

(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1月2日(02.01.2020)



(10) 国際公開番号

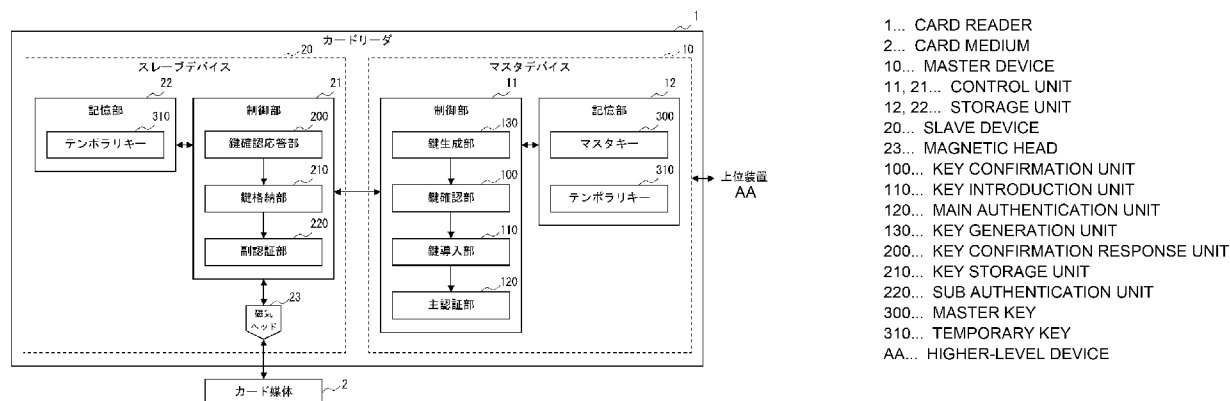
WO 2020/003958 A1

- (51) 国際特許分類:
H04L 9/32 (2006.01) *G09C 1/00* (2006.01)
G06F 21/44 (2013.01) *H04L 9/08* (2006.01)
- (21) 国際出願番号: PCT/JP2019/022534
- (22) 国際出願日: 2019年6月6日(06.06.2019)
- (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 2018-124592 2018年6月29日(29.06.2018) JP
- (71) 出願人: 日本電産サンキョー株式会社(NIDEC SANKYO CORPORATION) [JP/JP];
〒3938511 長野県諏訪郡下諏訪町 5 3 2 9 番地 Nagano (JP).
- (72) 発明者: 佐伯 和人(SAEKI kazuto); 〒3938511 長野県諏訪郡下諏訪町 5 3 2 9 番地 日本電産サンキョー株式会社内 Nagano (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, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS,

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

(54) 発明の名称: 相互認証システム及び相互認証方法

[図1]



(57) Abstract: The present invention provides a mutual authentication system in which a master key need not be erased when a slave device is replaced. A storage unit 12 stores a temporary key 310 that is temporarily used key data, and a master key 300 that is key data used for authentication. A storage unit 22 stores the temporary key 310. A key confirmation unit 100 inquires whether a slave device 20 stores the master key 300. A key confirmation response unit 200 responds to an inquiry from a master device 10 after confirming whether the master key 300 is already stored in the storage unit 22. A key introduction unit 110 encrypts the master key 300 with the temporary key 310, and transmits the encrypted master key to the slave device 20. A key storage unit 210 decrypts the encrypted master key 300 with the temporary key 310 and stores the decrypted master key in the storage unit 22. A main authentication unit 120 and a sub authentication unit 220 perform mutual authentication with the master key 300.

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)）

(57) 要約：スレーブデバイスの交換時にマスタキーを消去しなくてもよい相互認証システムを提供する。記憶部12は、一時的に用いられる鍵データであるテンポラリキー310、及び認証に用いられる鍵データであるマスタキー300を格納する。記憶部22は、テンポラリキー310を格納する。鍵確認部100は、マスタキー300をスレーブデバイス20が格納しているか問い合わせる。鍵確認応答部200は、マスタデバイス10からの問い合わせに対して、マスタキー300が記憶部22に既に格納されているか確認して応答する。鍵導入部110は、マスタキー300をテンポラリキー310にて暗号化して、スレーブデバイス20に送信する。鍵格納部210は、暗号化されたマスタキー300をテンポラリキー310で復号化して記憶部22に格納する。主認証部120及び副認証部220は、このマスタキー300にて相互認証する。

明 細 書

発明の名称： 相互認証システム及び相互認証方法

技術分野

[0001] 本発明は、相互認証システム及び相互認証方法に係り、特にマスタデバイスとスレーブデバイスとの間で相互認証可能な相互認証システム及び相互認証方法に関する。

背景技術

[0002] 従来から、本体側基板（マスタデバイス）と、ヘッド側基板（スレーブデバイス）とを備えるカードリーダーが存在する。

特許文献１には、このようなカードリーダーの一例が記載されている。このカードリーダーのマスタデバイスは、磁気ヘッドを制御するＣＰＵ（主制御部）を備える。スレーブデバイスは、一体的に形成された暗号磁気ヘッドとして構成される。この暗号磁気ヘッドは、磁気ヘッド、復調用ＩＣ、及び暗号化並びに復号化を行うＣＰＵ（副制御部）を備える。副制御部は、暗号化のための鍵データであるマスタキーを格納する。これにより、スレーブデバイスは、復調した磁気データを暗号化して、安全に主制御部及び上位装置に送信する。

[0003] 一方、複数のデバイス間で暗号の相互認証を行う相互認証システムが存在する。たとえば、このような相互認証を行うシステムが、特許文献２に記載されている。

先行技術文献

特許文献

[0004] 特許文献１：特開２０１４－８１９３１号公報

特許文献２：特開２０１３－１０９５５４号公報

発明の概要

発明が解決しようとする課題

[0005] ここで、特許文献１に記載されたような典型的なカードリーダーでも、マス

タデバイスとスレーブデバイスとで、相互認証を行うものが存在した。

このようなカードリーダーでは、スレーブデバイスを取り換える際（交換時）に、安全（セキュリティ）上の要求から、マスタキーをいったん消去する必要があった。しかし、マスタキーを消去すること自体に、セキュリティ上の懸念があった。

[0006] 本発明は、このような状況に鑑みてなされたものであり、上述の問題を解消し、マスタキーを消去しなくても、安全にスレーブデバイスを交換可能とする相互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

[0007] 本発明の相互認証システムは、相互に認証するマスタデバイスとスレーブデバイスとを備える相互認証システムであって、前記マスタデバイスは、一時的に用いられる鍵データであるテンポラリキー、及び認証に用いられる鍵データであるマスタキーを格納する記憶部と、前記マスタキーを前記スレーブデバイスが格納しているか問い合わせる鍵確認部と、前記鍵確認部の問い合わせの応答において、前記スレーブデバイスが前記マスタキーを格納していない場合、前記テンポラリキーにて、前記マスタキーを暗号化して前記スレーブデバイスに送信する鍵導入部と、前記鍵導入部により送信された前記マスタキーにて、前記スレーブデバイスとの間で相互認証する主認証部とを備え、前記スレーブデバイスは、前記テンポラリキーを格納する記憶部と、前記マスタデバイスからの問い合わせに対して、前記記憶部にマスタキーが既に格納されているか確認して応答する鍵確認応答部と、前記鍵確認応答部の応答に対して、前記マスタデバイスから送信された前記マスタキーを前記テンポラリキーで復号化して前記記憶部に格納する鍵格納部と、前記鍵格納部により前記記憶部に格納された前記マスタキーにて、前記マスタデバイスとの間で相互認証する副認証部とを備えることを特徴とする。

