(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
2009 年7 月2 日 (02.07.2009)

PCT

(10) 国際公開番号
WO 2009/081896 A1

(51) 国際特許分類:
G06K 17/00 (2006.01) *G11B 5/10* (2006.01)
G11B 5/09 (2006.01) *G11B 20/10* (2006.01)

(21) 国際出願番号: PCT/JP2008/073285

(22) 国際出願日: 2008 年12 月22 日 (22.12.2008)

(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 2007-334490
2007 年12 月26 日 (26.12.2007) JP

(71) 出願人 (米国を除く全ての指定国について): シーイエス エレクトロニカ インダストリア エ コメルスィオ リミタダ (CIS Eletronica Industria e Comercio Ltda.) [BR/BR]; 04371000 サンパウロ州サンパウロ市ヴィラサンタカタリーナ区リッシンマツダ街５８５番地 Sao Paulo (BR).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 伊豆山 康夫 (ISUYAMA, Yasuo) [JP/BR]; 04371000 サンパウロ州サンパウロ市ヴィラサンタカタリーナ区リッシンマツダ街５８５番地 シーイエス エレクトロニカ インダストリア エ コメルスィオ リミタダ 内 Sao Paulo (BR).

(74) 代理人: 小林 義孝 (KOBAYASHI, Yoshitaka); 〒1050003 東京都港区西新橋１丁目１４番９号 西新橋ビル Tokyo (JP).

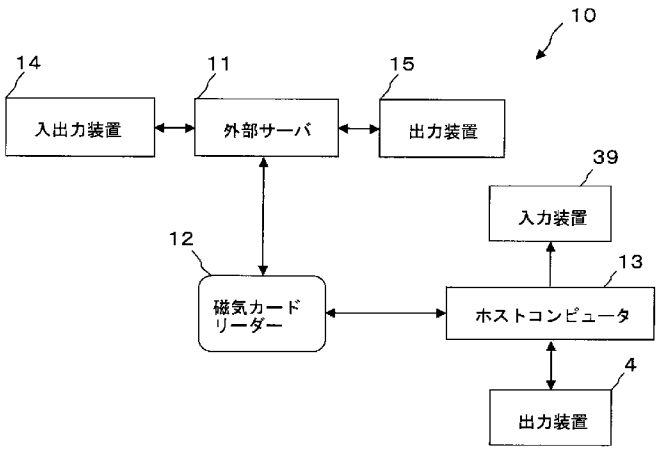
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG,

[続葉有]

(54) Title: MAGNETIC HEAD

(54) 発明の名称: 磁気ヘッド

[図1]



14 INPUT AND OUTPUT DEVICE
11 EXTERNAL SERVER
15 OUTPUT DEVICE
12 MAGNETIC CARD READER
39 INPUT DEVICE
13 HOST COMPUTER
4 OUTPUT DEVICE

(57) Abstract: [PROBLEMS] To provide a magnetic head provided with a microprocessor capable of storing a firmware downloaded from an external server. [MEANS FOR SOLVING PROBLEMS] The magnetic head has a core which is provided with a coil for converting data stored in a magnetic card to analog signals, an A/D conversion chip which is connected to the core to convert the analog signals to digital signals, and the microprocessor which is connected to the A/D conversion chip. The processor has a firmware storage means. When the firmware which controls its arithmetic/storage functions and controls an external hardware is downloaded from the external server (11) to the magnetic head, the firmware storage means stores the firmware.

(57) 要約: 【課題】外部サーバからダウンロードされたファームウェアを記憶することができるマイクロプロセッサを備えた磁気ヘッドを提供する。【解決手段】磁気ヘッドは、磁気カードに記憶されたデータをアナログ信号に変換するコ

[続葉有]

WO 2009/081896 A1

BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

イルを備えたコアと、コアに接続されてアナログ信号をデジタル信号に変換するＡ／Ｄ変換チップと、Ａ／Ｄ変換チップに接続されたマイクロプロセッサとを有する。プロセッサは、その演算・記憶機能を制御するとともに外部ハードウェアを制御するファームウェアが外部サーバ１１から磁気ヘッドにダウンロードされたときに、そのファームウェアを記憶するファームウェア記憶手段を有する。

明 細 書

磁気ヘッド

技術分野

[0001] 本発明は、磁気カードから各種データを読み取る磁気ヘッドに関する。

背景技術

[0002] 磁気ヘッドと、磁気ヘッドに接続されたホストコンピュータとから形成された磁気カード読み取りシステムがある(特許文献1参照)。磁気ヘッドは、磁気カードに記憶されたデータを読み取るヘッド本体と、ヘッド本体が読み取ったアナログ信号をデジタル信号に変換し、デジタル信号を対象鍵暗号化方式または非対象鍵暗号化方式によって暗号化する制御部とから形成されている。ヘッド本体と制御部とは、ヘッド容器に収容されている。磁気ヘッドの制御部は、その記憶領域内に記憶された鍵を使用してデジタル信号を暗号化し、暗号化したデジタル信号をホストコンピュータに送信する。ホストコンピュータの制御部は、それに記憶された鍵を使用して暗号化されたデジタル信号を復号化する。

[0003] このシステムでは、磁気ヘッドの制御部が暗号化したデジタル信号をホストコンピュータの制御部に送信すると、ホストコンピュータの制御部が磁気ヘッドの制御部に鍵の変更を指示する。このシステムにおける鍵の変更手順は、以下のとおりである。ホストコンピュータの制御部は、磁気ヘッドから受信したデジタル信号を復号化すると、あらたに鍵を生成し、生成した鍵を磁気ヘッドの制御部に送信する。磁気ヘッドの制御部は、記憶領域内に記憶された既存の鍵をあらたに送信された鍵に変更する。また、ホストコンピュータの制御部は、操作者がキーボードから関数の変更指示とあらたな関数とを入力すると、関数変更指示とあらたな関数とを磁気ヘッドの制御部に送信する。磁気ヘッドの制御部は、既存の関数をあらたに送信された関数に変更する。

特許文献1:特開2001－143213号公報

発明の開示

発明が解決しようとする課題

[0004] 前記公報に開示の磁気カード読み取りシステムにおける磁気ヘッドの制御部は、磁

気ヘッドが市場に出荷された後や磁気ヘッドが磁気カードリーダに設置された後に、制御部の演算・記憶機能や外部ハードウェアを制御するファームウェアが外部サーバから磁気ヘッドにダウンロードされたとしても、そのファームウェアを記憶領域内に記憶することはないから、ダウンロードされる各種のファームウェアを制御部に格納することはできない。また、この磁気ヘッドの制御部は、バージョンアップされたファームウェアが外部サーバからダウンロードされたとしても、バージョンアップ後のファームウェアを記憶領域内に記憶することはないから、ファームウェアのバージョンアップに対応することができず、磁気カードのフォーマットが変更されると、その磁気カードのデータを読み取ることができない場合があり、フォーマットの変更にともなって磁気ヘッド自体を取り換えなければならない。

[0005] 本発明の目的は、外部サーバからダウンロードされたファームウェアを記憶することができるデジタルICを備えた磁気ヘッドを提供することにある。本発明の他の目的は、外部サーバからダウンロードされたバージョンアップ後のファームウェアを記憶することができるデジタルICを備えた磁気ヘッドを提供することにある。

課題を解決するための手段

[0006] 前記課題を解決するための本発明の前提は、磁性体を利用して各種データを記憶した磁気カードからそのデータを読み取る磁気ヘッドである。

[0007] 前記前提における本発明の特徴は、磁気ヘッドが、磁気カードに記憶されたデータをアナログ信号に変換するコイルを有するコアと、コアに接続されてアナログ信号をデジタル信号に変換するA／D変換チップと、A／D変換チップに接続されたデジタルICとを備え、デジタルICは、その演算・記憶機能を制御するとともに外部ハードウェアを制御するファームウェアが外部サーバから磁気ヘッドにダウンロードされたときに、そのファームウェアを記憶するファームウェア記憶手段を有することにある。

[0008] 本発明の一例として、ファームウェアには、磁気カードの各種フォーマットに対応させてデジタルICに該磁気カードの各種データを読み取らせるデータ読み取り制御が含まれ、デジタルICが磁気カードの各種フォーマットに対応して該磁気カードから各種データを読み取るフォーマット対応読み取り手段を有する。

[0009] 本発明の他の一例として、ファームウェアには、所定の暗号化アルゴリズムに基づ

いてデジタルICにデジタル信号を暗号化させるデータ暗号化制御が含まれ、デジタルICがデジタル信号を所定の暗号化アルゴリズムに基づいて暗号化するデータ暗号化手段を有する。

[0010] 本発明の他の一例として、デジタルICは、バージョンアップされたファームウェアが外部サーバから磁気ヘッドにダウンロードされたときに、バージョンアップ前のファームウェアをバージョンアップ後のファームウェアに書き換えるファームウェア更新手段を有する。

[0011] 本発明の他の一例としては、外部サーバがそれに格納された鍵を使用してファームウェアを暗号化しつつ、暗号化したファームウェアを磁気ヘッドにダウンロードし、デジタルICがそれに格納された鍵を使用して暗号化されたファームウェアを復号化しつつ、復号化したファームウェアを記憶する。

[0012] 本発明の他の一例としては、デジタルICと外部サーバとがそれらの間で認証を行う相互認証を実行し、デジタルICと外部サーバとが相互認証による互いの認証結果を正当であると判断した後、外部サーバが磁気ヘッドにファームウェアをダウンロードし、デジタルICが外部サーバからダウンロードされたファームウェアを記憶する。

[0013] 本発明の他の一例として、デジタルICは、デジタル信号を暗号化する各種の暗号化アルゴリズムが外部サーバから磁気ヘッドにダウンロードされたときに、その暗号化アルゴリズムを記憶するアルゴリズム記憶手段を有する。

[0014] 本発明の他の一例として、デジタルICは、あらたな暗号化アルゴリズムが外部サーバから磁気ヘッドにダウンロードされたときに、すでに記憶した暗号化アルゴリズムをあらたな暗号化アルゴリズムに書き換えるアルゴリズム更新手段を有する。

[0015] 本発明の他の一例としては、外部サーバがそれに格納された鍵を使用して暗号化アルゴリズムを暗号化しつつ、暗号化した暗号化アルゴリズムを磁気ヘッドにダウンロードし、デジタルICがそれに格納された鍵を使用して暗号化された暗号化アルゴリズムを復号化しつつ、復号化した暗号化アルゴリズムを記憶する。

[0016] 本発明の他の一例としては、デジタルICと外部サーバとがそれらの間で認証を行う相互認証を実行し、デジタルICと外部サーバとが相互認証による互いの認証結果を正当であると判断した後、外部サーバが磁気ヘッドに暗号化アルゴリズムをダウンロ

ードし、デジタルICが外部サーバからダウンロードされた暗号化アルゴリズムを記憶する。

[0017] 本発明の他の一例としては、磁気ヘッドがその外周を包被するハウジングを有し、コアとA／D変換チップとデジタルICとがハウジングの内部に収容されている。

[0018] 本発明の他の一例としては、A／D変換チップとデジタルICとがハウジングの内部に充填された固形物質によって該ハウジングに固定されている。

発明の効果

[0019] 本発明にかかる磁気ヘッドによれば、デジタルICの演算・記憶機能を制御するとともに外部ハードウェアを制御するファームウェアが外部サーバから磁気ヘッドにダウンロードされると、デジタルICがそのファームウェアを記憶するから、磁気ヘッドが市場に出荷された後や磁気ヘッドが磁気カードリーダに設置された後において、外部サーバからダウンロードされたファームウェアをデジタルICに随時格納することができる。この磁気ヘッドは、その出荷後や設置後においても各種のファームウェアに対応することができ、それらファームウェアを利用することで、磁気ヘッドの動作環境に応じてデジタルICの演算・記憶機能や外部ハードウェアの最適な制御を行うことができる。

[0020] 磁気カードの各種フォーマットに対応させてデジタルICに磁気カードの各種データを読み取らせるデータ読み取り制御がファームウェアに含まれ、デジタルICが磁気カードの各種フォーマットに対応して磁気カードから各種データを読み取る磁気ヘッドは、磁気カードのフォーマットに対応して磁気カードからデータを読み取るデータ読み取り制御が外部サーバからデジタルICにダウンロードされると、デジタルICがそのデータ読み取り制御を記憶するから、磁気ヘッドが市場に出荷された後や磁気ヘッドが磁気カードリーダに設置された後において、外部サーバからダウンロードされたデータ読み取り制御をデジタルICに随時格納することができる。この磁気ヘッドは、その出荷後や設置後においても磁気カードの各種フォーマットに対応することができ、磁気カードの各種仕様に適応しつつ、それらカードに記憶されたデータを確実に読み取ることができる。この磁気ヘッドは、磁気カードのフォーマット変更にともなって磁気ヘッドを取り換える必要はなく、同一の磁気ヘッドを継続して使用することができる

。

[0021] 所定の暗号化アルゴリズムに基づいてデジタルICにデジタル信号を暗号化させるデータ暗号化制御がファームウェアに含まれ、デジタルICがデジタル信号を所定の暗号化アルゴリズムに基づいて暗号化する磁気ヘッドは、磁気カードから読み取った各種データ(デジタル信号)をデジタルICが暗号化するから、データが第3者に盗取されたとしても、盗取したデータを復号化しなければそのデータを利用することができず、第3者による磁気カードの不正な複製を防ぐことができる。なお、インターネットバンキングにおいて、磁気カードのデータを盗取した第3者が銀行やクレジットカード会社のサイトに偽サイトを作成するいわゆる「なりすまし」行為を行い、銀行やクレジットカード会社に対して不正な取引を行う場合がある。しかし、この磁気ヘッドは、第3者が磁気カードのデータを盗取することができないから、偽サイトを作ることはできず、第3者による「なりすまし」を防ぐことができる。

[0022] デジタルICがバージョンアップ前のファームウェアをバージョンアップ後のファームウェアに書き換える磁気ヘッドは、磁気ヘッドが市場に出荷された後や磁気ヘッドが磁気カードリーダに設置された後において、ファームウェアのバージョンアップが行われたとしても、バージョンアップ後のファームウェアに即座に対応することができる。この磁気ヘッドは、磁気カードのフォーマットの変更にともなってファームウェアが変更されたとしても、変更後のファームウェアを記憶することができるから、磁気カードの変更された各種フォーマットに対応することができ、磁気カードの各種仕様に適応しつつ、それらカードに記憶されたデータを確実に読み取ることができる。

