第２通信部と、

前記第２通信部が前記第１暗号値及び前記第１数値を受信すると、前記共通鍵で前記第１暗号値を復号化する復号部と、

前記復号化で得る第１復号値と前記第１数値との一致性を判定し、前記一致性が成立する場合に、前記第１復号値が前記第２カウント値と等しいか、又は、前記第２カウント値よりも進んでいれば、第１通信機の認証が成立したと判定する認証部と

を有する、通信システム。

[請求項14] 第１通信機と第２通信機とを含み、前記第１通信機及び前記第２通信機が共通鍵を有する通信システムであって、

前記第１通信機は、

通信回数を表す第１カウント値をカウントする第１カウンタと、

前記共通鍵で前記第１カウント値を復号化して第１復号値を生成する復号部と、

前記第１復号値と、前記第１カウント値の少なくとも一部分を含む第１数値とを前記第２通信機に送信する第１通信部と

を有し、

前記第２通信機は、

通信回数を表す第２カウント値をカウントする第２カウンタと、

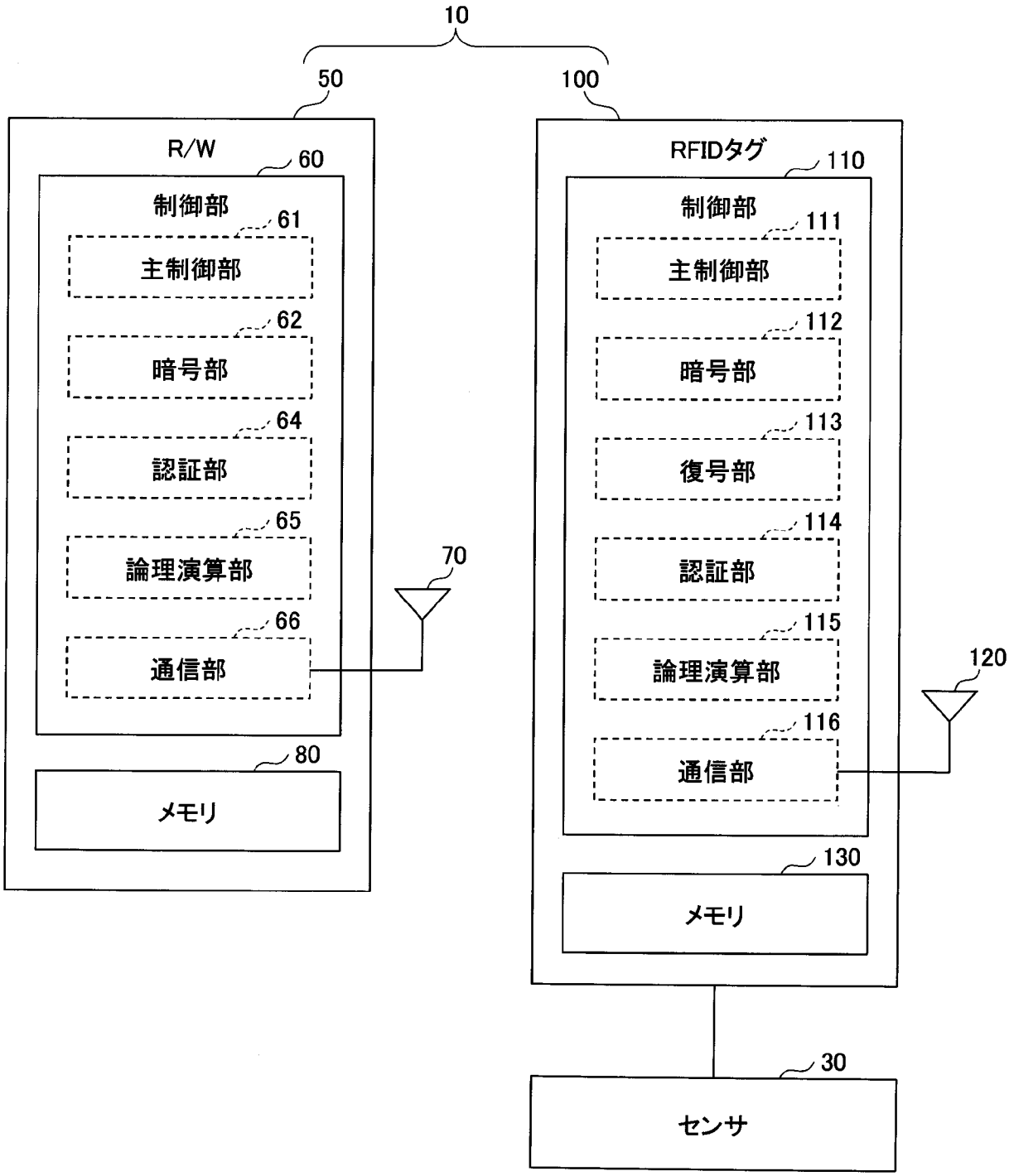
前記第１復号値及び前記第１数値を前記第１通信機から受信する第２通信部と、

前記第２通信部が前記第１復号値及び前記第１数値を受信すると、前記共通鍵で前記第１復号値を暗号化する暗号部と、

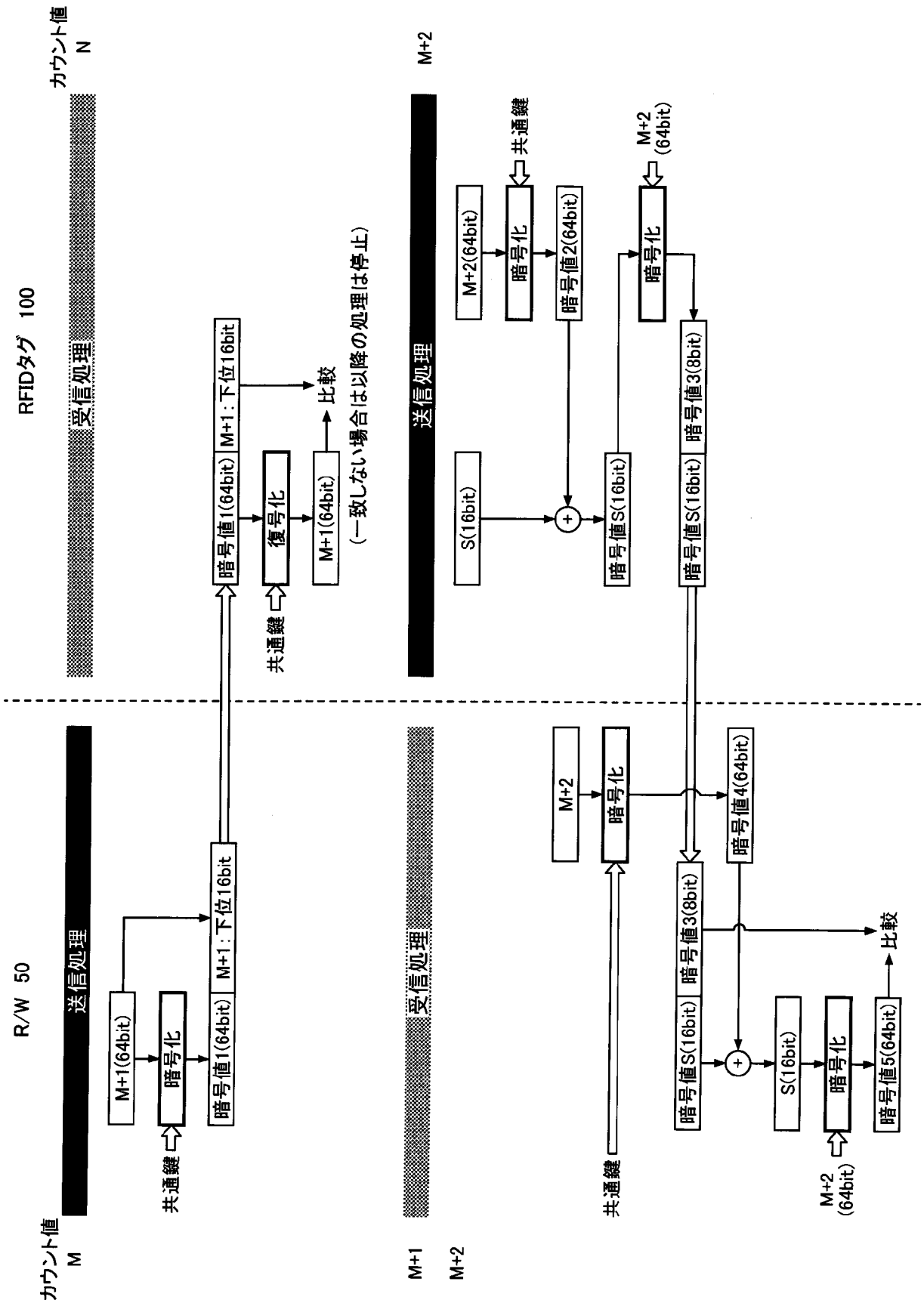
前記暗号化で得る第１暗号値と前記第１数値との一致性を判定し、前記一致性が成立する場合に、前記第１暗号値が前記第２カウント値と等しいか、又は、前記第２カウント値よりも進んでいれば、第１通信機の認証が成立したと判定する認証部と