このように構成することで、マスタキーを消去しなくても、安全にスレーブデバイスを交換することができる。

[0008] 本発明の相互認証システムは、前記マスタデバイスは、初期起動した際に

、乱数を用いて前記マスタキーを生成し、前記記憶部に格納する鍵生成部を更に備えることを特徴とする。

このように構成することで、工場出荷時等において、マスタデバイスを初期起動した際に、デバイスユニークな鍵データを安全に生成することができる。

[0009] 本発明の相互認証システムは、前記鍵確認部は、特定タイミングで、前記スレーブデバイスが前記マスタキーを格納しているか問い合わせることを特徴とする。

このように構成することで、不正ヘッド等が取り付けられたことを、検知することができる。

[0010] 本発明の相互認証システムは、前記主認証部及び前記副認証部による相互認証には、対称鍵暗号方式を用いることを特徴とする。

このように構成することで、相互認証に係る処理速度を向上させることができ、安価な制御部をもつ装置で相互認証ができる。

[0011] 本発明の相互認証方法は、相互に認証するマスタデバイスとスレーブデバイスとを備える相互認証システムにより実行される相互認証方法であって、前記マスタデバイスは、一時的に用いられる鍵データであるテンポラリキー、及び認証に用いられる鍵データであるマスタキーを格納する記憶部を備え、前記スレーブデバイスは、前記テンポラリキーを格納する記憶部を備え、前記マスタデバイスにより、前記マスタキーを前記スレーブデバイスが格納しているか問い合わせ、前記スレーブデバイスにより、前記マスタデバイスからの問い合わせに対して、前記記憶部にマスタキーが既に格納されているか確認して応答し、前記マスタデバイスにより、問い合わせの応答において、前記スレーブデバイスが前記マスタキーを格納していない場合、前記テンポラリキーにて、前記マスタキーを暗号化して前記スレーブデバイスに送信し、前記スレーブデバイスにより、応答に対して、前記マスタデバイスから送信された前記マスタキーを前記テンポラリキーで復号化して前記記憶部に格納し、前記マスタキーにて、前記マスタデバイス及び前記スレーブデバイ

スとの間で相互認証することを特徴とする。

このように構成することで、マスタキーを消去しなくても、安全にスレーブデバイスを交換することができる。

発明の効果

[0012] 本発明によれば、マスタデバイスのマスタキーを変更せず、交換後のスレーブデバイスにマスタキーを格納しているか問い合わせ、格納していなければ、テンポラリキーを用いてマスタキーを暗号化してスレーブデバイスに送信し、これをスレーブデバイスにて格納することで、マスタキーを消去しなくても、安全にスレーブデバイスを交換することができる相互認証システムを提供することができる。

図面の簡単な説明

[0013] [図1]本発明の実施の形態に係る相互認証システムのシステム構成図である。

[図2]本発明の実施の形態に係る相互認証処理のフローチャートである。

[図3]図2に示す相互認証処理におけるスレーブデバイス交換時のシーケンスチャートである。

[図4]従来の相互認証システムの新規組み込み時のシーケンスチャートである。

[図5]従来の相互認証システムにおいて、スレーブデバイス交換時（消去なし）を行った場合のシーケンスチャートである。

[図6]従来の相互認証システムのスレーブデバイス交換時（マスタキー消去）のシーケンスチャートである。

発明を実施するための形態

[0014] <実施の形態>

図1を参照して、本発明の実施の形態に係る相互認証システムであるカードリーダー1の構成について説明する。

カードリーダー1は、本実施形態においては、カード発行機能を備えたATM (Automated Teller Machine)、キオスク (Kiosk) の端末、交通機関のチケット発行システム、コンビニエンスストア等のポイントカード発行システ

ム、小売店のメンバーカード発行システム、遊技機のカード発行、支払システム、入退場管理システム等（以下、単に「ＡＴＭ等」と省略して記載する。）に搭載されるカードリーダである。

[0015] 具体的には、カードリーダ１は、接触型又は非接触型のＩＣカード及び／又は磁気ストライプを備えた磁気カードであるカード媒体２を読み込み（リード）又は書き込み（ライト）可能な装置である。

カードリーダ１の詳細な構成については後述する。

[0016] さらに、カードリーダ１は、ＡＴＭ等の各機能を実現するための本体装置である上位装置と接続される。この上位装置は、例えば、各部の制御用のＰＣ（Personal Computer）、タブレット端末、携帯電話等の情報処理装置を含み、ＡＴＭ等の機能を実現するためのアプリケーション（Application Program、図示せず）を実行する。加えて、上位装置には、カード媒体２の表面に印刷や刻印を行うプリンタ、ＬＣＤパネルや有機ＥＬパネル等のディスプレイ、タッチパネル、及びボタン等の周辺装置が接続されている。

[0017] より具体的に説明すると、カードリーダ１は、相互に認証するマスタデバイス１０とスレーブデバイス２０とを備える。

[0018] マスタデバイス１０は、カードリーダ１としての一般的な処理を行い、カード媒体２に対する情報の書き込みと読み出しを制御するメイン処理装置である。マスタデバイス１０は、例えば、カードリーダ１全体を制御するメイン（主）基板上の各種回路として構成される。本実施形態において、マスタデバイス１０は、接続されたスレーブデバイス２０を通信により制御する。

[0019] スレーブデバイス２０は、暗号磁気ヘッド（Encrypting Head、E-Head）等である。この暗号磁気ヘッドは、復調した磁気データを暗号化して、安全に制御部１１及び上位装置に送信する。このため、スレーブデバイス２０は、磁気ヘッド２３により読み取られた情報を暗号化又は復号化し、情報を暗号化又は復号化して磁気ヘッド２３によりカード媒体２に記録させる機能を実現する。このため、スレーブデバイス２０は、例えば、カード媒体２に記憶されたＩＤ、暗証番号、パスワード等のデータの詐取を防御するためのデー

タ暗号化機能、復号化機能等を備えている。加えて、本実施形態のスレーブデバイス20は、セキュリティのため、特定の処理手順を遵守して制御しないと処理を実行しないよう構成されている。

[0020] さらに詳細に説明すると、マスタデバイス10は、制御部11及び記憶部12を備えている。スレーブデバイス20は、制御部21、記憶部22、及び磁気ヘッド23を備えている。

[0021] 制御部11は、カードリーダ1全体の処理を行うCPU (Central Processing Unit)、MPU (Micro Processing Unit)、GPU (Graphics Processing Unit)、DSP (Digital Signal Processor)、ASIC (Application Specific Integrated Circuit) 等を含む制御演算手段である。

[0022] 記憶部12は、RAM (Random Access Memory) 及びROM (Read Only Memory) 等の記憶媒体である。RAMは、例えば、SRAM (Static RAM)、DRAM (Dynamic RAM) 等の揮発性の記録媒体、FeRAM (Ferroelectric Random Access Memory)、MRAM (Magnetoresistive Random Access Memory) 等の不揮発性の記録媒体等である。ROMは、例えば、EEPROM (Electrically Erasable and Programmable ROM)、フラッシュメモリ (Flash Memory) 等の不揮発性の記録媒体である。

記憶部12は、マスタデバイス10に実装されている制御部11の制御プログラム(組み込みソフトウェア)を格納している。この制御用プログラムは、カード媒体2の検知用のセンサの監視、カード媒体2のリード、ライト、スレーブデバイス20の制御等の処理が組み込まれている。本実施形態において、記憶部12は、例えば、制御部11の内蔵メモリとして構成される。

[0023] 制御部21は、スレーブデバイス20の状態監視及び制御を行うCPU、MPU、GPU、DSP、ASIC等を含む制御演算手段である。制御部21は、情報の暗号処理や暗号を利用した認証等の処理を実行する。具体的には、制御部21は、例えば、AES (Advanced Encryption Standard) 等の方式で、各種暗号化や復号化を行う制御プログラムを実行し、演算を専用に