[0023] 外部サーバがそれに格納された鍵を使用してファームウェアを暗号化し、デジタルICがそれに格納された鍵を使用して暗号化されたファームウェアを復号化し、復号化したファームウェアを記憶する磁気ヘッドは、ファームウェアが暗号化された状態で磁気ヘッドにダウンロードされるから、ファームウェアが第3者に盗取されたとしても、盗取したファームウェアを復号化しなければそのファームウェアを利用することができず、ファームウェアの改竄による第3者の磁気カードの不正利用を防ぐことができる。

[0024] デジタルICと外部サーバとが相互に認証を行う相互認証を実行し、デジタルICと外部サーバとが相互認証による互いの認証結果を正当であると判断した後、外部サー

バが磁気ヘッドにファームウェアをダウンロードし、デジタルICが外部サーバからダウンロードされたファームウェアを記憶する磁気ヘッドは、デジタルICと外部サーバとが相互認証を実行することで互いの正当性を判断することができるから、偽サーバが磁気ヘッドに接続された場合や偽磁気ヘッドが外部サーバに接続された場合であっても、それを見破ることができる。この磁気ヘッドは、第3者が偽サーバを利用して磁気ヘッドにアクセスすることはできず、ファームウェアの改竄による第3者の磁気カードの不正利用を防ぐことができる。

[0025] 暗号化アルゴリズムが外部サーバからダウンロードされたときに、デジタルICがその暗号化アルゴリズムを記憶する磁気ヘッドは、磁気ヘッドが市場に出荷された後や磁気ヘッドが磁気カードリーダに設置された後において、各種の暗号化アルゴリズムをデジタルICに随時格納することができ、各種の暗号化アルゴリズムを利用して磁気カードのデータ(デジタル信号)を暗号化することができる。この磁気ヘッドは、各種の暗号化アルゴリズムを利用してデジタルICが磁気カードのデータを暗号化するから、データが第3者に盗取されたとしても、盗取したデータを復号化しなければそのデータを利用することができず、第3者による磁気カードのデータの不正な取得を確実に防ぐことができ、第3者による磁気カードの不正な複製や第3者による「なりすまし」を確実に防ぐことができる。

[0026] あらたな暗号化アルゴリズムが外部サーバからダウンロードされたときに、デジタルICがすでに記憶した暗号化アルゴリズムをあらたな暗号化アルゴリズムに書き換える磁気ヘッドは、磁気ヘッドが市場に出荷された後や磁気ヘッドが磁気カードリーダに設置された後にデジタルICに記憶された暗号化アルゴリズムが解析され、そのアルゴリズムの変更が必要になったとしても、暗号化アルゴリズムの変更に即座に対応することができ、変更された暗号化アルゴリズムに基づいてデータを暗号化することができる。この磁気ヘッドは、あらたな暗号化アルゴリズムを利用してデジタルICが磁気カードのデータ(デジタル信号)を暗号化するから、データが第3者に盗取されたとしても、盗取したデータを復号化しなければそのデータを利用することができず、第3者による磁気カードのデータの不正な取得を確実に防ぐことができ、第3者による磁気カードの不正な複製や第3者による「なりすまし」を確実に防ぐことができる。

[0027] 外部サーバがそれに格納された鍵を使用して暗号化アルゴリズムを暗号化し、デジタルICがそれに格納された鍵を使用して暗号化された暗号化アルゴリズムを復号化し、復号化した暗号化アルゴリズムを記憶する磁気ヘッドは、暗号化アルゴリズムが暗号化された状態で磁気ヘッドにダウンロードされるから、暗号化アルゴリズムが第3者に盗取されたとしても、盗取した暗号化アルゴリズムを復号化しなければその暗号化アルゴリズムを利用してデータを復号化することができない。この磁気ヘッドは、第3者による磁気カードのデータの不正な取得を確実に防ぐことができ、第3者による磁気カードの不正な複製や第3者による「なりすまし」を確実に防ぐことができる。

[0028] デジタルICと外部サーバとが相互に認証を行う相互認証を実行し、デジタルICと外部サーバとが相互認証による互いの認証結果を正当であると判断した後、外部サーバが磁気ヘッドに暗号化アルゴリズムをダウンロードし、デジタルICが外部サーバからダウンロードされた暗号化アルゴリズムを記憶する磁気ヘッドは、デジタルICと外部サーバとが相互認証を実行することで互いの正当性を判断することができるから、偽磁気ヘッドが外部サーバに接続されたとしても、偽磁気ヘッドが外部サーバにアクセスすることはできず、外部サーバから偽磁気ヘッドに暗号化アルゴリズムがダウンロードされることはない。この磁気ヘッドは、第3者が暗号化アルゴリズムを利用して磁気カードのデータを復号化することができず、第3者による磁気カードのデータの不正な取得を確実に防ぐことができ、第3者による磁気カードの不正な複製や第3者による「なりすまし」を確実に防ぐことができる。

[0029] コアとA／D変換チップとデジタルICとがハウジングに収容された磁気ヘッドは、磁気ヘッド自体を分解しなければ、アナログ信号やデジタル信号に変換されたデータを盗取することができないから、磁気カードに記憶されたデータの盗取を確実に防ぐことができ、第3者による磁気カードの不正な複製や第3者による「なりすまし」を確実に防ぐことができる。

[0030] A／D変換チップとデジタルICとがハウジングの内部に合成樹脂によって固定された磁気ヘッドは、磁気ヘッドを分解するときに合成樹脂を取り除かなければならず、合成樹脂を取り除く際にA／D変換チップとデジタルICとが破壊されるから、A／D変換チップとデジタルICとに対するデータ盗取用機器の取り付けを防ぐことができる

。この磁気ヘッドは、第3者による磁気カードのデータの不正な取得を確実に防ぐことができ、第3者による磁気カードの不正な複製や第3者による「なりすまし」を確実に防ぐことができる。

図面の簡単な説明

[0031] [図1]磁気ヘッドを利用した一例として示す磁気カード読み取りシステムのハードウェア構成図。

[図2]一例として示す磁気カードリーダの内部構造の概略図。

[図3]ハウジングの一部を破断して示す磁気ヘッドの部分破断斜視図。

[図4]一例として示すマイクロプロセッサ(プロセッサ)の構成図。

[図5]外部サーバと磁気ヘッドとの間で行われる処理の一例を示すブロック図。

[図6]外部認証の一例を示すラダー図。

[図7]内部認証の一例を示すラダー図。

[図8]外部サーバとマイクロプロセッサとの間におけるダウンロード処理の一例を示すラダー図。

[図9]暗号化および復号化に使用する鍵の生成の一例を説明する図。

[図10]暗号化および復号化に使用する鍵の生成の一例を説明する図。

[図11]暗号化および復号化に使用する鍵の生成の一例を説明する図。

[図12]暗号化および復号化に使用する鍵の生成の一例を説明する図。

[図13]暗号化および復号化に使用する鍵の生成の一例を説明する図。

[図14]暗号化および復号化に使用する鍵の生成の一例を説明する図。

[図15]磁気ヘッドとホストコンピュータとの間で行われる処理の一例を示すブロック図。

[図16]外部認証の一例を示すラダー図。

[図17]内部認証の一例を示すラダー図。

[図18]システムにおけるメイン処理の一例を示すラダー図。

[図19]暗号化および復号化に使用する鍵の生成の他の一例を説明する図。

[図20]暗号化および復号化に使用する鍵の生成の他の一例を説明する図。

[図21]暗号化および復号化に使用する鍵の生成の他の一例を説明する図。

[図22]暗号化および復号化に使用する鍵の生成の他の一例を説明する図。

[図23]暗号化および復号化に使用する鍵の生成の他の一例を説明する図。

[図24]暗号化および復号化に使用する鍵の生成の他の一例を説明する図。

符号の説明

[0032] 10 磁気カード読み取りシステム

11 外部サーバ

12 磁気カードリーダ

13 ホストコンピュータ

19 磁気ヘッド

23 ハウジング

24 コア

25 A／D変換チップ

26 マイクロプロセッサ(デジタルIC)

35 中央処理部

36 メモリ

発明を実施するための最良の形態

[0033] 添付の図面を参照し、本発明に係る磁気ヘッドの詳細を説明すると、以下のとおりである。図1は、磁気ヘッド19を利用した一例として示す磁気カード読み取りシステム10のハードウェア構成図であり、図2は、一例として示す磁気カードリーダ12の内部構造の概略図である。図3は、ハウジング23の一部を破断して示す磁気ヘッド19の部分破断斜視図であり、図4は、一例として示すマイクロプロセッサ26(デジタルIC)の構成図である。図3では、コア24の先端部27が磁気カード29の表面に接触した状態にあり、ハウジング23に充填された合成樹脂28(固形物質)の図示を一部省略している。

[0034] 磁気カード読み取りシステム10は、外部サーバ11と、磁気カード29に記憶されたカードデータ(各種データ)を読み取る磁気カードリーダ12と、ホストコンピュータ13とから形成されている。システム10では、サーバ11とカードリーダ12とがインターフェイス(有線または無線)を介して連結され、カードリーダ12とコンピュータ13とがインター

フェイス(有線または無線)を介して連結されている。カードデータには、カード番号や暗証番号、ユーザID、パスワード、カード所持者の個人情報(郵便番号、住所または居所、氏名または名称、生年月日、家族構成、年収、勤務会社、電話番号、ファクシミリ番号、メールアドレス、URL等)、カード所持者の法人情報(郵便番号、住所、名称、設立年月日、各種の経営情報、取引先情報、電話番号、ファクシミリ番号、メールアドレス、URL等)、商取引内容等が含まれる。

[0035] 外部サーバ11は、中央処理部(CPUまたはMPU)とメモリ(大容量ハードディスク)とを有するコンピュータであり、DNSサーバ機能を備えている。メモリには、カードリーダ12のURLが格納されている。サーバ11の中央処理部は、演算ユニットおよび制御ユニットから形成されている。サーバ11には、キーボードやマウス等の入力装置14、ディスプレイやプリンタ等の出力装置15がインターフェイスを介して接続されている。サーバ11の中央処理部は、オペレーティングシステムによる制御に基づいて、メモリに格納されたアプリケーションを起動し、起動したアプリケーションに従って以下の各手段を実行する。

[0036] 外部サーバ11の中央処理部は、メモリに格納された鍵を使用して所定のファームウェアを暗号化するファームウェア暗号化手段を実行し、メモリに格納された鍵を使用して所定の暗号化アルゴリズムを暗号化するアルゴリズム暗号化手段を実行する。サーバ11の中央処理部は、インターネットを介してカードリーダ12の後記するコントローラにアクセスするアクセス手段を実行し、磁気ヘッド19との間で相互に認証を行う相互認証手段を実行する。

[0037] 外部サーバ11の中央処理部は、暗号化していないファームウェアまたは暗号化した後のファームウェアを磁気ヘッド19にダウンロードするファームウェア第1ダウンロード手段を実行し、暗号化していないあらたなファームウェア(バージョンアップファームウェア)または暗号化した後のあらたなファームウェア(バージョンアップファームウェア)を磁気ヘッド19にダウンロードするファームウェア第2ダウンロード手段を実行する。サーバ11の中央処理部は、暗号化していない暗号化アルゴリズムまたは暗号化した後の暗号化アルゴリズムを磁気ヘッド19にダウンロードするアルゴリズム第1ダウンロード手段を実行し、暗号化していないあらたな暗号化アルゴリズムまたは暗号

化した後のあらたな暗号化アルゴリズムを磁気ヘッド19にダウンロードするアルゴリズム第2ダウンロード手段を実行する。

[0038] ファームウェアとは、磁気ヘッド19の後記するマイクロプロセッサ26の演算・記憶機能を制御するとともにプロセッサ26につながる外部ハードウェアを制御するアプリケーションである。ファームウェアには、磁気カード29の各種フォーマットに対応させて磁気ヘッド19のプロセッサ26にカード29の各種データを読み取らせるデータ読み取り制御が含まれる。さらに、所定の暗号化アルゴリズムに基づいて磁気ヘッド19のプロセッサ26にカードデータ(デジタル信号)を暗号化させるデータ暗号化制御が含まれる。ファームウェアは、それを利用することで、磁気ヘッド19の動作環境に応じたプロセッサ26の演算・記憶機能の最適な制御を行うことができるとともに、プロセッサ26につながる外部ハードウェアの最適な制御を行うことができる。

[0039] 磁気カードリーダ12は、挿入電動型であり、コントローラ(図示せず)が内蔵されている。カードリーダ12は、図2に示すように、前端に形成されたカード挿入口16と、後端に形成されたカード排出口17と、カード挿入口16からカード排出口17につながるカード案内レール18とを有する。カードリーダ12の中央には、磁気ヘッド19が取り付けられている。挿入口16や排出口17、磁気ヘッド19の近傍には、案内レール18を移動する磁気カード29の位置を検出するための光センサ20が取り付けられている。

[0040] 挿入口16からカード29を挿入すると、カード29が案内レール18を自動的に移動して排出口17から排出される。案内レール18におけるカード29の移動は、カードリーダ12内に取り付けられたベルト21によって行われる。ベルト21の駆動は、カードリーダ12内に設置されたモータ22によって行われる。磁気ヘッド19や各センサ20、モータ22は、カードリーダ12のコントローラに連結されている。

[0041] カードリーダ12のコントローラは、中央処理部(CPUまたはMPU)とメモリ(大容量フラッシュメモリ)とを有するコンピュータである。メモリには、外部サーバ11のURLが格納されている。コントローラの中央処理部は、演算ユニットおよび制御ユニットから形成されている。コントローラは、DNSサーバ(図示せず)とホストコンピュータ13とに連結されている。コントローラは、インターネットを介して外部サーバ11にアクセス可能である。コントローラは、スイッチのON／OFFによってモータ22の駆動や停止を

行うとともに、カードデータの読み取り開始指令やカードデータの読み取り停止指令を磁気ヘッド19に出力する。

[0042] 磁気ヘッド19は、磁気カード29の磁性層32に記憶されたカードデータを電気信号に変換する。磁気ヘッド19は、図3に示すように、その外周面を包被するハウジング23と、磁気カードに記憶されたカードデータをアナログ信号(電気信号)に変換するコイル(図示せず)が取り付けられたコア24と、アナログ信号をデジタル信号(電気信号)に変換するA／D変換チップ25と、マイクロプロセッサ26(MPU)とから形成されている。カードリーダ12内に設置された磁気ヘッド19では、それを形成するコア24の先端部27が案内レール18に対向している。A／D変換チップ25は、コア24に電気的に連結されている。プロセッサ26は、A／D変換チップ25に電気的に連結され、インターフェイスを介してホストコンピュータ13に連結されている。