を有する、通信システム。

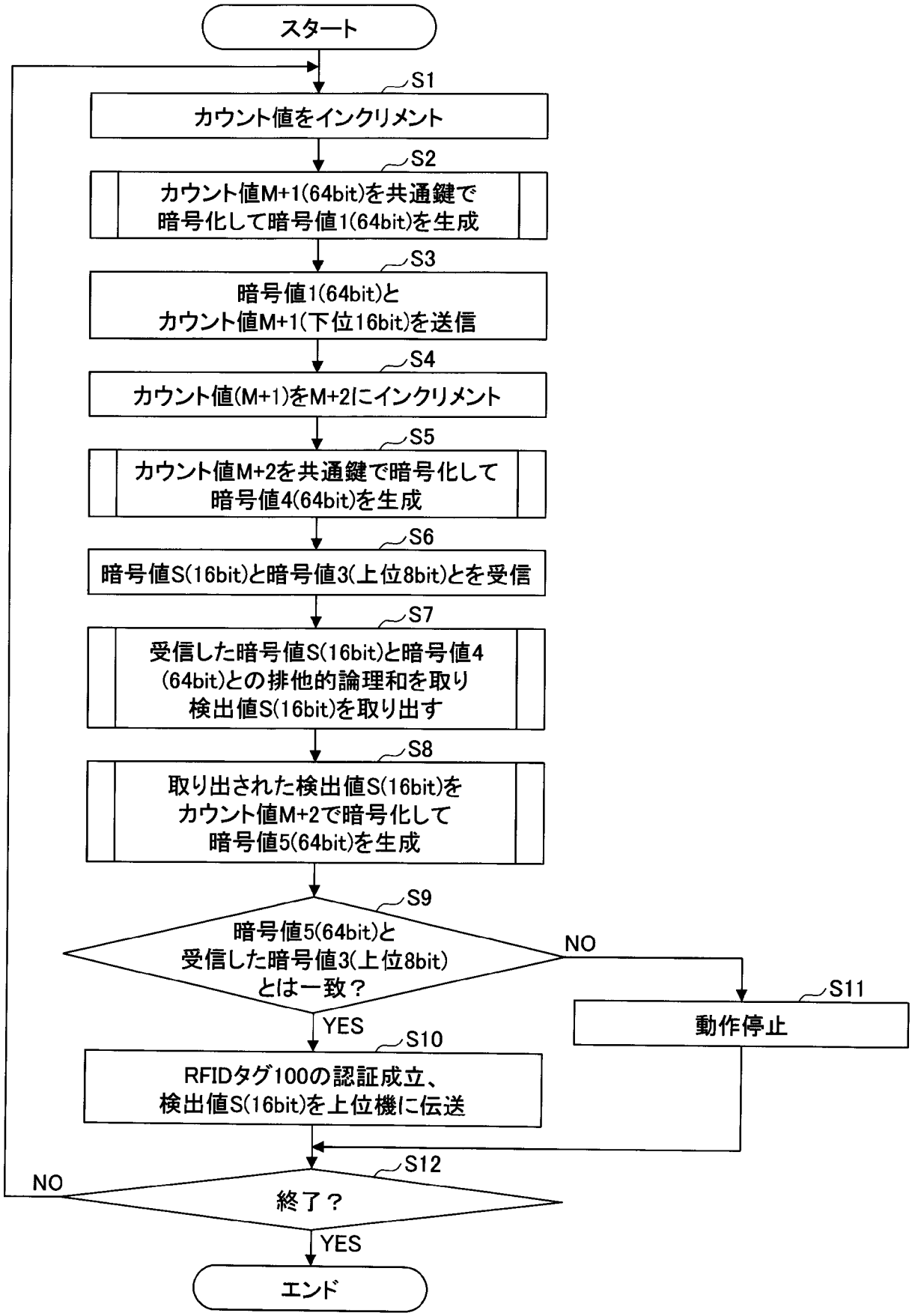
[図1]


10
50
100
R/W
60
制御部
61
主制御部
62
暗号部
64
認証部
65
論理演算部
66
通信部
70
80
メモリ
RFIDタグ
110
制御部
111
主制御部
112
暗号部
113
復号部
114
認証部
115
論理演算部
116
通信部
120
130
メモリ
30
センサ