実行するアクセラレータ (Accelerator) を含むこともある。

[0024] 記憶部 22 は、RAM 及び ROM 等の一時的でない記憶媒体である。記憶部 22 は、記憶部 12 と同様に、揮発性及び不揮発性の記録媒体を含んでいる。

記憶部 22 は、スレーブデバイス 20 に実装されている制御部 21 の制御プログラム (組み込みソフトウェア) を格納している。本実施形態において、記憶部 22 は、例えば、制御部 21 の内蔵メモリとして構成される。

[0025] 磁気ヘッド 23 は、カード媒体 2 へのリード (読み出し)、ライト (書き込み) を行う磁気ヘッドや電磁誘導コイルや端子等と、このための回路等を含む。加えて、磁気ヘッド 23 は、カード媒体 2 の検知用のセンサ、駆動機構等も含むこともある。

[0026] ここで、カードリーダ 1 の機能構成について説明する。

図 1 は、マスタデバイス 10 が初期起動した後、スレーブデバイス 20 が消耗、故障、規格変更等により、交換される際 (交換時) の状態を示している。この交換時の状態において、スレーブデバイス 20 は、例えば、工場出荷された補修用部品 (新品) 等として提供される。

[0027] マスタデバイス 10 の制御部 11 は、機能構成部として、鍵確認部 100、鍵導入部 110、主認証部 120、及び鍵生成部 130 を備えている。

記憶部 12 は、マスタキー 300 及びテンポラリキー 310 を格納している。

スレーブデバイス 20 の制御部 21 は、機能構成部として、鍵確認応答部 200、鍵格納部 210、及び副認証部 220 を備えている。

記憶部 22 は、テンポラリキー 310 を格納している。

[0028] 鍵確認部 100 は、記憶部 12 に格納されたのと同様のマスタキー 300 をスレーブデバイス 20 が格納しているか問い合わせる。この際、鍵確認部 100 は、特定タイミングで、スレーブデバイス 20 がマスタキー 300 を格納しているか問い合わせる。この特定タイミングは、例えば、電源オン時等のタイミングである。

- [0029] 鍵導入部 110 は、鍵確認部 100 の問い合わせの応答において、スレーブデバイス 20 がマスタキー 300 を格納していない場合、テンポラリキー 310 にて、マスタキー 300 を暗号化してスレーブデバイス 20 に送信する。これにより、鍵導入部 110 は、マスタキー 300 を消去することなく、スレーブデバイス 20 の交換等を認識して、交換前に生成されたマスタキー 300 をスレーブデバイス 20 に導入可能となる。
- [0030] 主認証部 120 は、鍵導入部 110 により送信されたマスタキー 300 にて、スレーブデバイス 20 との間で相互認証する。本実施形態において、主認証部 120 は、副認証部 220 との間で相互認証を行う。本実施形態においては、この相互認証は、マスタキー 300 を用いる対称鍵暗号方式にて行われる。
- [0031] 鍵生成部 130 は、マスタデバイス 10 が初期起動した際に、乱数を用いてマスタキー 300 を生成し、記憶部 12 の不揮発性の記録媒体に格納する。この初期起動は、例えば、工場出荷の検査時、顧客環境に設置された際の最初の電源投入時等（以下、「工場出荷時等」という。）に行われる。
- [0032] 鍵確認応答部 200 は、マスタデバイス 10 からの問い合わせに対して、記憶部 22 にマスタキー 300 が既に格納されているか否かについて確認して応答する。
- [0033] 鍵格納部 210 は、鍵確認応答部 200 の応答に対して、マスタデバイス 10 から送信されたマスタキー 300 をテンポラリキー 310 で復号化して記憶部 22 に格納する。
- [0034] 副認証部 220 は、鍵格納部 210 により記憶部 22 に格納されたマスタキー 300 にて、マスタデバイス 10 との間で相互認証する。本実施形態において、副認証部 220 は、主認証部 120 との間で、マスタキー 300 を用いる対称鍵暗号方式にて、相互認証を行う。
- [0035] マスタキー 300 は、認証に用いられる鍵データである。本実施形態において、マスタキー 300 は、例えば、対称鍵の鍵データである。この対称鍵は、カードリーダ 1 毎に個別ものが提供される（以下、「デバイスユニーク

」という。)になるよう、ANSI X9.17等の規格で生成される乱数値を用いることが可能である。

[0036] テンポラリキー310は、一時的に用いられる鍵データである。テンポラリキー310は、例えば、対称鍵であり、機種毎に共通な鍵データである。テンポラリキー310も、例えば、対称鍵の鍵データである。

[0037] ここで、制御部11は、記憶部12に格納された制御プログラムを実行することで、鍵確認部100、鍵導入部110、主認証部120、及び鍵生成部130として機能させられる。

制御部21は、記憶部22に格納された制御プログラムを実行することで、鍵確認応答部200、鍵格納部210、及び副認証部220として機能させられる。

また、上述のカードリーダ1の各部は、本発明の情報処理方法を実行するハードウェア資源となる。

なお、上述の機能構成部の一部又は任意の組み合わせをICやプログラマブルロジックやFPGA (Field-Programmable Gate Array) 等でハードウェア的に構成してもよい。

[0038] [カードリーダによる相互認証処理]

次に、図2及び図3により、本発明の実施の形態に係るカードリーダ1により実行される相互認証処理の説明を行う。

本実施形態の相互認証処理では、マスタデバイス10は、マスタキー300をスレーブデバイス20が格納しているか問い合わせる。この問い合わせに対して、スレーブデバイス20は、記憶部22にマスタキー300が既に格納されているか確認して応答する。問い合わせの応答において、スレーブデバイス20がマスタキー300を格納していない場合、マスタデバイス10は、テンポラリキー310にて、マスタキー300を暗号化してスレーブデバイス20に送信する。スレーブデバイス20は、応答に対して、マスタデバイス10から送信されたマスタキー300をテンポラリキー310で復号化して記憶部22に格納する。そして、マスタデバイス10及びスレーブ

デバイス 20 は、このマスタキー 300 にて相互認証する。

本実施形態の相互認証処理は、主にマスタデバイス 10 の制御部 11 及びスレーブデバイス 20 の制御部 21 が、それぞれ、記憶部 12 及び記憶部 22 に格納された制御プログラムを実行することで、各部と協同し、ハードウェア資源を用いて実行する。

以下で、図 2 のフローチャートにより、相互認証処理の詳細をステップ毎に説明する。

[0039] (ステップ S 101)

まず、マスタデバイス 10 の処理について説明する。

鍵生成部 130 は、起動時等に、マスタキー 300 が記憶部 12 に格納されているか否かを確認する。

鍵生成部 130 は、マスタキー 300 が記憶部 12 に既に格納されている場合には、Yes と判断する。鍵生成部 130 は、マスタデバイス 10 が工場出荷時等において初期起動し、まだマスタキー 300 が記憶部 12 に格納されていない等の場合には、No と判断する。

Yes の場合、鍵生成部 130 は、処理をステップ S 103 に進める。

No の場合、鍵生成部 130 は、処理をステップ S 102 に進める。

[0040] (ステップ S 102)

マスタキー 300 が記憶部 12 に格納されていない場合、鍵生成部 130 が、マスタキー生成格納処理を行う。

ここで、本実施形態においては、初期起動時には、記憶部 12 は、鍵データとしてテンポラリキー 310 のみが格納されている。

このため、鍵生成部 130 は、初期起動の際に、乱数を用いてマスタキー 300 を生成し、記憶部 12 の不揮発性の記録媒体に格納する。このマスタキー 300 の生成について、鍵生成部 130 は、例えば、ANSI X9.17 等の規格で生成される乱数値を用いる。

すなわち、本実施形態においては、初期起動時に、デバイスユニークなマスタキー 300 が生成される。この初期起動は、例えば、工場出荷の検査の

際等に行われるため、セキュリティ性の高い場所で行われる。

図 1 は、この状態の記憶部 12 の構成を示している。

[0041] (ステップ S 103、S 201)