[0043] コア24やA／D変換チップ25、マイクロプロセッサ26は、ハウジング23の内部に収容されている。ただし、コア24の先端部27は、ハウジング23の下端から外側に露出している。A／D変換チップ25とプロセッサ26とは、その全体がハウジング23の内部に充填された合成樹脂28(固形物質)によって包被され、合成樹脂28を介してハウジング23の内部に固定されている。合成樹脂28には、熱硬化性合成樹脂を使用することが好ましいが、熱硬化性合成樹脂の他に、熱可塑性合成樹脂を使用することもできる。また、合成樹脂等の有機化合物の他に、化学溶剤に対する耐性が高いセラミック等(固形物質)の無機化合物を使用することもできる。磁気カード29は、その下面から、カラー印刷層30、ベース層31、磁性層32、遮蔽層33、印字層34の順で並んでいる。磁性層32は強磁性体から作られ、ベース層31はポリエチレン・テレフタレートから作られている。なお、磁気ヘッド19には、マイクロプロセッサ26に変えて、ゲートアレイやフィールドプログラマブルゲートアレイ、専用ハードウェアのうちのいずれかのデジタルICが取り付けられていてもよい。

[0044] マイクロプロセッサ26は、図4に示すように、中央処理部35とメモリ36(フラッシュメモリやEEROM)とを有する。プロセッサ26の中央処理部35は、演算ユニット37および制御ユニット38から形成されている。中央処理部35は、オペレーティングシステムによる制御に基づいて、メモリ36に格納されたアプリケーションを起動し、起動したア

プリケーションに従って以下の各手段を実行する。中央処理部35は、外部サーバ11またはホストコンピュータ13との間で相互に認証を行う相互認証手段を実行する。

[0045] マイクロプロセッサ26の中央処理部35は、暗号化していないファームウェアが外部サーバ11から磁気ヘッド19にダウンロードされると、そのファームウェアをメモリ36に格納するファームウェア記憶手段を実行する。または、暗号化されたファームウェアがサーバ11から磁気ヘッド19にダウンロードされると、メモリ36に格納された鍵を使用して暗号化されたファームウェアを復号化するファームウェア復号化手段を実行し、復号化したファームウェアをメモリ36に格納するファームウェア記憶手段を実行する。中央処理部35は、バージョンアップされたあらたなファームウェアがサーバ11から磁気ヘッド19にダウンロードされると、バージョンアップ前のファームウェアをバージョンアップ後のファームウェアに書き換えるファームウェア更新手段を実行する。

[0046] ファームウェアをメモリ36に格納すると、マイクロプロセッサ26の中央処理部35は、メモリに格納したファームウェアを起動し、起動したファームウェアに従って以下の各手段を実行する。中央処理部35は、暗号化前の各種の暗号化アルゴリズムが外部サーバ11から磁気ヘッド19にダウンロードされると、その暗号化アルゴリズムをメモリ36に格納するアルゴリズム記憶手段を実行する。または、暗号化後の各種の暗号化アルゴリズムが外部サーバ11から磁気ヘッド19にダウンロードされると、メモリ36に格納された鍵を使用して暗号化された暗号化アルゴリズムを復号化するアルゴリズム復号化手段を実行し、復号化した暗号化アルゴリズムをメモリ36に格納するアルゴリズム記憶手段を実行する。

[0047] マイクロプロセッサ26の中央処理部35は、暗号化していないあらたな暗号化アルゴリズムが外部サーバ11から磁気ヘッド19にダウンロードされると、すでに記憶した暗号化アルゴリズムをあらたな暗号化アルゴリズムに書き換えるアルゴリズム更新手段を実行する。または、暗号化されたあらたな暗号化アルゴリズムが外部サーバ11から磁気ヘッド19にダウンロードされると、メモリ36に格納された鍵を使用して暗号化されたあらたな暗号化アルゴリズムを復号化するアルゴリズム復号化手段を実行し、すでに記憶した暗号化アルゴリズムを復号化したあらたな暗号化アルゴリズムに書き換えるアルゴリズム更新手段を実行する。中央処理部35は、磁気カード29の各種フォ

ーマットに対応してカード29から各種データを読み取るフォーマット対応読み取り手段を実行し、カードデータ(デジタル信号)を所定の暗号化アルゴリズムに基づいて暗号化するデータ暗号化手段を実行する。中央処理部35は、暗号化したカードデータをホストコンピュータ13に出力する暗号化データ出力手段を実行する。

[0048] ホストコンピュータ13は、中央処理部(CPUまたはMPU)とメモリ(大容量ハードディスク)とを有する。コンピュータ13の中央処理部は、演算ユニットおよび制御ユニットから形成されている。コンピュータ13には、キーボードやマウス等の入力装置39、ディスプレイやプリンタ等の出力装置40がインターフェイスを介して接続されている。コンピュータ13の中央処理部は、オペレーティングシステムによる制御に基づいて、メモリに格納されたアプリケーションを起動し、起動したアプリケーションに従って以下の各手段を実行する。

[0049] ホストコンピュータ13の中央処理部は、磁気ヘッド19のマイクロプロセッサ26との間で相互に認証を行う相互認証手段を実行する。コンピュータ13の中央処理部は、暗号化されたカードデータが磁気ヘッド19から出力されると、そのデータを複合化するデータ復号化手段を実行し、復号化したデータをメモリに格納するデータ記憶手段を実行する。コンピュータ13の中央処理部は、復号化したデータを出力装置40を介して出力するデータ出力手段を実行する。なお、外部サーバ11や磁気カードリーダ12、ホストコンピュータ13、各入力装置14, 39、各出力装置15, 40には、配線を介して電力が供給されている。

[0050] 図5は、外部サーバ11と磁気ヘッド19との間で行われる処理の一例を示すブロック図である。外部サーバ11と磁気ヘッド19との間で行われる相互認証の一例を説明すると、以下のとおりである。システム10を起動させると、外部サーバ11や磁気カードリーダ12、ホストコンピュータ13が稼動する。サーバ11がカードリーダ12のURLを利用し、インターネットを介してカードリーダ12にアクセスする(アクセス手段)。または、カードリーダ12がサーバ11のURLを利用し、インターネットを介してサーバ11にアクセスする。

[0051] 外部サーバ11と磁気カードリーダ12のコントローラとがインターネットを介して接続されると、サーバ11の中央処理部とマイクロプロセッサ26の中央処理部35とがカー

ドリーダ12のコントローラを介して接続される。サーバ11の中央処理部とプロセッサ26の中央処理部35とは、メモリーテスト(S－10)とコードサイニング(S－11)とを行う(初期テスト)。コードサイニング(S－11)は、ファームウェアのオブジェクトコードが書き替えられていないかを判定する。初期テストが終了し、その結果が正しい場合、サーバ11の中央処理部とプロセッサ26の中央処理部35とは、それらの正当性を判断する相互認証を行う(相互認証手段)。相互認証は、サーバ11が磁気ヘッド19の正当性を認証する外部認証(S－12)を行った後、磁気ヘッド19がサーバ11の正当性を認証する内部認証(S－13)を行う。

[0052] 外部サーバ11の中央処理部とマイクロプロセッサ26の中央処理部35とが相互認証による互いの認証結果を正当であると判断すると、サーバ11からファームウェアや暗号化アルゴリズムの磁気ヘッド19へのダウンロードが可能となり、サーバ11とプロセッサ26との間でダウンロード処理が行われる(S－14)。逆に、サーバ11とプロセッサ26との少なくとも一方が認証結果を不可であると判断すると、認証不可メッセージがサーバ11のディスプレイに表示され、ファームウェアや暗号化アルゴリズムの磁気ヘッド19へのダウンロードを行うことができない。

[0053] サーバ11とプロセッサ26との間の相互認証は、システム10を起動させる度毎に行われる場合、システム10を連続して稼働させるきは日時単位や週単位、月単位で行われる場合、あるいは、ファームウェアを磁気ヘッド19にダウンロードする度毎に行われる場合、暗号化アルゴリズムを磁気ヘッド19にダウンロードする度毎に行われる場合がある。なお、サーバ11とプロセッサ26とが相互認証を行うことなく、サーバ11とプロセッサ26とがインターネットを介して接続され、サーバ11が磁気ヘッド19へファームウェアや暗号化アルゴリズムのダウンロードを行うこともできる。

[0054] 図6は、外部認証の一例を示すラダー図であり、図7は、内部認証の一例を示すラダー図である。外部認証における認証手順は、以下のとおりである。外部サーバ11の中央処理部がマイクロプロセッサ26の中央処理部35に乱数(認証子)の生成と送信とを要求する(S－20)。プロセッサ26の中央処理部35は、サーバ11の指令に従って64bit乱数を生成し、生成した乱数をサーバ11に送信する(S－21)。64bit乱数を取得したサーバ11の中央処理部は、メモリに格納された認証用の鍵を使用し、ト

リプルDES(Triple Data Encryption Standard)によって乱数を暗号化した後、暗号化した乱数をプロセッサ26に送信する(S－22)。プロセッサ26の中央処理部35は、メモリ36に格納された認証用の鍵を使用し、トリプルDESによって暗号化された乱数を復号化する。プロセッサ26の中央処理部35は、それが生成した乱数と復号化した乱数とを比較し、両者が同一であれば認証結果を正当であると判断し、認証結果正当情報をサーバ11に送信する(S－23)。一方、生成した乱数と復号化した乱数とが異なる場合、認証結果を不可であると判断し、認証結果不可情報をサーバ11に送信する(S－23)。サーバ11は、プロセッサ26から外部認証結果を取得する(S－24)。

[0055] トリプルDESは、シングルDES(Single Data Encryption Standard)を3回繰り返すことにより、鍵の伸長やアルゴリズムの偏りの減少を図り、暗号強度を強化する。トリプルDESには、3つの鍵が全て異なる3－KeyトリプルDESと、1回目と3回目とに同じ鍵を用いる2－KeyトリプルDESとがある。なお、トリプルDESは、3－KeyトリプルDESと2－KeyトリプルDESとのいずれでもよい。また、DESは、トリプルDESではなく、シングルDESであってもよい。

[0056] 内部認証における認証手順は、以下のとおりである。外部サーバ11の中央処理部は、64bit乱数(認証子)を生成し、それをマイクロプロセッサ26に送信する(S－25)。64bit乱数を取得したプロセッサ26の中央処理部35は、メモリ36に格納された認証用の鍵を使用し、トリプルDESによって乱数を暗号化した後、暗号化した乱数をサーバ11に送信する(S－26)。サーバ11の中央処理部は、メモリに格納された認証用の鍵を使用し、トリプルDESによって暗号化された乱数を復号化する(S－27)。サーバ11の中央処理部は、それが生成した乱数と復号化した乱数とを比較し、両者が同一であれば認証結果を正当であると判断する。一方、生成した乱数と復号化した乱数とが異なる場合、認証結果を不可であると判断し、磁気ヘッド19へのファームウェアや暗号化アルゴリズムのダウンロードを不可とする。

[0057] 図8は、外部サーバ11とマイクロプロセッサ26との間におけるダウンロード処理の一例を示すラダー図である。外部サーバ11のメモリには、ファームウェアおよび暗号化アルゴリズムとそれらを暗号化する暗号化用の鍵とが格納されており、必要に応じてバージョンアップされたあらたなファームウェアまたはあらたな暗号化アルゴリズムが

随時格納される。マイクロプロセッサ26のメモリ36には、ファームウェアおよび暗号化アルゴリズムの復号化用の鍵が格納されている。

[0058] 外部サーバ11の中央処理部は、ファームウェアおよび暗号化アルゴリズムと暗号化用の鍵とをメモリから取り出し、その鍵を使用してトリプルDESによってファームウェアや暗号化アルゴリズムを暗号化する(ファームウェア暗号化手段、アルゴリズム暗号化手段)(S－28)。サーバ11の中央処理部は、暗号化したファームウェアや暗号化アルゴリズムをインターネットを介して磁気ヘッド19にダウンロードする(ファームウェア第1ダウンロード手段、アルゴリズム第1ダウンロード手段)(S－29)。なお、ファームウェアや暗号化アルゴリズムを暗号化しない場合、サーバ11の中央処理部は、それらを暗号化せずにそのまま磁気ヘッド19にダウンロードする(ファームウェア第1ダウンロード手段、アルゴリズム第1ダウンロード手段)(S－29)。

[0059] 外部サーバ11の中央処理部は、バージョンアップされたあらたなファームウェアまたはあらたな暗号化アルゴリズムの磁気ヘッド19へのダウンロードが必要になると、あらたなファームウェアやあらたな暗号化アルゴリズムと暗号化用の鍵とをメモリから取り出し、その鍵を使用してトリプルDESによってファームウェアや暗号化アルゴリズムを暗号化する(ファームウェア暗号化手段、アルゴリズム暗号化手段)(S－28)。サーバ11の中央処理部は、暗号化したあらたなファームウェアおよびあらたな暗号化アルゴリズムをインターネットを介して磁気ヘッド19にダウンロードする(ファームウェア第2ダウンロード手段、アルゴリズム第2ダウンロード手段)(S－29)。なお、あらたなファームウェアやあらたな暗号化アルゴリズムを暗号化しない場合、サーバ11の中央処理部は、それらを暗号化せずにそのまま磁気ヘッド19にダウンロードする(ファームウェア第2ダウンロード手段、アルゴリズム第2ダウンロード手段)(S－29)。サーバ11からダウンロードされたファームウェアや暗号化アルゴリズムは、磁気カードリーダ19のコントローラのメモリに一時保管された後、コントローラから磁気ヘッド19に出力される。

[0060] マイクロプロセッサ26の中央処理部35は、暗号化されたファームウェアおよび暗号化アルゴリズムを外部サーバ11から受け取ると、メモリ36から復号化用の鍵を取り出し、その鍵を使用してリプルDESによって暗号化されたファームウェアや暗号化アル

ゴリズムを復号化する(ファームウェア復号化手段、アルゴリズム復号化手段)(S－30)。中央処理部35は、複合化したファームウェアおよび暗号化アルゴリズムをメモリ36に格納する(ファームウェア記憶手段、アルゴリズム記憶手段)。暗号化していないファームウェアおよび暗号化アルゴリズムを外部サーバ11から受け取ると、中央処理部35は、そのファームウェアや暗号化アルゴリズムをメモリ36に格納する(ファームウェア記憶手段、アルゴリズム記憶手段)。

[0061] マイクロプロセッサ26の中央処理部35は、暗号化されたあらたなファームウェアおよびあらたな暗号化アルゴリズムを外部サーバ11から受け取ると、復号化用の鍵を使用してリプルDESによって暗号化されたあらたなファームウェアやあらたな暗号化アルゴリズムを復号化する(ファームウェア復号化手段、アルゴリズム復号化手段)(S－30)。中央処理部35は、バージョンアップ前のファームウェアをバージョンアップ後の複合化したファームウェアに書き換え(ファームウェア更新手段)、バージョンアップ後のファームウェアをメモリ36に格納する。さらに、すでに記憶した暗号化アルゴリズムを復号化したあらたな暗号化アルゴリズムに書き換え(アルゴリズム更新手段)、あらたな暗号化アルゴリズムをメモリ36に格納する。暗号化していないあらたなファームウェアやあらたな暗号化アルゴリズムをサーバ11から受け取ると、中央処理部35は、バージョンアップ前のファームウェアをバージョンアップ後のファームウェアに書き換え(ファームウェア更新手段)、バージョンアップ後のファームウェアをメモリ36に格納するとともに、すでに記憶した暗号化アルゴリズムをあらたな暗号化アルゴリズムに書き換え(アルゴリズム更新手段)、あらたな暗号化アルゴリズムをメモリ36に格納する。