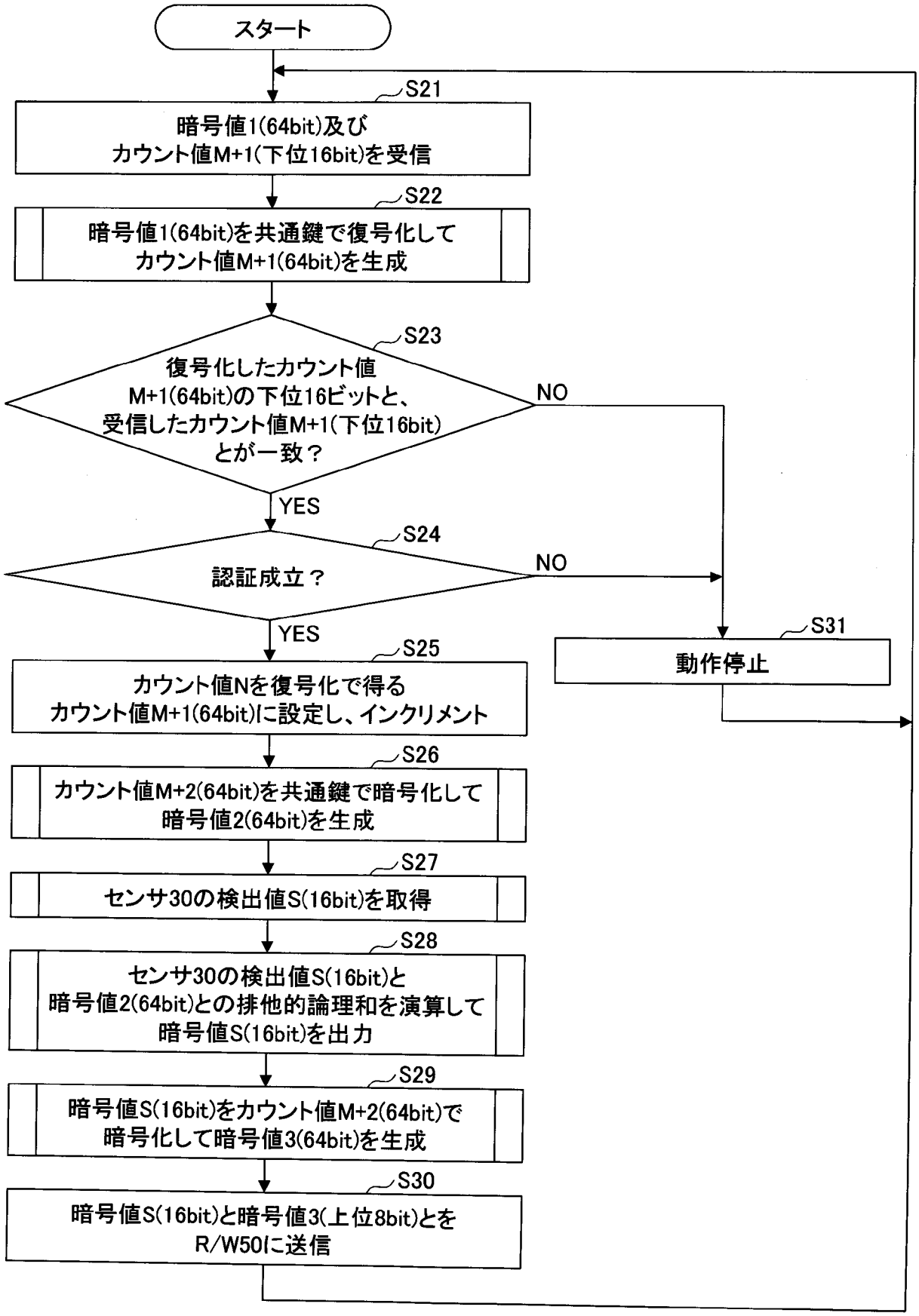
[図2]


RFIDタグ 100
R/W 50
カウント値 N
カウント値 M
M+2
M+1
M+2
受信処理
送信処理
送信処理
受信処理
M+1(64bit)
暗号化
共通鍵
暗号値1(64bit)
M+1:下位16bit
暗号値1(64bit)
M+1:下位16bit
復号化
共通鍵
M+1(64bit)
比較
(一致しない場合は以降の処理は停止)
M+2(64bit)
暗号化
共通鍵
暗号値2(64bit)
S(16bit)
暗号値S(16bit)
M+2
(64bit)
暗号化
暗号値3(8bit)
暗号値S(16bit)
暗号値3(8bit)
M+2
暗号化
共通鍵
暗号値4(64bit)
暗号値S(16bit)
暗号値3(8bit)
S(16bit)
暗号化
M+2
(64bit)
暗号値5(64bit)
比較