ここで、マスタデバイス 10 の鍵確認部 100 及びスレーブデバイス 20 の鍵確認応答部 200 が、マスタキー確認処理を行う。

[0042] まず、鍵確認部 100 は、電源オンの度に、スレーブデバイス 20 がマスタキー 300 を格納しているか問い合わせる。この際に、鍵確認部 100 は、スレーブデバイス 20 に確認コマンド等を送信する (タイミング T 1)。

[0043] これに対して、鍵確認応答部 200 は、マスタデバイス 10 からの問い合わせに対して、記憶部 22 にマスタキー 300 が既に格納されているか確認して応答する (タイミング T 2)。

図 1 に示すように、スレーブデバイス 20 の交換時には、テンポラリキー 310 のみが格納されており、マスタキー 300 は格納されていない。この場合、鍵確認応答部 200 は、まだ格納されていない旨を応答する。

しかしながら、例えば、通常に電源をオンした場合や、既にマスタキー 300 を受け取って格納した場合、中古のスレーブデバイス 20 である場合等の場合、マスタキー 300 が既に記憶部 22 に格納されていることもあり得る。このように、マスタキー 300 が既に記憶部 22 に格納されている場合、鍵確認応答部 200 は、その旨を応答する。

[0044] (ステップ S 104)

次に、マスタデバイス 10 の鍵導入部 110 が、スレーブデバイス 20 にマスタキー 300 が格納されているか否かを判断する。

鍵導入部 110 は、スレーブデバイス 20 から、既に格納されている旨の応答を取得した場合には、Y e s と判断する。鍵導入部 110 は、まだ格納されていない旨の応答を取得した場合には、N o と判断する。

Y e s の場合、鍵導入部 110 は、処理をステップ S 106 に進める。

N o の場合、鍵導入部 110 は、処理をステップ S 105 に進める。

[0045] (ステップ S 105)

スレーブデバイス２０においてマスタキー３００が格納されていない場合、鍵導入部１１０が、マスタキー送信処理を行う。

鍵導入部１１０は、テンポラリキー３１０にて、マスタキー３００を暗号化してスレーブデバイス２０に送信する。具体的には、鍵導入部１１０は、例えば、記憶部１２に格納されたマスタキー３００を読み出し、ＡＥＳ等の方式を用いて、テンポラリキー３１０を鍵データとしてマスタキー３００を暗号化する。そして、鍵導入部１１０は、暗号化されたマスタキー３００を、スレーブデバイス２０へ鍵導入用コマンドを用いて送信する（タイミングＴ３）。

[0046] (ステップＳ２０２)

ここで、スレーブデバイス２０の処理について説明する。

鍵確認応答部２００は、鍵導入用コマンドを受信すると、マスタキー３００が記憶部２２に格納されているか否かを判断した結果により処理を分岐する。この判断においては、鍵確認応答部２００は、マスタキー３００が記憶部２２に格納されている場合に、Ｙｅｓと判断する。鍵確認応答部２００は、マスタキー３００が記憶部２２に格納されていない場合には、Ｎｏと判断する。

Ｙｅｓの場合、鍵確認応答部２００は、処理をステップＳ２０４に進める。

Ｎｏの場合、鍵確認応答部２００は、処理をステップＳ２０３に進める。

[0047] (ステップＳ２０３)

マスタキー３００が記憶部２２に格納されていない場合、鍵格納部２１０が、マスタキー格納処理を行う。

鍵格納部２１０は、鍵確認応答部２００の応答に対して、マスタデバイス１０から送信された、暗号化されたマスタキー３００を、マスタデバイス１０から受信する。

鍵格納部２１０は、受信した暗号化されたマスタキー３００を、テンポラリキー３１０で復号化し、記憶部２２に格納する。

鍵格納部 210 は、この格納が成功した場合、その旨をマスタデバイス 10 に返信する（タイミング T4）。

[0048] （ステップ S106、S204）

ここで、マスタデバイス 10 の主認証部 120 と、スレーブデバイス 20 の副認証部 220 が、相互認証処理を行う。

この処理では、マスタデバイス 10 の主認証部 120 と、スレーブデバイス 20 の副認証部 220 とが、マスタキー 300 を用いて相互認証する。具体的には、主認証部 120 は、記憶部 12 に格納されたマスタキー 300 にて、スレーブデバイス 20 との間で相互認証する。また、副認証部 220 は、鍵格納部 210 により記憶部 22 に格納されたマスタキー 300 にて、マスタデバイス 10 との間で相互認証する（タイミング T5、T6）。

この相互認証は、例えば、特許文献 2 に記載されたような方式で行うことが可能である。より具体的には、例えば、主認証部 120 と副認証部 220 が、それぞれ乱数値を作成してマスタキー 300 で暗号化し、これらをお互いに送受信した後、合計値を求めることで確認する。

ここでは、主認証部 120 は、スレーブデバイスからの返信の内容を確認して、相互認証が成功したか、失敗したかを判断する（タイミング T7）。主認証部 120 は、認証が成功した場合に、その旨を記憶部 12 の記録媒体に格納する。

以上により、本発明の実施の形態に係る相互認証処理を終了する。

[0049] [本実施形態の主な効果]

以上のように構成することで、以下のような効果を得ることができる。

上述したように、特許文献 1 に記載されたような従来のカードリーダーでは、スレーブデバイスが交換された際に、マスタキーを消去する必要があった。

[0050] ここで、図 4～図 6 を参照して、典型的なカードリーダーによる相互認証の例について説明する。

図 4 は、マスタデバイスとスレーブデバイスにおいて、工場等における製

造、検査時に、最初（初回）に起動され、相互認証をする場合の認証シーケンスを示す。マスタデバイスとスレーブデバイスは、それぞれ共通のテンポラリキーを格納している。まず、マスタデバイスにおいて、マスタキーを生成する（タイミングT1-2）。この例では、マスタキーは、カードリーダー毎にユニーク（デバイスユニーク）となる。そして、マスタデバイスは、テンポラリキーを用いて、マスタキーを送信し、スレーブデバイスに導入させる（タイミングT2-2）。スレーブデバイスは、成功返信を行う（タイミングT3-2）。その後、マスタデバイスは、マスタキーによる相互認証を行う（タイミングT4-2）。これに対して、スレーブデバイスは、返信を行う（タイミングT5-2）。マスタデバイスは、スレーブデバイスからの返信の内容を確認して、相互認証が成功したか、失敗したかを判断する（タイミングT6-2）。

[0051] 図5は、スレーブデバイスの交換時に、仮にマスタキーを消去せずに、そのまま相互認証をしようとした場合のシーケンスを示す。

典型的なカードリーダーにおいて、マスタキーはデバイスユニークである。このため、マスタデバイスからマスタキーによる相互認証を行うと（タイミングT4-3）、スレーブデバイスからの返信（タイミングT5-3）をマスタデバイスが判定して、相互認証が失敗する（タイミングT6-3）。これは、交換時にはスレーブデバイスに交換後のマスタキーが格納されていないため、「マスタキーが異なる」とマスタデバイスが判断するためである。

さらに、既にマスタキーが格納された中古のスレーブデバイス、不正なスレーブデバイス等に交換された場合も、相互認証が失敗し、使用が禁止される。

[0052] 図6は、典型的なカードリーダーにおいて、図4の初回の相互認証が行われた後の状態における、スレーブデバイス交換時のシーケンスを示す。このように、典型的なカードリーダーでは、マスタキーがカードリーダー毎にユニークのため、相互認証の前に、最初にマスタキーを消去する手順が必要となる（タイミングT0-4）。その後は、上述の図4と同様の手順で相互認証が行