[0062] ファームウェアの書き換えは、それがバージョンアップされた場合、磁気カード29の仕様が変更され、カード29のフォーマットが変更された場合に行われる。暗号化アルゴリズムの書き換えは、第3者にアルゴリズムが解析されたことで、書き換えの必要が生じた場合、システム10を起動させる度毎に行う場合、日時単位や週単位、月単位で行う場合、同期がずれた後、再び同期する場合に行われる。

[0063] 図9～図14は、暗号化および復号化に使用する鍵の生成の一例を説明する図である。外部サーバ11の中央処理部とマイクロプロセッサ26の中央処理部35とは、暗号化されたファームウェアまたは暗号化アルゴリズムが磁気ヘッド19にダウンロードさ

れる度毎に、それらのメモリ36にあらかじめ格納された同一かつ有限の回帰カウンタ値を使用して互いに同期しつつ、ファームウェアまたは暗号化アルゴリズムの暗号化と復号化とに必要な同一のあらたな第2～第n鍵を順に生成する(鍵生成手段)。サーバ11の中央処理部とプロセッサ26の中央処理部35とが行う鍵生成手順の一例を説明すると、以下のとおりである。なお、回帰カウンタ値は1～20とする。ただし、回帰カウンタ値に特に限定はなく、カウンタ値を21以上とすることもできる。

[0064] 外部サーバ11が第1番目のファームウェア(新規ファームウェア)または暗号化アルゴリズム(新規アルゴリズム)を磁気ヘッド19にダウンロードする場合、サーバ11の中央処理部は、図9に示すように、メモリに格納されたカウンタテーブルから回帰カウンタ値1を選択し、ファームウェアや暗号化アルゴリズムにカウンタ値1を添付する。カウンタテーブルには、カウンタ値(1～20)の格納エリアとそれに対応する3つの鍵の格納エリア(K1, K2, K3)とが作られている。ただし、図9のカウンタデーブルでは、回帰カウンタ値2～20に対応する第2鍵～第20鍵は生成されていない。なお、カウンタ値1に対応する第1鍵(Key1)は、初期値としてシステム10の導入時に設定される。

[0065] 外部サーバ11の中央処理部は、カウンタテーブルからカウンタ値1に対応する第1鍵を取り出し、第1鍵を使用し、トリプルDES(3－Keyトリプル DES)によってファームウェアまたは暗号化アルゴリズムとカウンタ値1とを暗号化し(ファームウェア暗号化手段、アルゴリズム暗号化手段)、暗号化したファームウェアや暗号化アルゴリズムを磁気ヘッド19にダウンロードする(ファームウェア第1ダウンロード手段、アルゴリズム第1ダウンロード手段)。サーバ11の中央処理部は、暗号化したファームウェアや暗号化アルゴリズムを磁気ヘッド19にダウンロードした後、回帰カウンタ値を1から2に変更し、カウンタ値2をメモリに格納する。

[0066] 暗号化されたファームウェア(第1番目のファームウェア)または暗号化アルゴリズム(第1番目の暗号化アルゴリズム)を受け取ったマイクロプロセッサ26の中央処理部35は、図10に示すように、メモリ36に格納されたカウンタテーブルから回帰カウンタ値1を選択する。カウンタテーブルには、カウンタ値(1～20)の格納エリアとそれに対応する3つの鍵の格納エリア(K1, K2, K3)とが作られている。ただし、図10のカウンタデーブルでは、回帰カウンタ値2～20に対応する第2鍵～第20鍵は生成されていな

い。なお、カウンタ値1に対応する第1鍵(Key1)は、外部サーバ11のメモリに格納された第1鍵と同一であり、初期値としてシステム10の導入時に設定される。

[0067] マイクロプロセッサ26の中央処理部35は、カウンタテーブルからカウンタ値1に対応する第1鍵を取り出し、第1鍵を使用し、トリプルDES(3－Keyトリプル DES)によって暗号化されたファームウェアや暗号化アルゴリズムを復号化して平文ファームウェア、平文アルゴリズムを取得する(ファームウェア復号化手段、アルゴリズム復号化手段)。中央処理部35は、ファームウェアや暗号化アルゴリズムを復号化した後、それらをメモリ36に格納するとともに(ファームウェア記憶手段、アルゴリズム記憶手段)、回帰カウンタ値を1から2に変更し、カウンタ値2をメモリ36に格納する。

[0068] 外部サーバ11は、マイクロプロセッサ26が現在使用しているファームウェアや暗号化アルゴリズムの使用を中止させ、メモリに格納されたファームウェアや暗号化アルゴリズムの中からあらたなファームウェアやあらたなアルゴリズムを選択し、そのファームウェアやアルゴリズムを使用させることができる。サーバ11が第2番目のファームウェア(バージョンアップファームウェア)または第2番目の暗号化アルゴリズム(あらたな暗号化アルゴリズム)を磁気ヘッド19にダウンロードする場合、外部サーバ11の中央処理部は、図11に示すように、メモリに格納されたカウンタテーブルから回帰カウンタ値2を選択し、第2番目のファームウェアや暗号化アルゴリズムにカウンタ値2を添付する。

[0069] 外部サーバ11の中央処理部は、カウンタ値1に対応する第1鍵(初期値)とカウンタ値1とを一方向ハッシュ関数によってハッシュ化したハッシュ出力値を生成し、そのハッシュ出力値をカウンタ値2に対応する第2鍵(Key2)とする(鍵生成手段)。第2鍵(Key2)となるハッシュ出力値は、カウンタテーブルのカウンタ値2に対応する鍵格納エリア(K1, K2, K3)に書き込まれる。なお、図11のカウンタデーブルでは、回帰カウンタ値3～20に対応する第3鍵～第20鍵は生成されていない。

[0070] 外部サーバ11の中央処理部は、カウンタテーブルからカウンタ値2に対応する第2鍵を取り出し、第2鍵を使用し、トリプルDES(3－Keyトリプル DES)によってファームウェアや暗号化アルゴリズムを暗号化(カウンタ値2を含む)し(ファームウェア暗号化手段、アルゴリズム暗号化手段)、暗号化したファームウェアや暗号化アルゴリズム

を磁気ヘッド19にダウンロードする(ファームウェア第2ダウンロード手段、アルゴリズム第2ダウンロード手段)。サーバ11の中央処理部は、暗号化したファームウェアまたは暗号化アルゴリズムを磁気ヘッド19にダウンロードした後、回帰カウンタ値を2から3に変更し、カウンタ値3をメモリに格納する。

[0071] 暗号化されたファームウェア(第2番目のファームウェア)または暗号化アルゴリズム(第2番目の暗号化アルゴリズム)を受け取ったマイクロプロセッサ26の中央処理部35は、図12に示すように、メモリ36に格納されたカウンタテーブルから回帰カウンタ値2を選択する。中央処理部35は、カウンタ値1に対応する第1鍵(初期値)とカウンタ値1とを一方向ハッシュ関数によってハッシュ化したハッシュ出力値を生成し、そのハッシュ出力値をカウンタ値2に対応する第2鍵(Key2)とする(鍵生成手段)。中央処理部35が使用するハッシュ関数はサーバ11の中央処理部が使用するそれと同一であり、生成した第2鍵(Key2)はサーバ11の中央処理部が生成したそれと同一である。第2鍵(Key2)となるハッシュ出力値は、カウンタテーブルのカウンタ値2に対応する鍵格納エリア(K1, K2, K3)に書き込まれる。なお、図12のカウンタデーブルでは、回帰カウンタ値3～20に対応する第3鍵～第20鍵は生成されていない。

[0072] マイクロプロセッサ26の中央処理部35は、カウンタテーブルからカウンタ値2に対応する第2鍵を取り出し、第2鍵を使用し、トリプルDES(3－Keyトリプル DES)によって暗号化されたファームウェアや暗号化アルゴリズムを復号化して平文ファームウェア、平文アルゴリズムを取得する(ファームウェア復号化手段、アルゴリズム復号化手段)。中央処理部35は、ファームウェアや暗号化アルゴリズムを復号化した後、それらをメモリ36に格納するとともに(ファームウェア記憶手段、アルゴリズム記憶手段)、回帰カウンタ値を2から3に変更し、カウンタ値3をメモリ36に格納する。

[0073] 外部サーバ11が第3番目のファームウェア(バージョンアップファームウェア)または第3番目の暗号化アルゴリズム(あらたな暗号化アルゴリズム)を磁気ヘッドにダウンロードする場合、サーバ11の中央処理部は、図13に示すように、メモリに格納されたカウンタテーブルから回帰カウンタ値3を選択し、第3番目のファームウェアや暗号化アルゴリズムにカウンタ値3を添付する。

[0074] 外部サーバ11の中央処理部は、カウンタ値2に対応する第2鍵(Key2、ハッシュ値

)とカウンタ値2とを一方向ハッシュ関数によってハッシュ化したハッシュ出力値を生成し、そのハッシュ出力値をカウンタ値3に対応する第3鍵(Key3)とする(鍵生成手段)。第3鍵(Key3)となるハッシュ出力値は、カウンタテーブルのカウンタ値3に対応する鍵格納エリア(K1, K2, K3)に書き込まれる。なお、図13のカウンタデーブルでは、回帰カウンタ値4～20に対応する第4鍵～第20鍵は生成されていない。

[0075] 外部サーバ11の中央処理部は、カウンタテーブルからカウンタ値3に対応する第3鍵を取り出し、第3鍵を使用し、トリプルDES(3－KeyトリプルDES)によってファームウェアや暗号化アルゴリズムを暗号化(カウンタ値3を含む)し(ファームウェア暗号化手段、アルゴリズム暗号化手段)、暗号化したファームウェアや暗号化アルゴリズムを磁気ヘッド19にダウンロードする(ファームウェア第2ダウンロード手段、アルゴリズム第2ダウンロード手段)。サーバ11の中央処理部は、暗号化したファームウェアまたは暗号化アルゴリズムを磁気ヘッド19にダウンロードした後、回帰カウンタ値を3から4に変更し、カウンタ値4をメモリに格納する。

[0076] 暗号化されたファームウェア(第3番目のファームウェア)または暗号化アルゴリズム(第3番目の暗号化アルゴリズム)を受け取ったマイクロプロセッサ26の中央処理部35は、図14に示すように、メモリ36に格納されたカウンタテーブルから回帰カウンタ値3を選択する。中央処理部35は、カウンタ値2に対応する第2鍵(Key2)とカウンタ値2とを一方向ハッシュ関数によってハッシュ化したハッシュ出力値を生成し、そのハッシュ出力値をカウンタ値3に対応する第3鍵(Key3)とする(鍵生成手段)。中央処理部35が生成した第3鍵(Key3)は外部サーバ11の中央処理部が生成したそれと同一である。第3鍵(Key3)となるハッシュ出力値は、カウンタテーブルのカウンタ値3に対応する鍵格納エリア(K1, K2, K3)に書き込まれる。なお、図14のカウンタデーブルでは、回帰カウンタ値4～20に対応する第4鍵～第20鍵は生成されていない。

[0077] マイクロプロセッサ26の中央処理部35は、カウンタテーブルからカウンタ値3に対応する第3鍵を取り出し、第3鍵を使用し、トリプルDES(3－KeyトリプルDES)によって暗号化されたファームウェアや暗号化アルゴリズムを復号化して平文ファームウェア、平文アルゴリズムを取得する(ファームウェア復号化手段、アルゴリズム復号化手段)。中央処理部35は、ファームウェアや暗号化アルゴリズムを復号化した後、そ

れらをメモリ36に格納するとともに（ファームウェア記憶手段、アルゴリズム記憶手段）、回帰カウンタ値を3から4に変更し、カウンタ値4をメモリ36に格納する。

[0078] このように、外部サーバ11の中央処理部とマイクロプロセッサ26の中央処理部35とは、回帰カウンタ値1～20を順番に使って互いに同期しつつ、一方向ハッシュ関数を使用して第2～第n鍵を生成する。回帰カウンタ値が20を超えると、サーバ11の中央処理部とプロセッサ26の中央処理部35とは、再びカウンタ値1を使用し、第21鍵～第40鍵を順に生成する。サーバ11の中央処理部とプロセッサ26の中央処理部35とは、第21鍵を生成すると、鍵格納エリアに格納された第1鍵を第21鍵に書き換え、第22鍵を生成すると、鍵格納エリアに格納された第2鍵を第22鍵に書き替える。

[0079] この磁気カード読み取りシステム10は、相互認証手段を実行することで外部サーバ11の中央処理部とマイクロプロセッサ26の中央処理部35とが互いの正当性を判断することができるから、偽サーバが磁気ヘッド19に接続された場合や偽磁気ヘッドが外部サーバ11に接続された場合であっても、それを見破ることができる。このシステム10は、第3者が偽サーバを利用して磁気ヘッド19にアクセスすることはできず、ファームウェアの改竄による第3者の磁気カード29の不正利用を防ぐことができる。また、このシステム10は、第3者が偽磁気ヘッドを利用して外部サーバ11にアクセスすることはできず、サーバ11から偽磁気ヘッドに暗号化アルゴリズムがダウンロードされることはない。

[0080] システム10は、外部サーバ11の中央処理部とマイクロプロセッサ26の中央処理部35とが第2～第n鍵を個別に生成するから、サーバ11からプロセッサ26へ鍵を送信する必要はなく、鍵の送信過程における鍵の不正な取得を防ぐことができる。システム10は、サーバ11の中央処理部が常に別の鍵を使用してファームウェアや暗号化アルゴリズムの暗号化を行い、プロセッサ26の中央処理部35が常に別の鍵を使用してファームウェアや暗号化アルゴリズムの復号化を行うから、鍵を第3者に取得されたとしても、ファームウェアや暗号化アルゴリズムを復号化することはできない。また、第2～第n鍵にハッシュ値を使用するから、たとえ鍵が第3者に不正に取得されたとしても、鍵の解読をすることはできず、第3者による鍵の使用を確実に防ぐことができる。