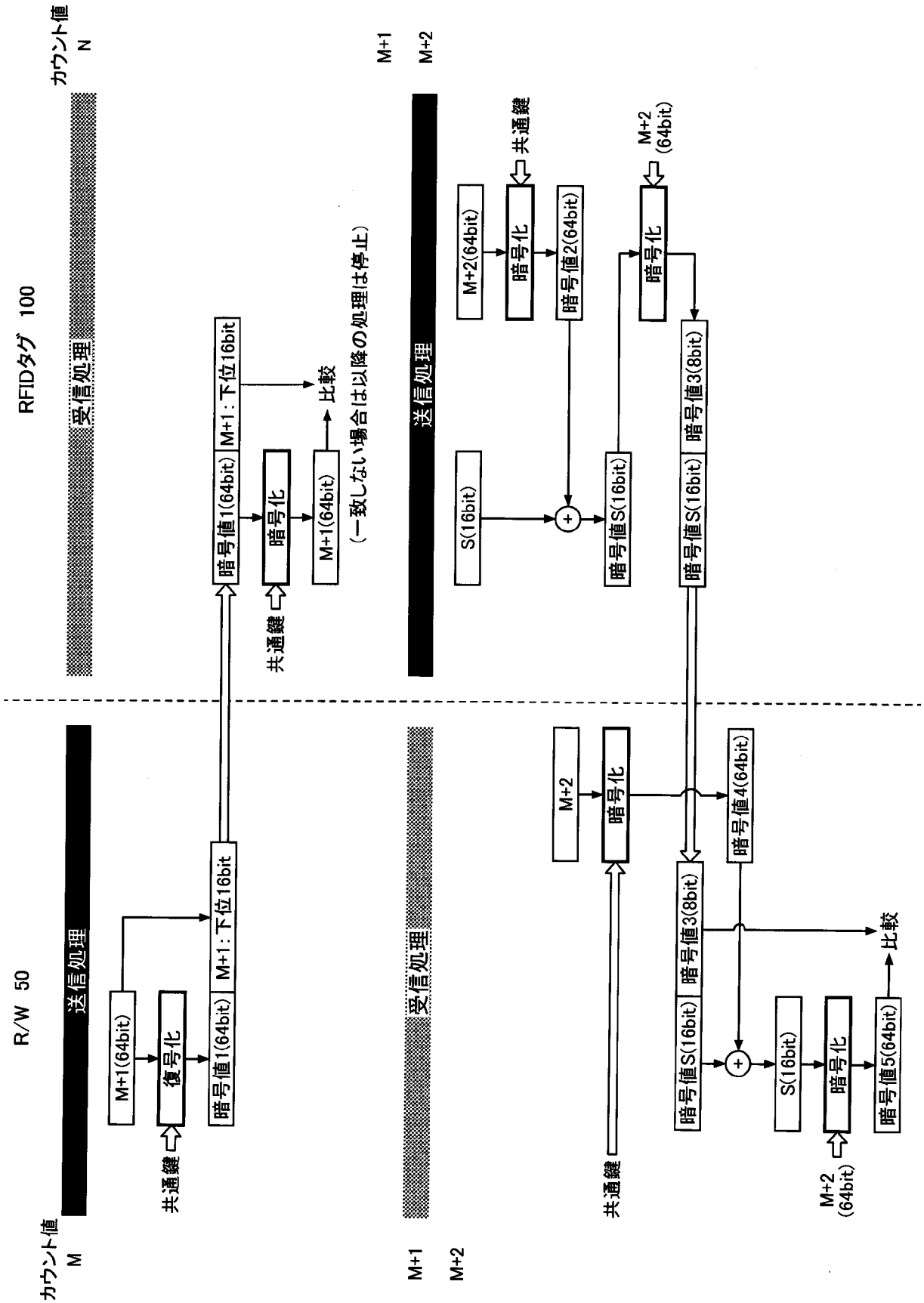
[図3]


スタート
S1
カウント値をインクリメント
S2
カウント値M+1(64bit)を共通鍵で
暗号化して暗号値1(64bit)を生成
S3
暗号値1(64bit)と
カウント値M+1(下位16bit)を送信
S4
カウント値(M+1)をM+2にインクリメント
S5
カウント値M+2を共通鍵で暗号化して
暗号値4(64bit)を生成
S6
暗号値S(16bit)と暗号値3(上位8bit)とを受信
S7
受信した暗号値S(16bit)と暗号値4
(64bit)との排他的論理和を取り
検出値S(16bit)を取り出す
S8
取り出された検出値S(16bit)を
カウント値M+2で暗号化して
暗号値5(64bit)を生成
S9
暗号値5(64bit)と
受信した暗号値3(上位8bit)
とは一致？
NO
S11
動作停止
YES
S10
RFIDタグ100の認証成立、
検出値S(16bit)を上位機に伝送
S12
NO
終了？
YES
エンド