われる（タイミングT1-4～T6-4）。

このように、暗号機能対応のセキュリティ製品であるスレーブデバイスの交換時には、相互認証のため、マスタキーをいったん消去する必要がある。このようにマスタキーを消去する際には、セキュリティ上の懸念があるため、例えば、安全な環境（セキュリティルーム等）で行わなければならなかった。

[0053] これに対して、本発明の実施の形態に係るカードリーダ1は、相互に認証するマスタデバイス10とスレーブデバイス20とを備える相互認証システムであって、マスタデバイス10は、一時的に用いられる鍵データであるテンポラリキー310、及び認証に用いられる鍵データであるマスタキー300を格納する記憶部12と、記憶部12に格納されたのと同様のマスタキー300をスレーブデバイス20が格納しているか問い合わせる鍵確認部100と、鍵確認部100の問い合わせの応答において、スレーブデバイス20がマスタキー300を格納していない場合、テンポラリキー310にて、マスタキー300を暗号化してスレーブデバイス20に送信する鍵導入部110と、鍵導入部110により送信されたマスタキー300にて、スレーブデバイス20との間で相互認証する主認証部120とを備え、スレーブデバイス20は、テンポラリキー310を格納する記憶部22と、マスタデバイス10からの問い合わせに対して、記憶部22にマスタキー300が既に格納されているか確認して応答する鍵確認応答部200と、鍵確認応答部200の応答に対して、マスタデバイス10から送信されたマスタキー300をテンポラリキー310で復号化して記憶部22に格納する鍵格納部210と、鍵格納部210により記憶部22に格納されたマスタキー300にて、マスタデバイス10との間で相互認証する副認証部220とを備えることを特徴とする。

[0054] このように構成し、カードリーダ1は、マスタキー300は変更せず、交換後のスレーブデバイス20にマスタキー300の有無を確認し、なければ、テンポラリキー310を用いてマスタキー300を導入する。これにより

、マスタデバイス１０は、マスタキー３００を消去せずにスレーブデバイス２０に対してマスタキー３００の導入を行い、相互認証を成功させることができる。結果として、高度なセキュリティが求められる暗号磁気ヘッド等のスレーブデバイス２０を安全に交換可能となり、セキュリティ性の高い状態や場所等を確保することなく、従来よりもセキュリティ性を高めることができる。

[0055] また、上述したように、マスタキーの消去にはセキュリティ上の懸念があり、安全な環境で行わなければならなかった。このように安全な環境を構築するためには労力やコストがかかっていた。

本実施形態のカードリーダー１は、このように安全な環境がない場合であっても、セキュリティ性が高い状態で相互認証が可能となり、労力やコストを低減できる。さらに、サービスパーソンが、ＡＴＭ等の修理現場で、直接、暗号磁気ヘッド等を交換して、稼働させることが可能となるため、メンテナンスの労力やコストも削減できる。

[0056] 本発明の実施の形態に係るカードリーダー１は、マスタデバイス１０にて、初期起動した際に、乱数を用いてマスタキー３００を生成し、記憶部１２に格納する鍵生成部１３０を更に備えることを特徴とする。

このように構成することで、工場出荷時等において、マスタデバイス１０を初期起動した際に、デバイスユニークな鍵データを安全に生成することが可能となる。

[0057] 本発明の実施の形態に係るカードリーダー１は、鍵確認部１００が、特定タイミングで、スレーブデバイス２０がマスタキー３００を格納しているか問い合わせることを特徴とする。

このように構成し、マスタデバイス１０は、電源オン時等の特定タイミングで、スレーブデバイス２０がマスタキー３００を格納しているか問い合わせる。これにより、不正ヘッド等が取り付けられたことを、検知することが可能となる。

[0058] 本発明の実施の形態に係るカードリーダー１は、主認証部１２０及び副認証

部 2 2 0 による相互認証には、対称鍵暗号方式を用いることを特徴とする。

このように構成し、R S Aのような非対称鍵暗号を使用せず、A E Sのような対称鍵暗号のみで認証を行うことで、相互認証に係る処理速度を向上させることができる。結果として、安価なC P Uでも相互認証が実現可能となる。

[0059] 〔他の実施の形態〕

なお、上述の実施の形態においては、相互認証システムの一例として、マスタデバイス 1 0 及びスレーブデバイス 2 0 を含むカードリーダー 1 を用いる構成について説明した。

しかしながら、本発明の他の実施の形態に係る相互認証システムは、カードリーダーと上位装置との間で相互認証を行うような相互認証システムとして構成することも可能である。加えて、カードリーダーにおいて、スレーブデバイス 2 0 も 1 つに限らず複数あってもよい。この場合、スレーブデバイス 2 0 として暗号 I C ブロックを用いるような構成も可能である。さらに、カードリーダー以外の相互認証を行うセキュリティ製品を含む相互認証システムを構成することも可能である。このセキュリティ製品としては、例えば、カードプリンタ、カード発行装置、その他のカード関連の装置、A T M 等の本体等が含まれていてもよい。また、スマートフォン等の携帯端末、P C (Personal Computer)、家電製品、自動車等の各種情報処理装置をマスタデバイス又はスレーブデバイスとして含む相互認証システムを構成することも可能である。

このように構成することで、様々な構成に対応した相互認証が可能となる。

[0060] また、上述の実施の形態においては、マスタデバイス 1 0 にてマスタキー 3 0 0 が生成される例について記載した。しかしながら、このマスタキー 3 0 0 は、上位装置から送信して導入させたり、別途、製造時にデバイスユニークな鍵データを導入させたりして、記憶部 1 2 に格納させてもよい。

このように構成することで、装置毎に格納されたマスタキー 3 0 0 を管理

等することも可能となる。

[0061] また、上述の実施の形態においては、認証を行うために共通鍵（対称鍵）暗号方式のAESを用いる例について説明した。しかしながら、Triple DES等の暗号方式を用いることも可能である。また、制御部11、21の演算性能によっては、公開鍵暗号を用いることも可能である。

このように構成することで、カードリーダーの構成や規格上の要求等に合わせた適切な相互認証システムを提供可能となる。

[0062] なお、上記実施の形態の構成及び動作は例であって、本発明の趣旨を逸脱しない範囲で適宜変更して実行することができることは言うまでもない。

符号の説明

[0063] 1 カードリーダー
2 カード媒体
10 マスタデバイス
11、21 制御部
12、22 記憶部
20 スレーブデバイス
23 磁気ヘッド
100 鍵確認部
110 鍵導入部
120 主認証部
130 鍵生成部
200 鍵確認応答部
210 鍵格納部
220 副認証部
300 マスタキー
310 テンポラリキー