[0081] システム10は、外部サーバ11の中央処理部とマイクロプロセッサ26の中央処理部

35とが同一かつ有限の回帰カウンタ値を使用して互いに同期しつつ、第2～第n鍵を順に生成するから、サーバ11が生成する鍵とプロセッサ26が生成する鍵とを一致させることができ、生成した鍵の不一致による暗号データの復号不能を防ぐことができる。また、第2～第n鍵となるハッシュ出力値に回帰カウンタ値をハッシュ化したハッシュ出力値が含まれるから、第3者がシステム10に不正に進入したとしても、ハッシュ化した回帰カウンタ値を解読することはできず、サーバ11の中央処理部とプロセッサ26の中央処理部35とがどのカウンタ値を使用して同期しているかを判別することができない。

[0082] システム10の稼働中に外部サーバ11の中央処理部とマイクロプロセッサ26の中央処理部35との同期がずれると、サーバ11の中央処理部が生成した鍵とプロセッサ26の中央処理部35が生成したそれとが異なり、中央処理部からダウンロードされた暗号データを中央処理部35が復号化することができない。この場合、プロセッサ26の中央処理部35は、生成した鍵による復号化が不可能であると判断し、復号化不能をサーバ11に送信するとともに(復号化不能情報送信手段)、サーバ11との再同期を要求する(再同期要求手段)。

[0083] マイクロプロセッサ26の中央処理部35は、カードリーダ12のコントローラに外部サーバ11へのアクセスを要求するとともに、メモリ36に格納されたデータ送受信用の鍵を使用し、トリプルDESによって復号化不能情報と再同期要求とを暗号化する。サーバ11とカードリーダ12とがインターネットを介して接続されると、プロセッサ26の中央処理部35は、暗号化した復号化不能情報と再同期要求とをサーバ11に送信する。プロセッサ26の中央処理部36と再同期要求を受け取ったサーバ11の中央処理部とは、それらの正当性を判断する外部認証と内部認証と(図6, 7参照)を行う(相互認証手段)。サーバ11の中央処理部とプロセッサ26の中央処理部35とは、相互認証による互いの認証結果を正当であると判断すると、回帰カウンタ値を1(初期値)に戻して再び同期を開始する。サーバ11の中央処理部とプロセッサ26の中央処理部35とは、カウンタ値を1に戻すと、再び第1鍵を使用して暗号化および復号化を行う。

[0084] システム10は、外部サーバ11とマイクロプロセッサ26とが生成した鍵に不一致が生じたとしても、サーバ11とプロセッサ26とが回帰カウンタ値を1に戻して再び同期する

ことができるから、サーバ11が生成する鍵とプロセッサ26が生成する鍵とを再度一致させることができ、生成した鍵の不一致によるファームウェアや暗号化アルゴリズムの復号不能を防ぐことができる。なお、システム10が連続して稼働し、相互認証を日時単位や週単位、月単位で行う場合、サーバ11の中央処理部とプロセッサ26の中央処理部35とは、相互認証による互いの認証結果を正当であると判断すると、回帰カウンタ値を1に戻して再び同期を開始する。以後の手順は、図9～図14に基づいて説明したそれと同一である。

[0085] 一方向ハッシュ関数には、SHA－1(Secure Hash Algorithm 1)、MD2, MD4, MD5(Message Digest2, 4, 5)、RIPEMD－80、RIPEMD－128、RIPEMD－160、N－Hashのいずれかを使用する。それらハッシュ関数は、外部サーバ11のメモリとホストコンピュータ13のメモリとに格納されている。

[0086] 暗号化アルゴリズムとしては、DESの他に、RSA、AES(Advanced Encryption Standard)、IDEA(International Data Encryption Algorithm)、FEAL－N／NX(Fast Encryption Algorithm)、MULTI2(Multimedia Encryption2)、MISTY、SXAL(Substitution Xor
Algorithm)、MBAL(Multi Block Algorithm)、RC2、RC5、ENCRiP、SAFER(Secure And Fast Encryption Routine)、Blowfish、Skipjack、Khufu、Khafre、CAST、GOST28147－89のいずれかを使用することもできる。それらアルゴリズムは、外部サーバ11のメモリとホストコンピュータ13のメモリとに格納されている。

[0087] このシステム10では、外部サーバ11とマイクロプロセッサ26とが図9～図14に示す鍵の生成を行うことなく、サーバ11がプロセッサ26にファームウェアや暗号化アルゴリズムをダウンロードすることもできる。その一例を説明すると、以下のとおりである。外部サーバ11がカードリーダ12のURLを利用し、インターネットを介してカードリーダ12にアクセスする(アクセス手段)。または、カードリーダ12が外部サーバ11のURLを利用し、インターネットを介してサーバ11にアクセスする。サーバ11とカードリーダ12とがインターネットを介して接続されると、サーバ11の中央処理部とマイクロプロセッサ26の中央処理部35とがコントローラを介して接続される。サーバ11の中央処理部とプロセッサ26の中央処理部35とは、それらの正当性を判断する外部認証と内部認

証と(図6，7参照)を行う(相互認証手段)。サーバ11の中央処理部とプロセッサ26の中央処理部35とが相互認証による互いの認証結果を正当であると判断すると、サーバ11からファームウェアや暗号化アルゴリズムの磁気ヘッド19へのダウンロードが可能となり、サーバ11とプロセッサ26との間でダウンロード処理が行われる。

[0088] 外部サーバ11の中央処理部は、メモリに格納された情報送受信用の鍵を使用し、トリプルDESによってあらたなファームウェアや暗号化アルゴリズムを暗号化し(ファームウェア暗号化手段、アルゴリズム暗号化手段)、暗号化したファームウェアやアルゴリズムを磁気ヘッド19にダウンロードする(ファームウェア第1ダウンロード手段、アルゴリズム第1ダウンロード手段)。サーバ11からダウンロードされたファームウェアや暗号化アルゴリズムは、カードリーダ12のコントローラのメモリに一時的に保管された後、磁気ヘッド19に出力される。

[0089] マイクロプロセッサ26の中央処理部35は、暗号化されたファームウェアや暗号化アルゴリズムをサーバ11から受け取ると、メモリ36に格納された情報送受信用の鍵を使用し、トリプルDESによって暗号化されたファームウェアやアルゴリズムを復号化して平文ファームウェア、平文アルゴリズムを取得する(ファームウェア復号化手段、アルゴリズム復号化手段)、復号化したファームウェアやアルゴリズムをメモリに格納する(ファームウェア記憶手段、アルゴリズム記憶手段)。

[0090] 外部サーバ11は、マイクロプロセッサ26が現在使用しているファームウェアや暗号化アルゴリズムの使用を中止させ、メモリに格納されたファームウェアや暗号化アルゴリズムの中からあらたなファームウェアやあらたなアルゴリズムを選択し、そのファームウェアやアルゴリズムを使用させることができる。サーバ11は、あらたなファームウェアやあらたな暗号化アルゴリズムをプロセッサ26に使用させる場合、プロセッサ26に既存のファームウェアや暗号化アルゴリズムの書き換えを指示する(更新指令)。なお、外部認証と内部認証と(図6，7参照)がすでに行われ、サーバ11とプロセッサ26とが相互認証による互いの認証結果を正当であると判断したものとする。

[0091] 外部サーバ11の中央処理部は、メモリに格納された情報送受信用の鍵を使用し、トリプルDESによって更新指令とあらたなファームウェアやあらたな暗号化アルゴリズムとを暗号化し(ファームウェア暗号化手段、アルゴリズム暗号化手段)、暗号化した

更新指令やファームウェア、アルゴリズムを磁気ヘッド19にダウンロードする(ファームウェア第2ダウンロード手段、アルゴリズム第2ダウンロード手段)。サーバ11からダウンロードされた更新指令やファームウェア、暗号化アルゴリズムは、カードリーダ12のコントローラのメモリに一時的に保管された後、磁気ヘッド19に出力される。

[0092] マイクロプロセッサ26の中央処理部35は、暗号化された更新指令やファームウェア、暗号化アルゴリズムを外部サーバ11から受け取ると、メモリ36に格納された情報送受信用の鍵を使用し、トリプルDESによって暗号化された更新指令とファームウェアやアルゴリズムとを復号化する(ファームウェア復号化手段、アルゴリズム復号化手段)。中央処理部35は、メモリ36に格納された既存のファームウェアを復号化したあらたなファームウェアに書き換え(ファームウェア更新手段)、あらたなファームウェアをメモリ36に格納する。さらに、メモリ36に格納された既存のアルゴリズムを復号化したあらたなアルゴリズムに書き換え(アルゴリズム更新手段)、あらたなアルゴリズムをメモリ36に格納する。中央処理部35は、更新完了をサーバ11に通知する(更新完了通知)。中央処理部35は、メモリ36に格納された情報送受信用の鍵を使用し、トリプルDESによって更新完了通知を暗号化し、暗号化した更新完了通知をサーバ11に送信する。

[0093] 外部サーバ11は、現在使用しているハッシュ関数の使用を中止し、メモリに格納されたハッシュ関数の中からあらたなハッシュ関数を選択し、そのハッシュ関数を使用することができる。ハッシュ関数の変更は、システム10を起動させる度毎に行う場合、日時単位や週単位、月単位で行う場合、同期がずれた後、再び同期するときに行う場合がある。サーバ11は、あらたなハッシュ関数を使用する場合、マイクロプロセッサ26に既存のハッシュ関数の書き換えを指示する(関数変更指令)。サーバ11の中央処理部は、カードリーダ12にアクセスする。サーバ11とカードリーダ12とがインターネットを介して接続されると、サーバ11の中央処理部とプロセッサ26の中央処理部35とは、それらの正当性を判断する外部認証と内部認証と(図6, 7参照)を行う(相互認証手段)。サーバ11の中央処理部とプロセッサ26の中央処理部35とが相互認証による互いの認証結果を正当であると判断すると、サーバ11の中央処理部は、メモリに格納されたデータ送受信用の鍵を使用し、トリプルDESによって関数変更指令と

あらたなハッシュ関数とを暗号化した後、暗号化した関数変更指令とハッシュ関数とをプロセッサ26に送信する。

[0094] マイクロプロセッサ26の中央処理部35は、関数変更指令とハッシュ関数とを受信すると、メモリ36に格納されたデータ送受信用の鍵を使用し、トリプルDESによって暗号化された関数変更指令とハッシュ関数とを復号化する。プロセッサ26の中央処理部35は、メモリ36に格納した既存のハッシュ関数を復号化したあらたなハッシュ関数に変更した後、変更完了を外部サーバ11に通知する(変更完了通知手段)。中央処理部35は、メモリ36に格納されたデータ送受信用の鍵を使用し、トリプルDESによって変更完了通知を暗号化し、暗号化した変更完了通知をサーバ11に送信する。このシステム10は、関数変更指令やハッシュ関数を暗号化してハッシュ関数の変更を行うから、使用するハッシュ関数を第3者に取得されることはなく、第3者によるハッシュ関数の解読を防ぐことができる。

[0095] この磁気カード読み取りシステム10は、ファームウェアまたは暗号化アルゴリズムが外部サーバ11から磁気ヘッド19にダウンロードされると、プロセッサ26がそのファームウェアや暗号化アルゴリズムをメモリ36に格納するから、磁気ヘッド19が市場に出荷された後や磁気ヘッド19が磁気カードリーダ12に設置された後において、サーバ11からダウンロードされたファームウェアや暗号化アルゴリズムをプロセッサ26に随時格納することができる。

[0096] システム10は、磁気ヘッド19の出荷後や設置後でも、各種のファームウェアに対応することができ、それらファームウェアを利用することで、磁気ヘッド19の動作環境に応じてプロセッサ26の演算・記憶機能や外部ハードウェアの最適な制御を行うことができる。このシステム10は、磁気ヘッド19の出荷後や設置後において、磁気ヘッド19を磁気カード29の各種フォーマットに対応させることができ、磁気カード29の各種仕様に適応しつつ、それらカード29に記憶されたデータを磁気ヘッド19に確実に読み取らせることができる。このシステム10は、磁気ヘッド19の出荷後や設置後でも、各種の暗号化アルゴリズムを利用することができ、それらアルゴリズムを利用してカードデータを暗号化することができる。このシステム10では、プロセッサ26がバージョンアップ前のファームウェアをバージョンアップ後のファームウェアに書き換えるから、磁

気ヘッド19の出荷後や設置後において、ファームウェアのバージョンアップが行われたとしても、バージョンアップ後のファームウェアに即座に対応することができる。

[0097] 図15は、磁気ヘッド19とホストコンピュータ13との間で行われる処理の一例を示すブロック図である。このシステム10を起動させると、ホストコンピュータ13の中央処理部とマイクロプロセッサ26の中央処理部35とは、メモリーテスト(S－50)とコードサイニング(S－51)とを行う(初期テスト)。初期テストが終了し、その結果が正しい場合、コンピュータ13の中央処理部とプロセッサ26の中央処理部35とは、それらの正当性を判断する相互認証を行う(相互認証手段)。相互認証は、コンピュータ13が磁気ヘッド19の正当性を認証する外部認証(S－52)を行った後、磁気ヘッド19がコンピュータ13の正当性を認証する内部認証(S－53)を行う。

[0098] コンピュータ13の中央処理部とマイクロプロセッサ26の中央処理部35とが相互認証による互いの認証結果を正当であると判断すると、磁気カードリーダ12における磁気カード29の読み取りが可能となり、コンピュータ13とプロセッサ26との間でメイン処理(S－54)が行われる。逆に、コンピュータ13とプロセッサ26との少なくとも一方が認証結果を不可であると判断すると、カードリーダ12による磁気カード29の読み取りができず、読み取り不能情報がコンピュータ13のディスプレイに表示される。相互認証は、システム10を起動させる度毎に行われる他、システム10を連続して稼働させる場合は日時単位や週単位、月単位で行われ、また、後記するように、コンピュータ13の中央処理部とプロセッサ26の中央処理部35との同期が不一致になった場合にも行われる。

[0099] 図16は、外部認証の一例を示すラダー図であり、図17は、内部認証の一例を示すラダー図である。外部認証における認証手順は、以下のとおりである。ホストコンピュータ13の中央処理部がマイクロプロセッサ26の中央処理部35に乱数(認証子)の生成と送信とを要求する(S－60)。プロセッサ26の中央処理部35は、コンピュータ13の指令に従って64bit乱数を生成し、生成した乱数をコンピュータ13に送信する(S－61)。64bit乱数を取得したコンピュータ13の中央処理部は、メモリに格納された認証用の鍵を使用し、トリプルDESによって乱数を暗号化した後、暗号化した乱数をプロセッサ26に送信する(S－62)。