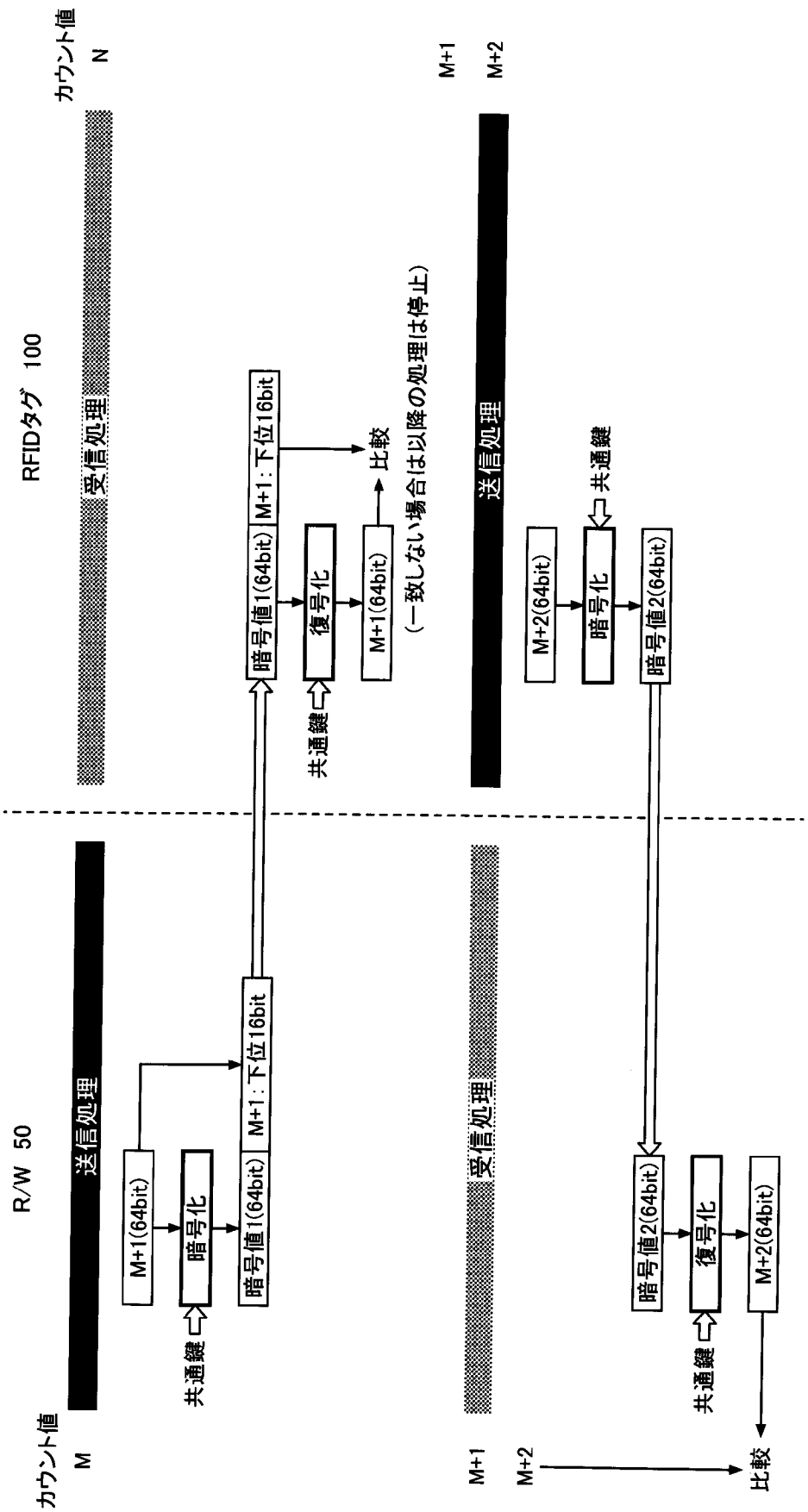
[図4]