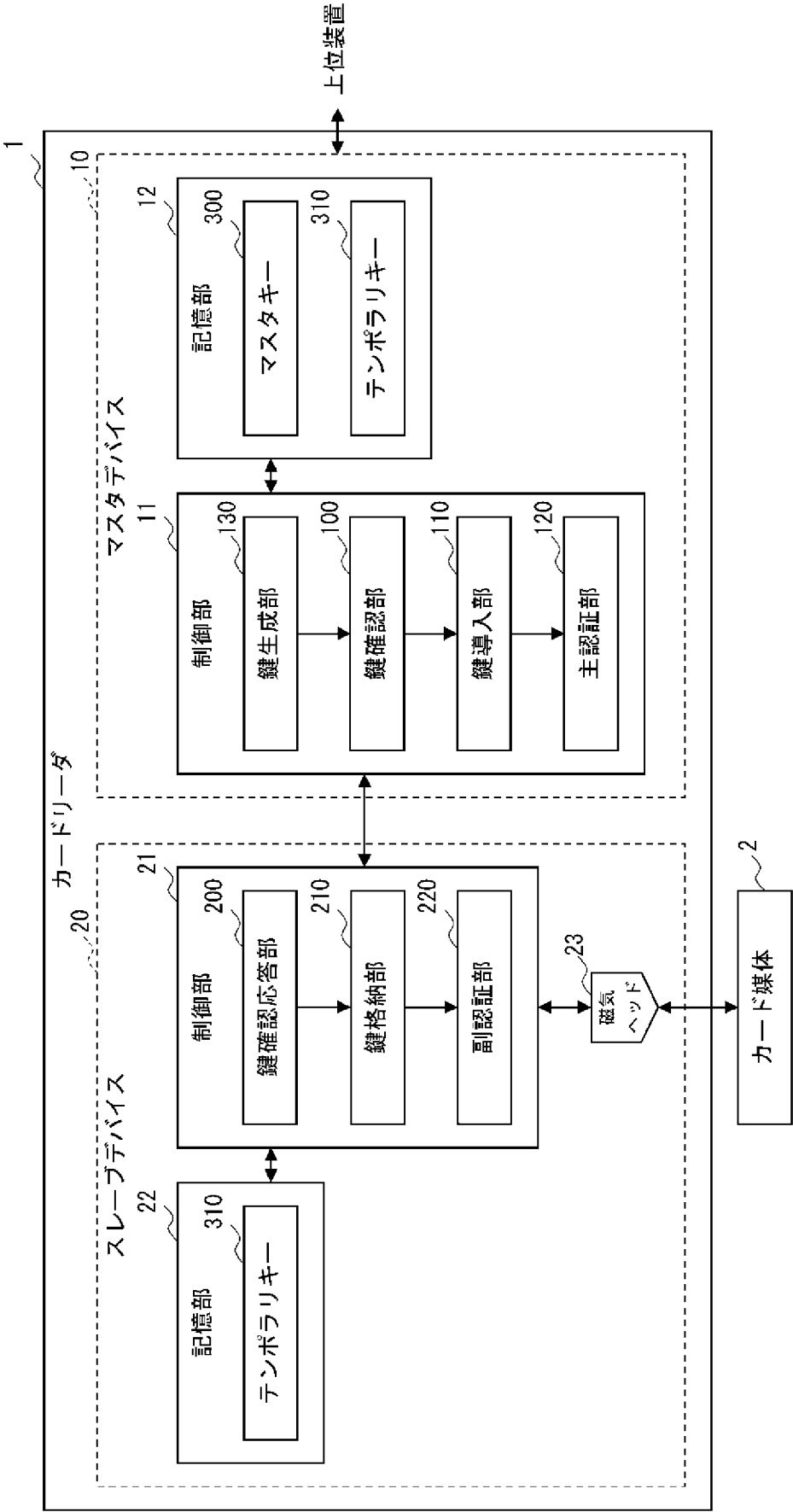
請求の範囲

- [請求項1] 相互に認証するマスタデバイスとスレーブデバイスとを備える相互認証システムであって、
- 前記マスタデバイスは、
- 一時的に用いられる鍵データであるテンポラリキー、及び認証に用いられる鍵データであるマスタキーを格納する記憶部と、
- 前記マスタキーを前記スレーブデバイスが格納しているか問い合わせる鍵確認部と、
- 前記鍵確認部の問い合わせの応答において、前記スレーブデバイスが前記マスタキーを格納していない場合、前記テンポラリキーにて、前記マスタキーを暗号化して前記スレーブデバイスに送信する鍵導入部と、
- 前記鍵導入部により送信された前記マスタキーにて、前記スレーブデバイスとの間で相互認証する主認証部とを備え、
- 前記スレーブデバイスは、
- 前記テンポラリキーを格納する記憶部と、
- 前記マスタデバイスからの問い合わせに対して、前記記憶部にマスタキーが既に格納されているか確認して応答する鍵確認応答部と、
- 前記鍵確認応答部の応答に対して、前記マスタデバイスから送信された前記マスタキーを前記テンポラリキーで復号化して前記記憶部に格納する鍵格納部と、
- 前記鍵格納部により前記記憶部に格納された前記マスタキーにて、前記マスタデバイスとの間で相互認証する副認証部とを備える
- ことを特徴とする相互認証システム。
- [請求項2] 前記マスタデバイスは、
- 初期起動した際に、乱数を用いて前記マスタキーを生成し、前記記憶部に格納する鍵生成部を更に備える
- ことを特徴とする請求項1に記載の相互認証システム。

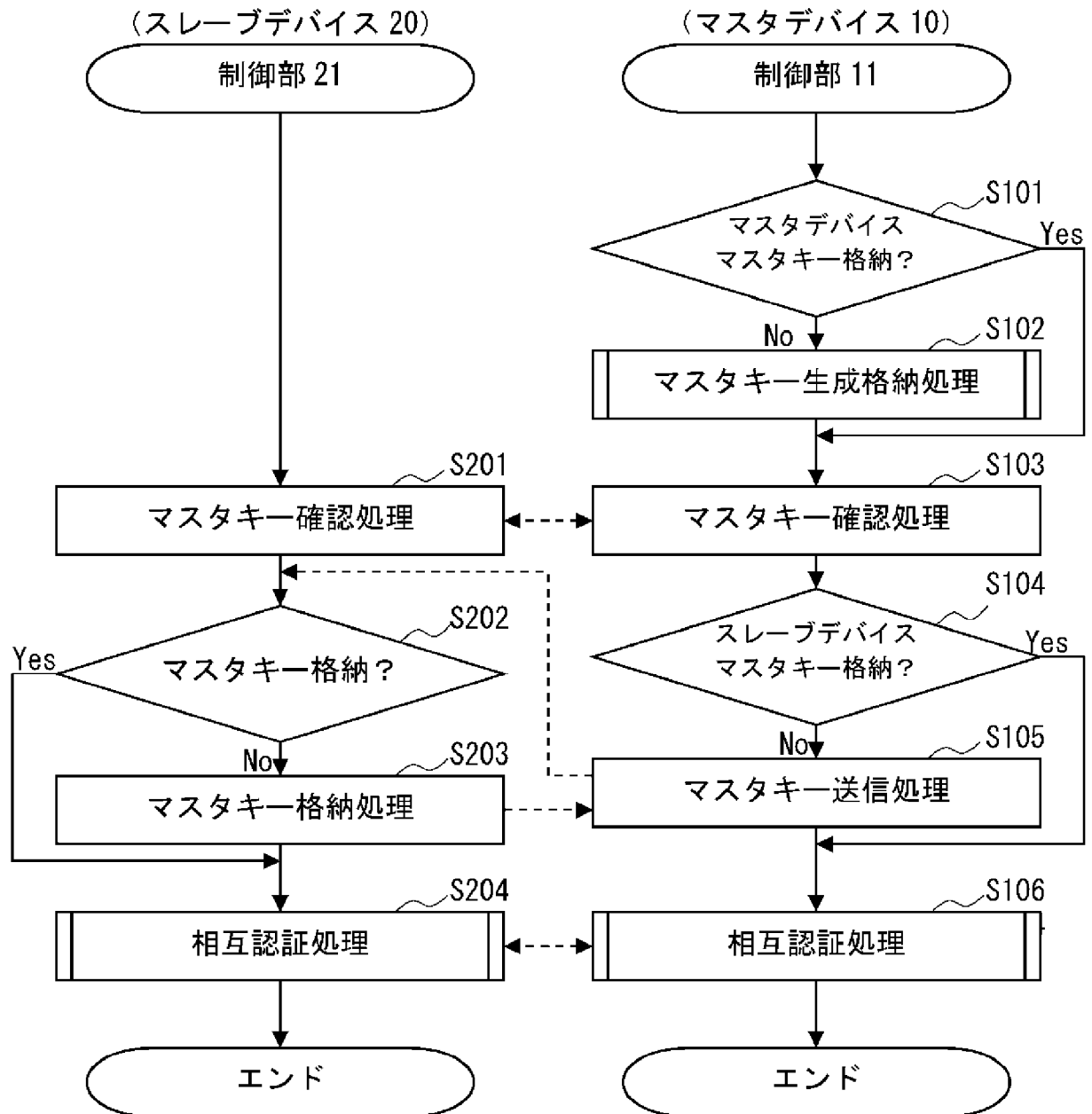
- [請求項3] 前記鍵確認部は、
特定タイミングで、前記スレーブデバイスが前記マスタキーを格納しているか問い合わせる
ことを特徴とする請求項1又は2に記載の相互認証システム。
- [請求項4] 前記主認証部及び前記副認証部による相互認証には、対称鍵暗号方式を用いる
ことを特徴とする請求項1乃至3のいずれか1項に記載の相互認証システム。
- [請求項5] 相互に認証するマスタデバイスとスレーブデバイスとを備える相互認証システムにより実行される相互認証方法であって、
前記マスタデバイスは、一時的に用いられる鍵データであるテンポラリキー、及び認証に用いられる鍵データであるマスタキーを格納する記憶部を備え、
前記スレーブデバイスは、前記テンポラリキーを格納する記憶部を備え、
前記マスタデバイスにより、前記マスタキーを前記スレーブデバイスが格納しているか問い合わせ、
前記スレーブデバイスにより、前記マスタデバイスからの問い合わせに対して、前記記憶部にマスタキーが既に格納されているか確認して応答し、
前記マスタデバイスにより、問い合わせの応答において、前記スレーブデバイスが前記マスタキーを格納していない場合、前記テンポラリキーにて、前記マスタキーを暗号化して前記スレーブデバイスに送信し、
前記スレーブデバイスにより、応答に対して、前記マスタデバイスから送信された前記マスタキーを前記テンポラリキーで復号化して前記記憶部に格納し、
前記マスタキーにて、前記マスタデバイス及び前記スレーブデバイ