[0100] マイクロプロセッサ26の中央処理部35は、メモリ36に格納された認証用の鍵を使用し、トリプルDESによって暗号化された乱数を復号化する(S－63)。プロセッサ26の中央処理部35は、それが生成した乱数と復号化した乱数とを比較し、両者が同一であれば認証結果を正当であると判断し、認証結果正当情報をコンピュータ13に送信する。一方、生成した乱数と復号化した乱数とが異なる場合、認証結果を不可であると判断し、認証結果不可情報と磁気カード29の読み取り不可情報とをコンピュータ13に送信する。コンピュータ13は、マイクロプロセッサ26から外部認証結果を取得する(S－64)。

[0101] 内部認証における認証手順は、以下のとおりである。コンピュータ13の中央処理部は、64bit乱数(認証子)を生成し、それをマイクロプロセッサ26に送信する(S－65)。64bit乱数を取得したプロセッサ26の中央処理部35は、メモリ36に格納された認証用の鍵を使用し、トリプルDESによって乱数を暗号化した後、暗号化した乱数をコンピュータ13に送信する(S－66)。コンピュータ13の中央処理部は、メモリに格納された認証用の鍵を使用し、トリプルDESによって暗号化された乱数を復号化する(S－67)。コンピュータ13の中央処理部は、それが生成した乱数と復号化した乱数とを比較し、両者が同一であれば認証結果を正当であると判断する。一方、生成した乱数と復号化した乱数とが異なる場合、認証結果を不可であると判断し、カードリーダ12における磁気カード29の読み取りを不可とする。

[0102] 図18は、このシステム10におけるメイン処理の一例を示すラダー図である。図19～図24は、暗号化および復号化に使用する鍵の生成の他の一例を説明する図である。相互認証の結果が正当であり、磁気カード29の読み取りが可能となった後、カード所持者がカード挿入口16から磁気カード29を挿入すると、モータ22が駆動してカード29が案内レール18を移動する。カード29が挿入口16を通過すると、光センサ20がそれを検出し、カード挿入信号が光センサ20から出力されてカードリーダ12のコントローラに入力される。コントローラは、カード挿入信号を受け取ると、磁気ヘッド19のマイクロプロセッサ26に、カード29に記憶されたカードデータの読み取り開始指令を出力する。磁気カード29が磁気ヘッド19を通過するとともに排出口17から排出されると、光センサ20がそれを検出し、カード通過信号が光センサ20から出力されて

カードリーダ12のコントローラに入力される。コントローラは、カード通過信号を受け取ると、磁気ヘッド19のプロセッサ26にカードデータの読み取り停止指令を出力するとともに、モータ22の駆動を停止する。

[0103] 磁気カード29の磁化された磁性層32が磁気ヘッド19のコア24の先端部27(コア24のギャップ)を通過すると、コア24内に磁束が発生し、磁束と鎖交する方向へ誘導起電力が生じてコイルに電流が流れる。コイルに流れる電流は、その値が磁束の変化にともなって変わる。磁気カード29の磁性層32に記憶されたカードデータは、コイルによってアナログ信号として取り出され、コイルに接続されたA/D変換チップ25に入力される。A/D変換チップ25は、コイルから入力されたアナログ信号をデジタル信号に変換する。デジタル信号は、A/D変換チップ25からマイクロプロセッサ26に入力され、プロセッサ26のメモリ36に格納される。

[0104] システム10の稼働中、ホストコンピュータ13の中央処理部は、マイクロプロセッサ26のメモリ36に処理すべきカードデータが存在するかを所定間隔でプロセッサ26に問い合わせる(データ確認指令)。コンピュータ13の中央処理部は、メモリに格納された情報送受信用の鍵を使用し、トリプルDESによってデータ確認指令を暗号化し、暗号化したデータ確認指令をプロセッサ26に送信する(S-68)。なお、所定間隔は、秒単位またはミリ秒単位であることが好ましい。プロセッサ26の中央処理部35は、データ確認指令を受信すると、メモリ36に格納された情報送受信用の鍵を使用し、トリプルDESによって暗号化されたデータ確認指令を復号化する。プロセッサ26の中央処理部35は、コンピュータ13からのデータ確認指令に従ってメモリ36を検索し、磁気カード29のカードデータがデジタル信号としてメモリ36に格納されている場合、データ保有をコンピュータ13に返答し(データ保有情報)、カードデータがメモリ36にない場合、データ非保有をコンピュータ13に返答する(データ非保有情報)。プロセッサ26は、情報送受信用の鍵を使用し、トリプルDESによってデータ保有情報やデータ非保有情報を暗号化し、暗号化したデータ保有情報やデータ非保有情報をコンピュータ13に送信する(S-69)。

[0105] ホストコンピュータ13の中央処理部は、データ保有情報やデータ非保有情報を受信すると、情報送受信用の鍵を使用し、トリプルDESによってデータ保有情報やデ

ータ非保有情報を復号化する。コンピュータ13の中央処理部は、データ非保有情報を受信すると、暗号化したデータ確認指令を所定の間隔で再びマイクロプロセッサ26に送信し、メモリ36に処理すべきカードデータが存在するかをプロセッサ26に問い合わせる(データ確認指令)。コンピュータ13の中央処理部は、データ保有情報を受信すると、プロセッサ26のメモリ36に格納されたカードデータの送信をプロセッサ26に要求する(データ送信指令)。コンピュータ13の中央処理部は、情報送受信用の鍵を使用し、トリプルDESによってデータ送信指令を暗号化し、暗号化したデータ送信指令をプロセッサ26に送信する(S－70)。プロセッサ26の中央処理部35は、データ送信指令を受信すると、情報送受信用の鍵を使用し、トリプルDESによって暗号化されたデータ送信指令を復号化する。

[0106] マイクロプロセッサ26の中央処理部35は、メモリ36からデジタル信号(カードデータ)と暗号用の鍵とを取り出し、その鍵を使用してデジタル信号を暗号化して暗号データとする(データ暗号化手段)(S－71)。中央処理部35は、暗号データをホストコンピュータ13に送信する(暗号データ送信手段)。コンピュータ13は、暗号データを増幅する増幅回路(図示せず)を有し、メモリから復号用の鍵を取り出し、その鍵を使用して増幅回路で増幅した暗号データを復号化する(データ復号化手段)(S－72)。コンピュータ13は、復号化したデジタル信号(平文カードデータ)を文字情報としてディスプレイに表示することができ(データ出力手段)、復号化したデジタル信号(平文カードデータ)を印字情報としてプリンタに印字させることができる(データ出力手段)。コンピュータ13は、暗号化されたデジタル信号または復号化されたデジタル信号をメモリに格納する(データ記憶手段)。コンピュータ13は、暗号データを復号化すると、暗号化したデータ確認指令を所定の間隔で再びプロセッサ26に送信し、メモリ36に処理すべきカードデータが存在するかをプロセッサ26に問い合わせる(データ確認指令)。

[0107] コンピュータ13の中央処置部とマイクロプロセッサ26の中央処理部35とは、暗号化されたデジタル信号がコンピュータ13に入力される度毎に、メモリとメモリ36とにあらかじめ格納された同一かつ有限の回帰カウンタ値を使用して互いに同期しつつ、デジタル信号の暗号化と復号化とに必要な同一のあらたな第2～第n鍵を順に生成

する(鍵生成手段)。コンピュータ13の中央処置部とプロセッサ26の中央処理部36とが行う鍵生成手順の一例を、図19～図24に基づいて説明すると、以下のとおりである。なお、回帰カウンタ値は1～20とする。ただし、回帰カウンタ値に特に限定はなく、カウンタ値を21以上とすることもできる。

[0108] システム10を起動した後、第1番目のデジタル信号(カードデータ)がA／D変換チップ25からマイクロプロセッサ26に入力され、デジタル信号をメモリ36に格納した後、データ送信指令を受信すると、プロセッサ26の中央処理部35は、図19に示すように、メモリ36に格納されたカウンタテーブルから回帰カウンタ値1を選択し、デジタル信号にカウンタ値1を添付する。カウンタテーブルには、カウンタ値(1～20)の格納エリアとそれに対応する3つの鍵の格納エリア(K1, K2, K3)とが作られている。ただし、図19のカウンタデーブルでは、回帰カウンタ値2～20に対応する第2鍵～第20鍵は生成されていない。なお、カウンタ値1に対応する第1鍵(Key1)は、初期値としてシステム10の導入時に設定される。

[0109] マイクロプロセッサ26の中央処理部35は、カウンタテーブルからカウンタ値1に対応する第1鍵を取り出し、第1鍵を使用し、トリプルDES(3－KeyトリプルDES)によってデジタル信号とカウンタ値1とを暗号化して暗号データとし(データ暗号化手段)、暗号データをコンピュータ13に送信する(データ送信手段)。プロセッサ26の中央処理部35は、暗号データをコンピュータ13に送信した後、回帰カウンタ値を1から2に変更し、カウンタ値2をメモリ36に格納するとともに、第1番目のデジタル信号(カードデータ)をメモリ36から消去する。

[0110] 第1番目の暗号データを受信したホストコンピュータ13の中央処理部は、図20に示すように、メモリに格納されたカウンタテーブルから回帰カウンタ値1を選択する。カウンタテーブルには、カウンタ値(1～20)の格納エリアとそれに対応する3つの鍵の格納エリア(K1, K2, K3)とが作られている。ただし、図20のカウンタデーブルでは、回帰カウンタ値2～20に対応する第2鍵～第20鍵は生成されていない。なお、カウンタ値1に対応する第1鍵(Key1)は、マイクロプロセッサ26のメモリ36に格納された第1鍵と同一であり、初期値としてシステム10の導入時に設定される。コンピュータ13の中央処理部は、カウンタテーブルからカウンタ値1に対応する第1鍵を取り出し、

第1鍵を使用し、トリプルDES(3－KeyトリプルDES)によって暗号データを復号化してデジタル信号(平文カードデータ)を取得する。コンピュータ13の中央処理部は、暗号データを復号化した後、回帰カウンタ値を1から2に変更し、カウンタ値2をメモリに格納する。

[0111] 第2番目のデジタル信号(カードデータ)がA／D変換チップ25からマイクロプロセッサ26に入力され、デジタル信号をメモリ36に格納した後、データ送信指令を受信すると、プロセッサ26の中央処理部35は、図21に示すように、メモリ36に格納されたカウンタテーブルから回帰カウンタ値2を選択し、デジタル信号にカウンタ値2を添付する。プロセッサ26の中央処理部36は、カウンタ値1に対応する第1鍵(初期値)とカウンタ値1とを一方向ハッシュ関数によってハッシュ化したハッシュ出力値を生成し、そのハッシュ出力値をカウンタ値2に対応する第2鍵(Key2)とする(鍵生成手段)。第2鍵(Key2)となるハッシュ出力値は、カウンタテーブルのカウンタ値2に対応する鍵格納エリア(K1, K2, K3)に書き込まれる。なお、図21のカウンタテーブルでは、回帰カウンタ値3～20に対応する第3鍵～第20鍵は生成されていない。

[0112] マイクロプロセッサ26の中央処理部35は、カウンタテーブルからカウンタ値2に対応する第2鍵を取り出し、第2鍵を使用し、トリプルDES(3－KeyトリプルDES)によってデジタル信号を暗号化(カウンタ値2を含む)して暗号データとし(データ暗号化手段)、暗号データをコンピュータ13に送信する。プロセッサ26の中央処理部35は、暗号データをコンピュータ13に送信した後、回帰カウンタ値を2から3に変更し、カウンタ値3をメモリ36に格納するとともに、第2番目のデジタル信号(カードデータ)をメモリ36から消去する。

[0113] 第2番目の暗号データを受信したコンピュータ13は、図22に示すように、メモリに格納されたカウンタテーブルから回帰カウンタ値2を選択する。コンピュータ13の中央処理部は、カウンタ値1に対応する第1鍵(初期値)とカウンタ値1とを一方向ハッシュ関数によってハッシュ化したハッシュ出力値を生成し、そのハッシュ出力値をカウンタ値2に対応する第2鍵(Key2)とする(鍵生成手段)。コンピュータ13の中央処理部が使用するハッシュ関数はマイクロプロセッサ26の中央処理部35が使用するそれと同一であり、生成した第2鍵(Key2)はプロセッサ26の中央処理部35が生成したそれと

同一である。第2鍵(Key2)となるハッシュ出力値は、カウンタテーブルのカウンタ値2に対応する鍵格納エリア(K1, K2, K3)に書き込まれる。なお、図22のカウンタテーブルでは、回帰カウンタ値3～20に対応する第3鍵～第20鍵は生成されていない。コンピュータ13の中央処理部は、カウンタテーブルからカウンタ値2に対応する第2鍵を取り出し、第2鍵を使用し、トリプルDES(3－KeyトリプルDES)によって暗号データを復号化してデジタル信号(平文カードデータ)を取得する。コンピュータ13の中央処理部は、暗号データを復号化した後、回帰カウンタ値を2から3に変更し、カウンタ値3をメモリに格納する。

[0114] 第3番目のデジタル信号(カードデータ)がA／D変換チップ25からマイクロプロセッサ26に入力され、デジタル信号をメモリ36に格納した後、データ送信指令を受信すると、プロセッサ26の中央処理部35は、図23に示すように、メモリ36に格納されたカウンタテーブルから回帰カウンタ値3を選択し、デジタル信号にカウンタ値3を添付する。プロセッサ26の中央処理部35は、カウンタ値2に対応する第2鍵(Key2、ハッシュ値)とカウンタ値2とを一方向ハッシュ関数によってハッシュ化したハッシュ出力値を生成し、そのハッシュ出力値をカウンタ値3に対応する第3鍵(Key3)とする(鍵生成手段)。第3鍵(Key3)となるハッシュ出力値は、カウンタテーブルのカウンタ値3に対応する鍵格納エリア(K1, K2, K3)に書き込まれる。なお、図12のカウンタテーブルでは、回帰カウンタ値4～20に対応する第4鍵～第20鍵は生成されていない。

[0115] マイクロプロセッサ26の中央処理部35は、カウンタテーブルからカウンタ値3に対応する第3鍵を取り出し、第3鍵を使用し、トリプルDES(3－KeyトリプルDES)によってデジタル信号を暗号化(カウンタ値3を含む)して暗号データとし(暗号化手段)、暗号データをコンピュータ13に送信する。プロセッサ26の中央処理部35は、暗号データをコンピュータ13に送信した後、回帰カウンタ値を3から4に変更し、カウンタ値4をメモリ36に格納するとともに、第3番目のデジタル信号(カードデータ)をメモリ36から消去する。

[0116] 第3番目の暗号データを受信したホストコンピュータ13の中央処理部は、図24に示すように、メモリに格納されたカウンタテーブルから回帰カウンタ値3を選択する。コンピュータ13の中央処理部は、カウンタ値2に対応する第2鍵(Key2)とカウンタ値2と