スタート
S21
暗号値1(64bit)及び
カウント値M+1(下位16bit)を受信
S22
暗号値1(64bit)を共通鍵で復号化して
カウント値M+1(64bit)を生成
S23
復号化したカウント値
M+1(64bit)の下位16ビットと、
受信したカウント値M+1(下位16bit)
とが一致？
NO
YES
S24
認証成立？
NO
YES
S31
動作停止
S25
カウント値Nを復号化で得る
カウント値M+1(64bit)に設定し、インクリメント
S26
カウント値M+2(64bit)を共通鍵で暗号化して
暗号値2(64bit)を生成
S27
センサ30の検出値S(16bit)を取得
S28
センサ30の検出値S(16bit)と
暗号値2(64bit)との排他的論理和を演算して
暗号値S(16bit)を出力
S29
暗号値S(16bit)をカウント値M+2(64bit)で
暗号化して暗号値3(64bit)を生成
S30
暗号値S(16bit)と暗号値3(上位8bit)とを
R/W50に送信

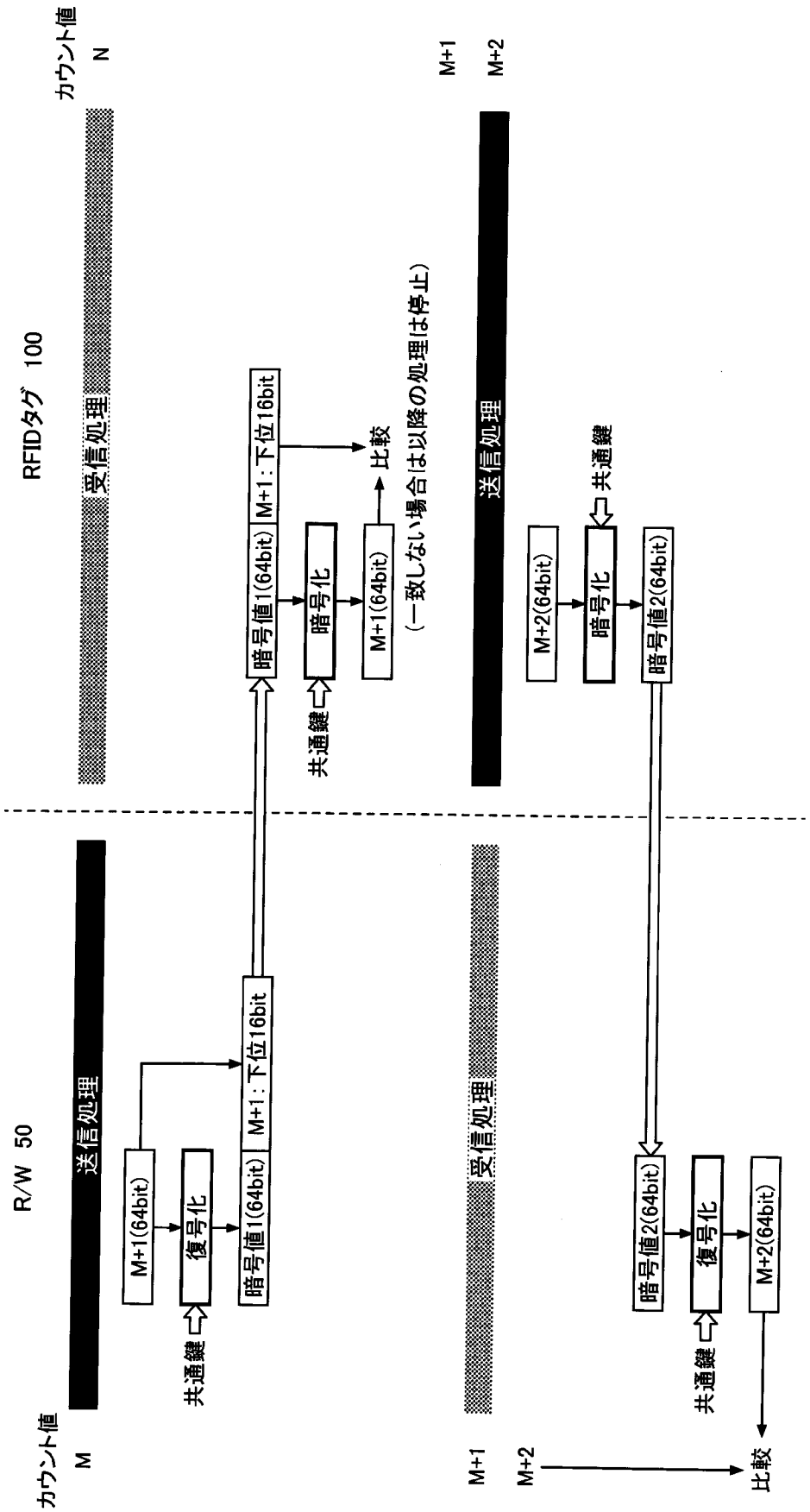
[図5]