スとの間で相互認証する
ことを特徴とする相互認証方法。

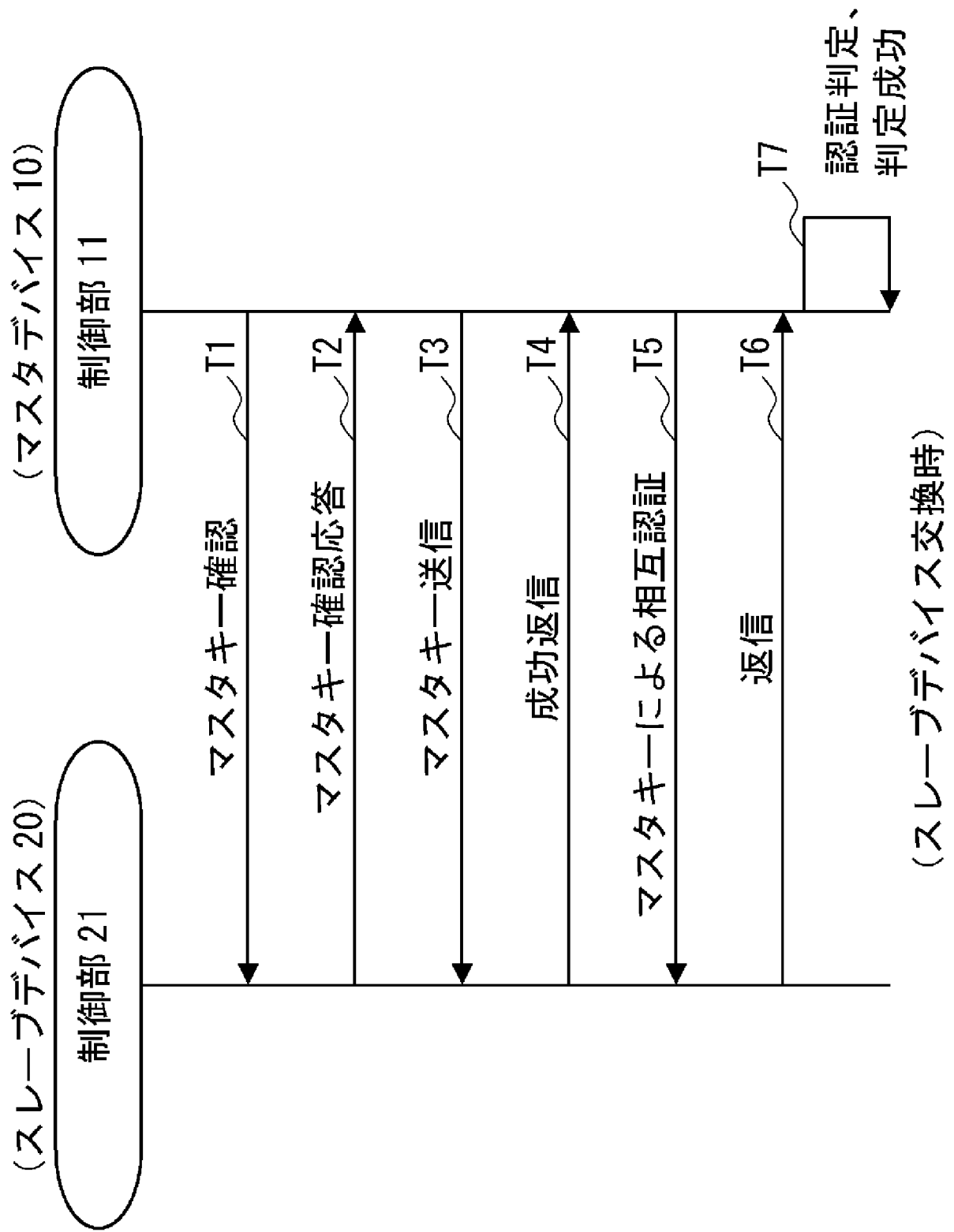
[図1]



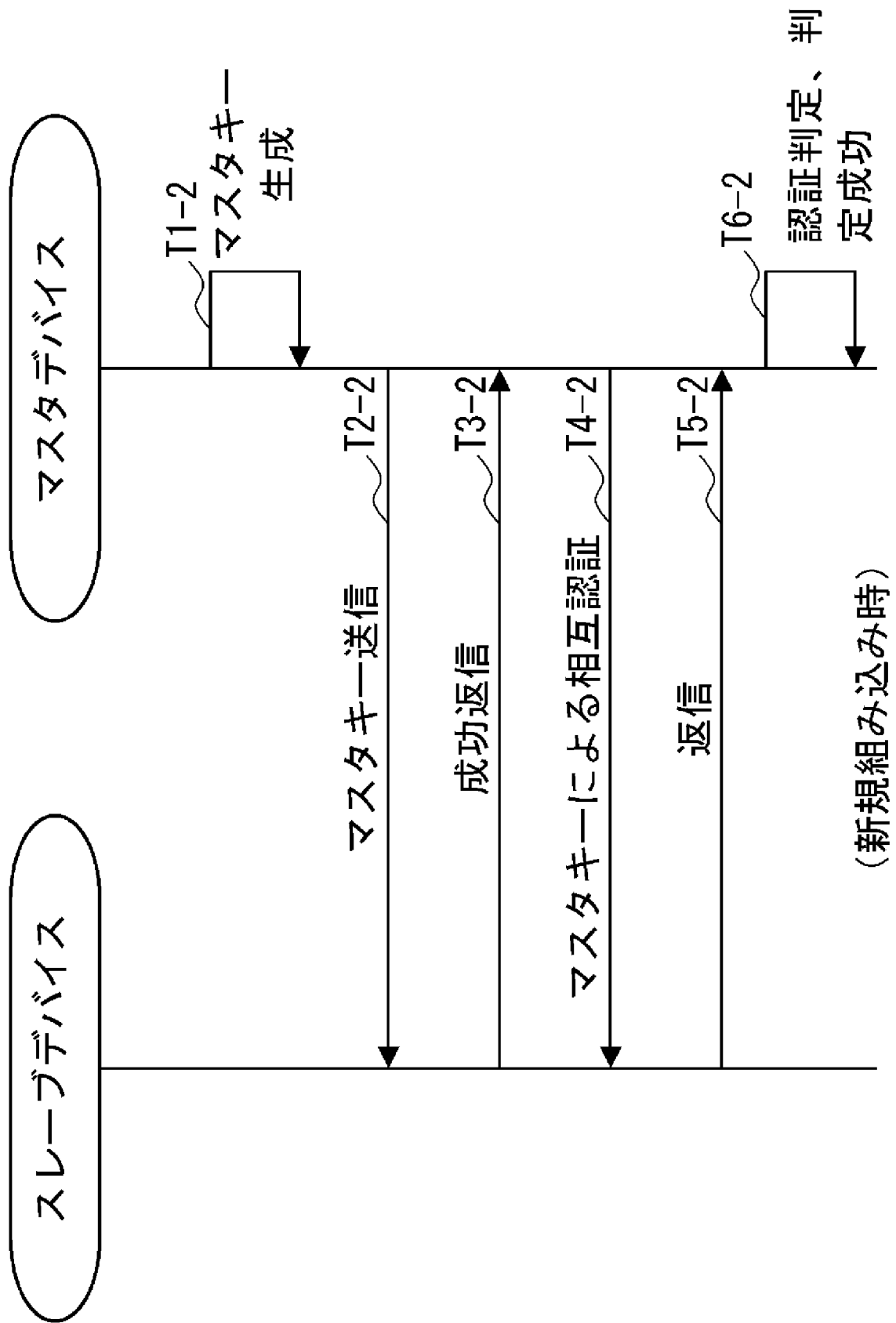
[図2]