を一方向ハッシュ関数によってハッシュ化したハッシュ出力値を生成し、そのハッシュ出力値をカウンタ値3に対応する第3鍵(Key3)とする(鍵生成手段)。コンピュータ13の中央処理部が生成した第3鍵(Key3)は、マイクロプロセッサ26の中央処理部35が生成したそれと同一である。第3鍵(Key3)となるハッシュ出力値は、カウンタテーブルのカウンタ値3に対応する鍵格納エリア(K1, K2, K3)に書き込まれる。なお、図13のカウンタテーブルでは、回帰カウンタ値4～20に対応する第4鍵～第20鍵は生成されていない。コンピュータ13の中央処理部は、カウンタテーブルからカウンタ値3に対応する第3鍵を取り出し、第3鍵を使用し、トリプルDES(3－KeyトリプルDES)によって暗号データを復号化してデジタル信号(平文カードデータ)を取得する。コンピュータ13の中央処理部は、暗号データを復号化した後、回帰カウンタ値を3から4に変更し、カウンタ値4をメモリに格納する。

[0117] このように、ホストコンピュータ13の中央処理部とマイクロプロセッサ26の中央処理部35とは、回帰カウンタ値1～20を順番に使って互いに同期しつつ、一方向ハッシュ関数を使用して第2～第n鍵を生成する。回帰カウンタ値が20を超えると、コンピュータ13の中央処理部とプロセッサ26の中央処理部35とは、再びカウンタ値1を使用し、第21鍵～第40鍵を順に生成する。コンピュータ13の中央処理部とプロセッサ26の中央処理部35とは、第21鍵を生成すると、鍵格納エリアに格納された第1鍵を第21鍵に書き換え、第22鍵を生成すると、鍵格納エリアに格納された第2鍵を第22鍵に書き替える。

[0118] この磁気カード読み取りシステム10は、相互認証手段を実行することでホストコンピュータ13の中央処理部とマイクロプロセッサ26の中央処理部35とが互いの正当性を判断することができるから、偽コンピュータが磁気ヘッド19に接続された場合や偽磁気ヘッドがコンピュータ13に接続された場合であっても、それを見破ることができる。システム10は、第3者が偽コンピュータや偽磁気ヘッドを利用してシステム10に進入することはできず、磁気カード29のカードデータ、ハッシュ関数、鍵の盗取を防ぐことができる。

[0119] このシステム10は、コンピュータ13の中央処理部とプロセッサ26の中央処理部35とが認証手段による認証結果が正当であると判断した後に、プロセッサ26の中央処

理部35がデータ暗号化手段とデータ送信手段とを実行し、コンピュータ13の中央処理部が復号化手段を実行するから、認証を行わずにそれら手段を実行する場合と比較し、磁気カード29に格納されたカードデータの盗取を確実に防ぐことができ、第3者による磁気カード29の不正な複製や第3者による「なりすまし」を確実に防ぐことができる。

[0120] システム10は、ホストコンピュータ13の中央処理部とマイクロプロセッサ26の中央処理部35とが第2～第n鍵を個別に生成するから、コンピュータ13からプロセッサ26へ鍵を送信する必要はなく、鍵の送信過程における鍵の不正な取得を防ぐことができる。システム10は、プロセッサ26の中央処理部35が常に別の鍵を使用して暗号化を行い、コンピュータ13の中央処理部が常に別の鍵を使用して復号化を行うから、鍵を第3者に取得されたとしても、磁気カード29に格納されたカードデータを復号化することはできない。また、第2～第n鍵にハッシュ値を使用するから、たとえ鍵が第3者に不正に取得されたとしても、鍵の解読をすることはできず、第3者による鍵の使用を確実に防ぐことができる。

[0121] システム10は、ホストコンピュータ13の中央処理部とマイクロプロセッサ26の中央処理部35とが同一かつ有限の回帰カウンタ値を使用して互いに同期しつつ、第2～第n鍵を順に生成するから、コンピュータ13が生成する鍵とプロセッサ26が生成する鍵とを一致させることができ、生成した鍵の不一致による暗号データの復号不能を防ぐことができる。また、第2～第n鍵となるハッシュ出力値に回帰カウンタ値をハッシュ化したハッシュ出力値が含まれるから、第3者がシステム10に不正に進入したとしても、ハッシュ化した回帰カウンタ値を解読することはできず、コンピュータ13の中央処理部とプロセッサ26の中央処理部35とがどのカウンタ値を使用して同期しているかを判別することができない。

[0122] システム10の稼働中にホストコンピュータ13の中央処理部とマイクロプロセッサ26の中央処理部35との同期がずれると、コンピュータ13の中央処理部が生成した鍵とプロセッサ26の中央処理部35が生成したそれとが異なり、中央処理部35から送信された暗号データをコンピュータ13の中央処理部が復号化することができない。この場合、コンピュータ13の中央処理部は、生成した鍵による復号化が不可能であると判

断し、復号化不能を通知するとともに（復号化不能情報）再同期を要求する（再同期要求）。コンピュータ13の中央処理部は、メモリに格納された情報送受信用の鍵を使用し、トリプルDESによって復号化不能情報と再同期要求とを暗号化し、暗号化した復号化不能情報と再同期要求とをプロセッサ26に送信する。コンピュータ13の中央処理部と再同期要求を受け取ったプロセッサ26の中央処理部35とは、それらの正当性を判断する外部認証と内部認証（図6，7参照）とを行う（相互認証手段）。コンピュータ13の中央処理部とプロセッサ26の中央処理部35とは、相互認証による互いの認証結果を正当であると判断すると、回帰カウンタ値を1（初期値）に戻して再び同期を開始する。コンピュータ13の中央処理部とプロセッサ26の中央処理部35とは、カウンタ値を1に戻すと、再び第1鍵を使用して暗号化および復号化を行う。

[0123] システム10は、生成した鍵に不一致が生じたとしても、ホストコンピュータ13とマイクロプロセッサ26とが回帰カウンタ値を1に戻して再び同期することができるから、コンピュータ13が生成する鍵とプロセッサ26が生成する鍵とを再度一致させることができ、生成した鍵の不一致によるカードデータの復号不能を防ぐことができる。なお、システム10が連続して稼働し、相互認証を日単位や週単位、月単位で行う場合、コンピュータ13の中央処理部とプロセッサ26の中央処理部35とは、相互認証による互いの認証結果を正当であると判断すると、回帰カウンタ値を1に戻して再び同期を開始する。以後の手順は、図19～図24に基づいて説明したそれと同一である。

[0124] ホストコンピュータ13は、現在使用しているハッシュ関数の使用を中止し、メモリに格納されたハッシュ関数の中からあらたなハッシュ関数を選択し、そのハッシュ関数を使用することができる。ハッシュ関数の変更は、システム10を起動させる度毎に行う場合、日単位や週単位、月単位で行う場合、同期がずれた後、再び同期するときに行う場合がある。コンピュータ13は、あらたなハッシュ関数を使用する場合、マイクロプロセッサ26に既存のハッシュ関数の書き換えを指示する（関数変更指令）。コンピュータ13の中央処理部は、メモリに格納された情報送受信用の鍵を使用し、トリプルDESによって関数変更指令とあらたなハッシュ関数とを暗号化し、暗号化した関数変更指令とハッシュ関数とをプロセッサ26に送信する。

[0125] マイクロプロセッサ26の中央処理部35は、関数変更指令とハッシュ関数とを受信

すると、メモリ36に格納された情報送受信用の鍵を使用し、トリプルDESによって暗号化された関数変更指令とハッシュ関数とを復号化する。プロセッサ26の中央処理部35は、メモリ36に格納した既存のハッシュ関数を復号化したあらたなハッシュ関数に変更した後、変更完了をコンピュータ13に通知する(変更完了通知)。中央処理部35は、メモリ36に格納された情報送受信用の鍵を使用し、トリプルDESによって変更完了通知を暗号化し、暗号化した変更完了通知をコンピュータ13に送信する。このシステム10は、関数変更指令やハッシュ関数を暗号化してハッシュ関数の変更を行うから、使用するハッシュ関数を第3者に取得されることはなく、第3者によるハッシュ関数の解読を防ぐことができる。

[0126] ホストコンピュータ13は、現在使用している暗号化アルゴリズムの使用を中止し、メモリに格納された暗号化アルゴリズムの中からあらたなアルゴリズムを選択し、そのアルゴリズムを使用することができる。暗号化アルゴリズムの変更は、システム10を起動させる度毎に行う場合、日単位や週単位、月単位で行う場合、同期がずれた後、再び同期するときに行う場合がある。コンピュータ13は、あらたな暗号化アルゴリズムを使用する場合、マイクロプロセッサ26に既存のアルゴリズムの書き換えを指示する(関数変更指令)。コンピュータ13の中央処理部は、メモリに格納された情報送受信用の鍵を使用し、トリプルDESによって関数変更指令とあらたな暗号化アルゴリズムとを暗号化し、暗号化した関数変更指令とアルゴリズムとをプロセッサ26に送信する。

[0127] マイクロプロセッサ26の中央処理部35は、関数変更指令と暗号化アルゴリズムとを受信すると、メモリ36に格納された情報送受信用の鍵を使用し、トリプルDESによって暗号化された関数変更指令とアルゴリズムとを復号化する。プロセッサ26の中央処理部35は、メモリ36に格納した既存のアルゴリズムを復号化したあらたなアルゴリズムに変更した後、変更完了をコンピュータ13に通知する(変更完了通知)。中央処理部35は、メモリ36に格納された情報送受信用の鍵を使用し、トリプルDESによって変更完了通知を暗号化し、暗号化した変更完了通知をコンピュータ13に送信する。このシステム10は、関数変更指令や暗号化アルゴリズムを暗号化してアルゴリズムの変更を行うから、使用するアルゴリズムを第3者に取得されることはない。

[0128] このシステム10おける磁気カードリーダには、挿入電動型の他に、磁気ヘッド19を

取り付けた手動ハンディカードリーダを使用することもできる。また、磁気カードリーダをPOSシステムに接続することもできる。磁気カードリーダがPOSシステムに接続された場合、カードリーダにコントローラを設置する必要はなく、外部サーバ11との接続はPOSシステムに内蔵されたコンピュータによって行われる。ファームウェアや暗号化アルゴリズムは、外部サーバからPOSシステムのコンピュータのメモリにダウンロードされて一時保管された後、カードリーダの磁気ヘッドのマイクロプロセッサ26に出力される。

請求の範囲

[1] 磁性体を利用して各種データを記憶した磁気カードから前記データを読み取る磁気ヘッドにおいて、

前記磁気ヘッドが、前記磁気カードに記憶されたデータをアナログ信号に変換するコイルを有するコアと、前記コアに接続されて前記アナログ信号をデジタル信号に変換するA／D変換チップと、前記A／D変換チップに接続されたデジタルICとを備え、

前記デジタルICは、その演算・記憶機能を制御するとともに外部ハードウェアを制御するファームウェアが外部サーバから前記磁気ヘッドにダウンロードされたときに、そのファームウェアを記憶するファームウェア記憶手段を有することを特徴とする磁気ヘッド。

[2] 前記ファームウェアには、前記磁気カードの各種フォーマットに対応させて前記デジタルICに該磁気カードの各種データを読み取らせるデータ読み取り制御が含まれ、前記デジタルICが、前記磁気カードの各種フォーマットに対応して該磁気カードから各種データを読み取るフォーマット対応読み取り手段を有する請求項1記載の磁気ヘッド。

[3] 前記ファームウェアには、所定の暗号化アルゴリズムに基づいて前記デジタルICに前記デジタル信号を暗号化させるデータ暗号化制御が含まれ、前記デジタルICが、前記デジタル信号を所定の暗号化アルゴリズムに基づいて暗号化するデータ暗号化手段を有する請求項1または請求項2に記載の磁気ヘッド。

[4] 前記デジタルICは、バージョンアップされたファームウェアが前記外部サーバから前記磁気ヘッドにダウンロードされたときに、バージョンアップ前のファームウェアをバージョンアップ後のファームウェアに書き換えるファームウェア更新手段を有する請求項1ないし請求項3いずれかに記載の磁気ヘッド。

[5] 前記外部サーバが、それに格納された鍵を使用して前記ファームウェアを暗号化しつつ、暗号化したファームウェアを前記磁気ヘッドにダウンロードし、前記デジタルICが、それに格納された鍵を使用して暗号化されたファームウェアを復号化しつつ、復号化したファームウェアを記憶する請求項1ないし請求項4いずれかに記載の磁気ヘ

ッド。

[6] 前記デジタルICと前記外部サーバとが、それらの間で認証を行う相互認証を実行し、前記デジタルICと前記外部サーバとが前記相互認証による互いの認証結果を正当であると判断した後、前記外部サーバが前記磁気ヘッドに前記ファームウェアをダウンロードし、前記デジタルICが前記外部サーバからダウンロードされた前記ファームウェアを記憶する請求項1ないし請求項5いずれかに記載の磁気ヘッド。

[7] 前記デジタルICは、前記デジタル信号を暗号化する各種の暗号化アルゴリズムが前記外部サーバから前記磁気ヘッドにダウンロードされたときに、その暗号化アルゴリズムを記憶するアルゴリズム記憶手段を有する請求項1ないし請求項6いずれかに記載の磁気ヘッド。

[8] 前記デジタルICは、あらたな暗号化アルゴリズムが前記外部サーバから前記磁気ヘッドにダウンロードされたときに、すでに記憶した暗号化アルゴリズムをあらたな暗号化アルゴリズムに書き換えるアルゴリズム更新手段を有する請求項7記載の磁気ヘッド。