R/W 50
RFIDタグ 100
送信処理
受信処理
送信処理
受信処理
カウント値 M
カウント値 N
M+1
M+2
M+1(64bit)
復号化
共通鍵
暗号値1(64bit)
M+1:下位16bit
暗号化
M+1(64bit)
比較
(一致しない場合は以降の処理は停止)
S(16bit)
M+2(64bit)
暗号値2(64bit)
暗号値S(16bit)
暗号値3(8bit)
M+2
(64bit)
M+2
暗号値4(64bit)
暗号値5(64bit)

[図6]


RFIDタグ 100
R/W 50
カウント値
M
カウント値
N
M+1
M+2
送信処理
受信処理
送信処理
受信処理
M+1(64bit)
暗号化
共通鍵
暗号値1(64bit)
M+1:下位16bit
暗号値1(64bit)
M+1:下位16bit
復号化
共通鍵
M+1(64bit)
比較
(一致しない場合は以降の処理は停止)
M+2(64bit)
暗号化
共通鍵
暗号値2(64bit)
暗号値2(64bit)
復号化
共通鍵
M+2(64bit)
M+1
M+2
比較

[図7]


RFIDタグ 100
R/W 50
カウント値
M
カウント値
N
M+1
M+2
送信処理
受信処理
M+1(64bit)
復号化
共通鍵
暗号値1(64bit)
M+1:下位16bit
暗号化
M+1(64bit)
比較
(一致しない場合は以降の処理は停止)
M+2(64bit)
暗号値2(64bit)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/009533

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. H04L9/32(2006.01)i, G06F21/44(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. H04L9/32, 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	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

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	US 2009/0019282 A1 (ARDITTI, D. et al.) 15 January 2009, paragraphs [0053]-[0081] & WO 2006/024732 A1 & FR 2874144 A1	1-14
A	WO 2014/147934 A1 (PANASONIC CORP.) 25 September 2014, paragraphs [0011]-[0097] & US 2015/0381733 A1, paragraphs [0019]-[0106] & CN 104969509 A	1-14

☒ 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 16 May 2019 (16.05.2019)	Date of mailing of the international search report 28 May 2019 (28.05.2019)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/009533

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2011-523264 A (ALCATEL-LUCENT USA INC.) 04 August 2011, paragraphs [0041], [0042] & WO 2009/136981 A1, page 14, lines 1-18 & US 2009/0280774 A1 & EP 2286611 A1 & KR 10-2011-0002076 A & CN 102440019 A	1-14
A	JP 10-304333 A (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) 13 November 1998, paragraphs [0073], [0074] & US 6182215 B1, column 17, lines 1-19 & EP 862293 A2 & CN 1200511 A & KR 10-0451012 B	1-14
A	US 2009/0153290 A1 (BIERACH, K. B.) 18 June 2009, paragraphs [0025], [0036] (Family: none)	1-14
A	JP 2014-168216 A (MITSUBISHI HEAVY INDUSTRIES, LTD.) 11 September 2014, paragraphs [0015]-[0042] (Family: none)	1-14

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１９／００９５３３

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/32(2006.01)i, G06F21/44(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.　H04L9/32, 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　１９７１－２０１９年
日本国実用新案登録公報　１９９６－２０１９年
日本国登録実用新案公報　１９９４－２０１９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	US 2009/0019282 A1 (ARDITTI, D. et al.) 2009.01.15, 段落 0053－0081 & WO 2006/024732 A1 & FR 2874144 A1	1-14
A	WO 2014/147934 A1 (パナソニック株式会社) 2014.09.25, 段落 0011－0097 & US 2015/0381733 A1, 段落 0019－0106 & CN 104969509 A	1-14

☑　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
１６．０５．２０１９	２８．０５．２０１９

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　６３０４
行田　悦資
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
A	JP 2011-523264 A (アルカテルールーセント　ユーエスエー　インコーポレーテッド) 2011.08.04, 段落 0041, 0042 & WO 2009/136981 A1, 14 頁 1－18 行 & US 2009/0280774 A1 & EP 2286611 A1 & KR 10-2011-0002076 A & CN 102440019 A	1-14
A	JP 10-304333 A (松下電器産業株式会社) 1998.11.13, 段落 0073, 0074 & US 6182215 B1, 17 欄 1－19 行 & EP 862293 A2 & CN 1200511 A & KR 10-0451012 B	1-14
A	US 2009/0153290 A1 (BIERACH, K. B.) 2009.06.18, 段落 0025, 0036 (ファミリーなし)	1-14
A	JP 2014-168216 A (三菱重工業株式会社) 2014.09.11, 段落 0015－0042 (ファミリーなし)	1-14