[図3]



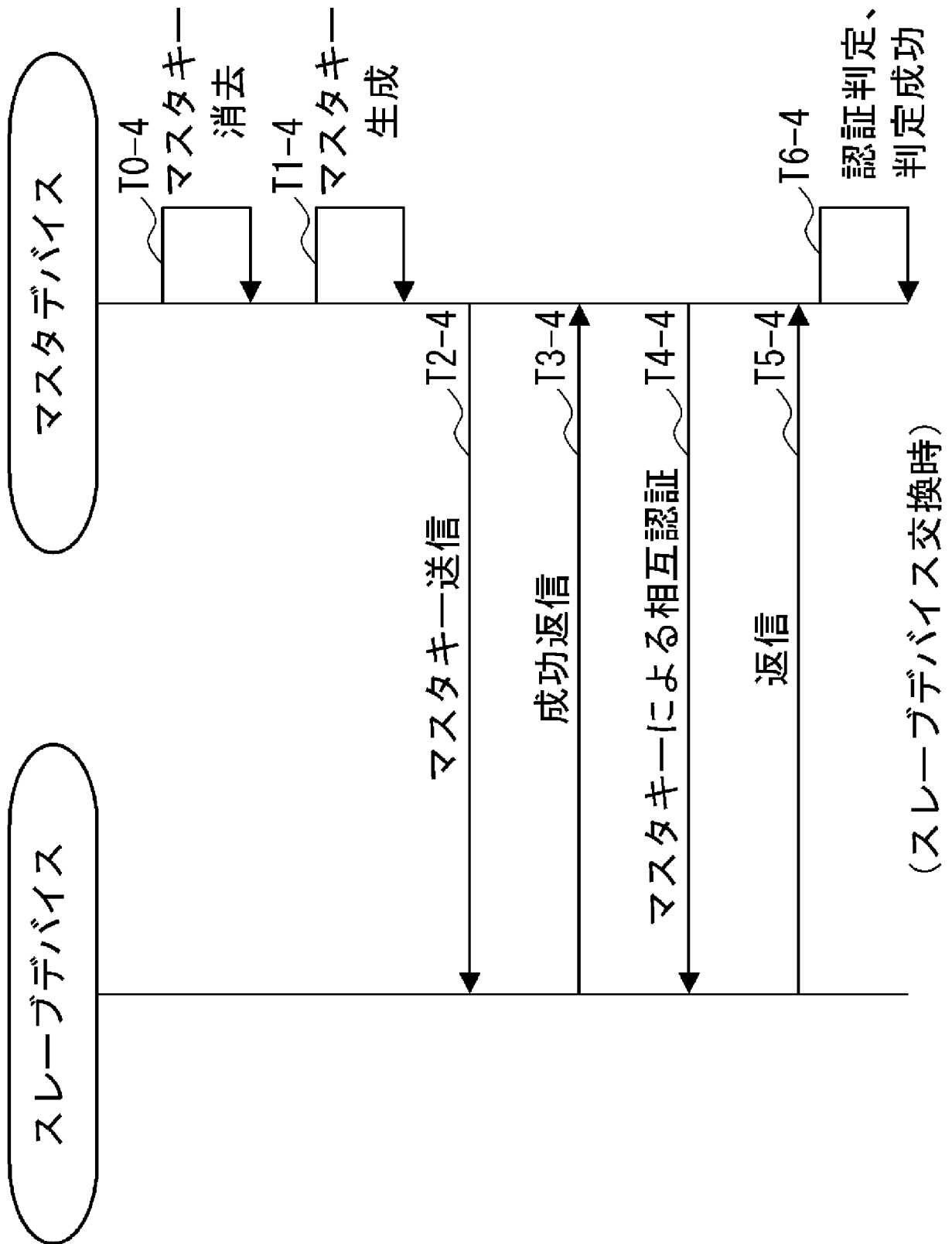
[図4]



```

sequenceDiagram
    participant Slave as スレーブデバイス
    participant Master as マスターデバイス
    Slave->>Master: マスターキーによる相互認証
    Master-->>Slave: 返信
    Slave->>Master: T4-3
    Master-->>Slave: T5-3
    Slave->>Master: T6-3
    Master-->>Slave: 認証判定、判定失敗
    Note over Slave, Master: (マスターキーを消去せずにスレーブデバイスを交換)
  
```

[図6]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/022534

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. H04L9/32 (2006.01) i, G06F21/44 (2013.01) i, G09C1/00 (2006.01) i, H04L9/08 (2006.01) 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, G09C1/00, H04L9/08

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	JP 2007-173911 A (OMRON CORP.) 05 July 2007, paragraphs [0019]-[0023], [0033]-[0044], fig. 1-3, 6-9 (Family: none)	1-5
A	JP 2016-116216 A (KDDI CORP.) 23 June 2016, paragraphs [0076]-[0084], fig. 9 & US 2017/0324558 A1, paragraphs [0142]-[0155], fig. 9 & EP 3232602 A1 & CN 107113167 A	1-5
A	JP 2008-271069 A (KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.) 06 November 2008, paragraphs [0010]-[0013], [0066], [0138] (Family: none)	1-5

☐ 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
25.07.2019

Date of mailing of the international search report
06.08.2019

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

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, G09C1/00(2006.01)i, H04L9/08(2006.01)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, G09C1/00, H04L9/08

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	JP 2007-173911 A (オムロン株式会社) 2007.07.05, 段落 [0019] - [0023], [0033] - [0044]、図1-3, 6-9 (ファミリーなし)	1-5
A	JP 2016-116216 A (KDDI株式会社) 2016.06.23, 段落 [0076] - [0084]、図9 & US 2017/0324558 A1, 段落[0142] - [0155], 図9 & EP 3232602 A1 & CN 107113167 A	1-5

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

25.07.2019

国際調査報告の発送日

06.08.2019

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

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)

打出 義尚

5 S

4440

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 2008-271069 A (コニカミノルタビジネステクノロジーズ株式会社) 2008.11.06, 段落 [0010] – [0013], [0066], [0138] (ファミリーなし)	1-5