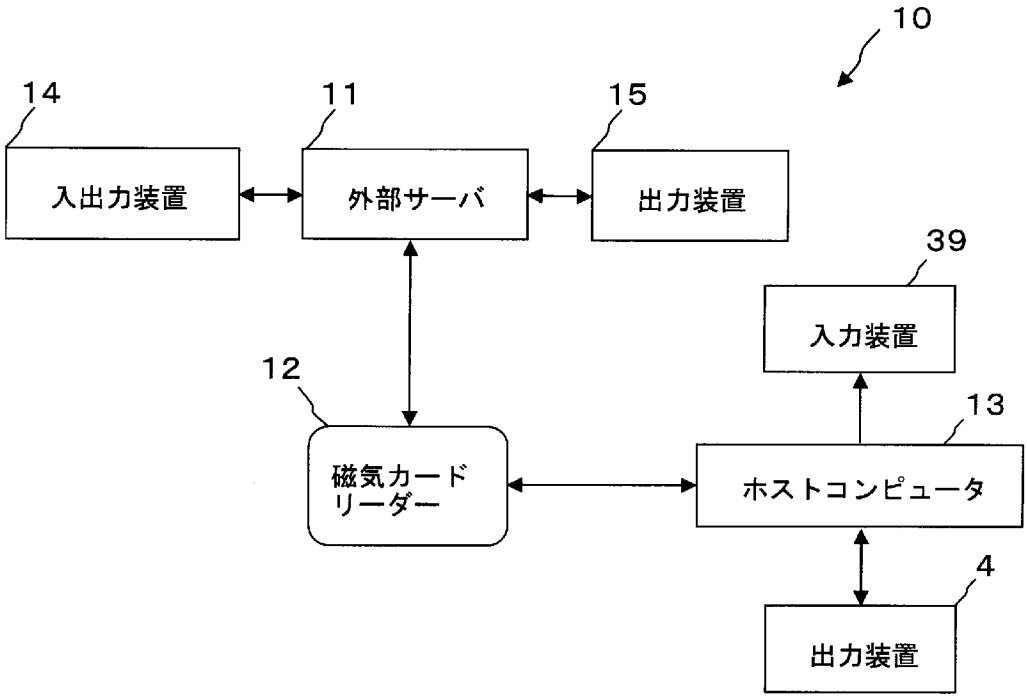
[9] 前記外部サーバが、それに格納された鍵を使用して前記暗号化アルゴリズムを暗号化しつつ、暗号化した暗号化アルゴリズムを前記磁気ヘッドにダウンロードし、前記デジタルICが、それに格納された鍵を使用して暗号化された暗号化アルゴリズムを復号化しつつ、復号化した暗号化アルゴリズムを記憶する請求項7または請求項8に記載の磁気ヘッド。

[10] 前記デジタルICと前記外部サーバとが、それらの間で認証を行う相互認証を実行し、前記デジタルICと前記外部サーバとが前記相互認証による互いの認証結果を正当であると判断した後、前記外部サーバが前記磁気ヘッドに前記暗号化アルゴリズムをダウンロードし、前記デジタルICが前記外部サーバからダウンロードされた前記暗号化アルゴリズムを記憶する請求項7ないし請求項9いずれかに記載の磁気ヘッド。

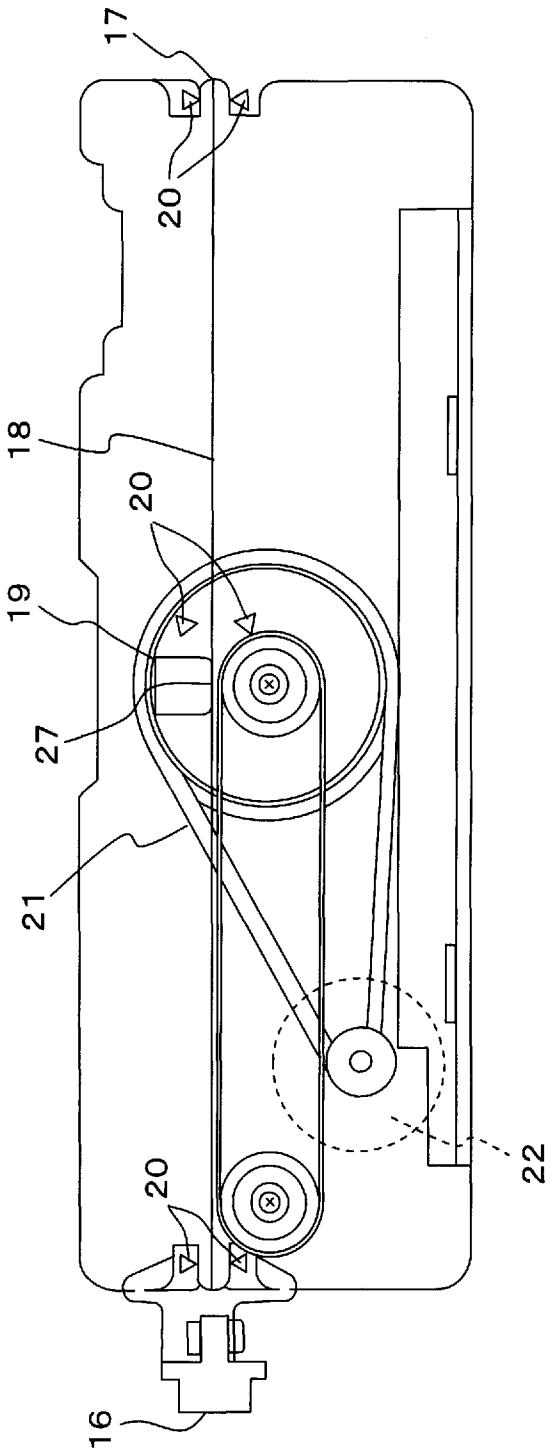
[11] 前記磁気ヘッドが、その外周を包被するハウジングを有し、前記コアと前記A／D変換チップと前記デジタルICとが、前記ハウジングの内部に収容されている請求項1ないし請求項10いずれかに記載の磁気ヘッド。

[12] 前記A／D変換チップと前記デジタルICとが、前記ハウジングの内部に充填された固形物質によって該ハウジングに固定されている請求項1ないし請求項11いずれかに記載の磁気ヘッド。

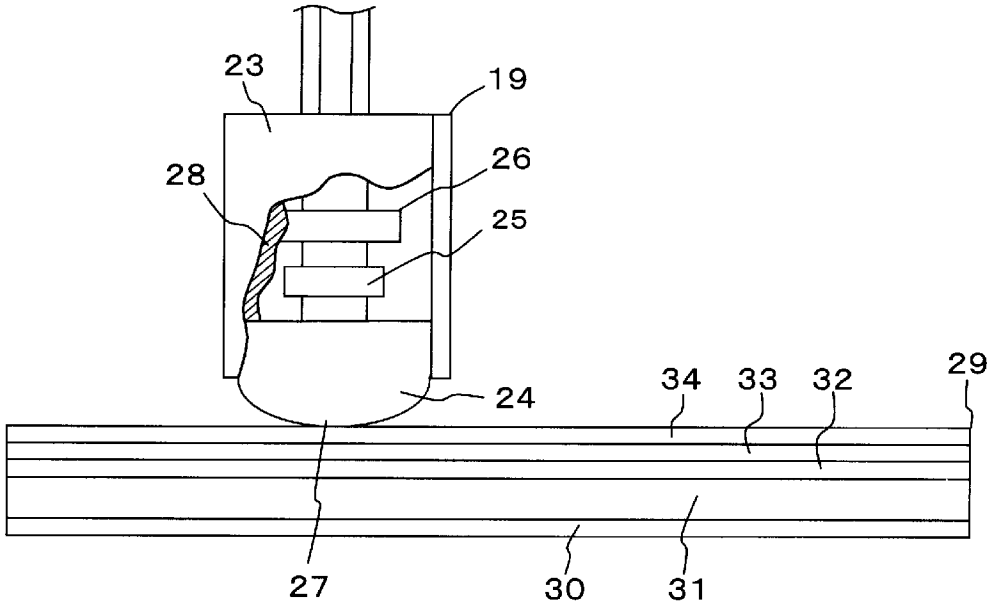
[図1]


10
14
11
15
入出力装置
外部サーバ
出力装置
39
入力装置
12
13
磁気カード
リーダー
ホストコンピュータ
4
出力装置

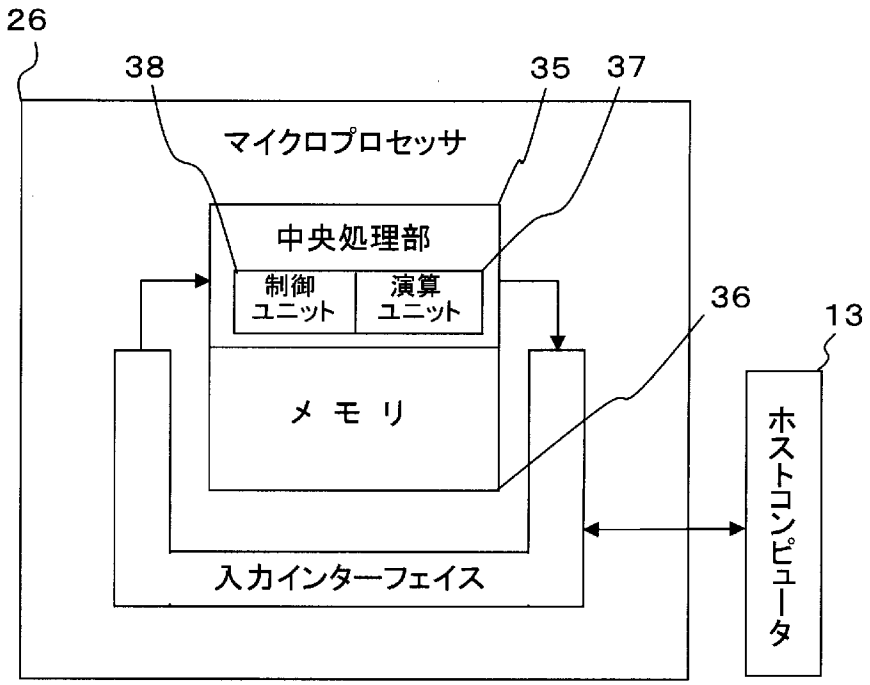
[図2]



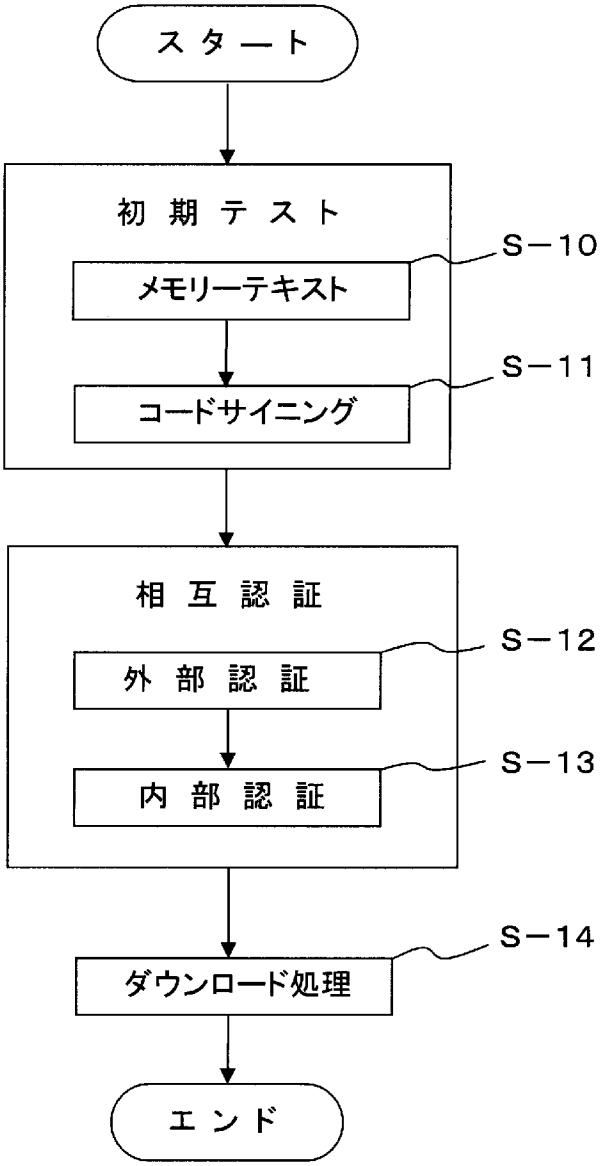
[図3]


23
19
28
26
25
24
34
33
32
29
27
30
31

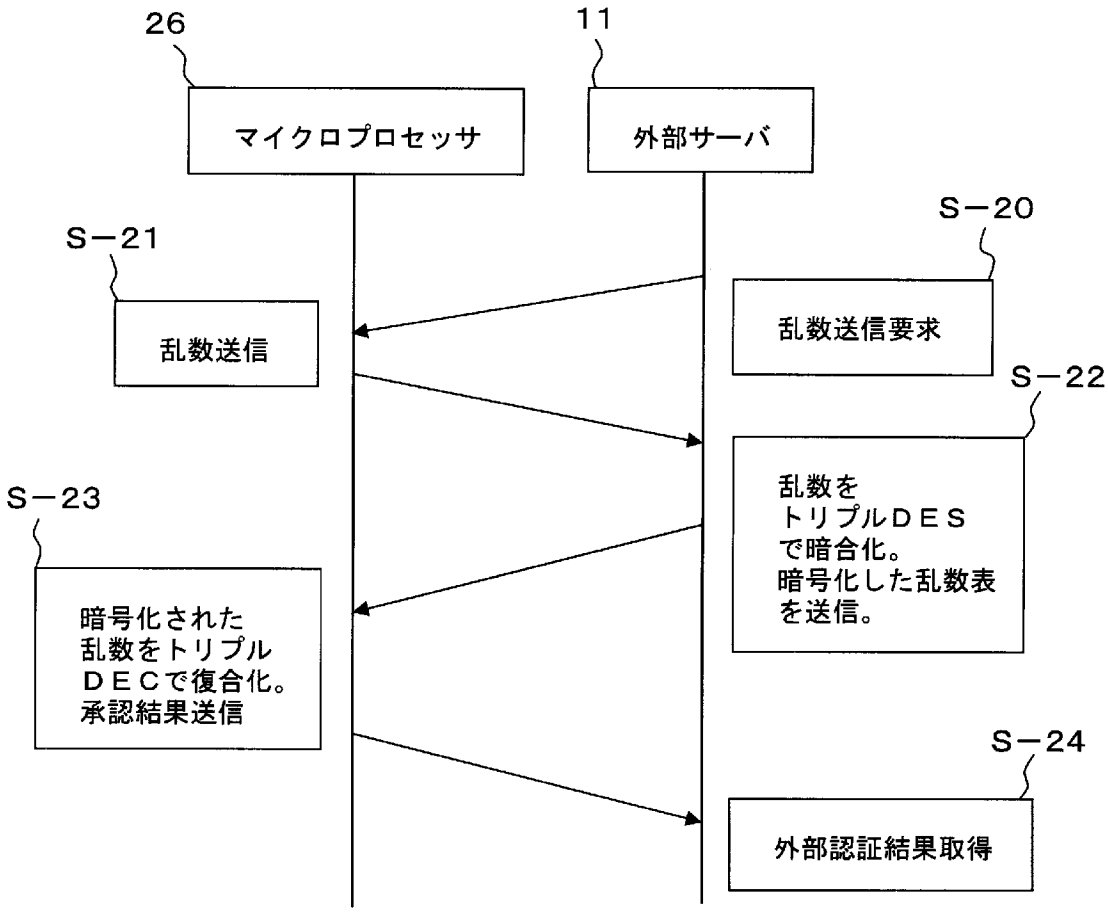
[図4]


26
38
35
37
マイクロプロセッサ
中央処理部
制御ユニット
演算ユニット
メモリ
36
13
入力インターフェイス
ホストコンピュータ

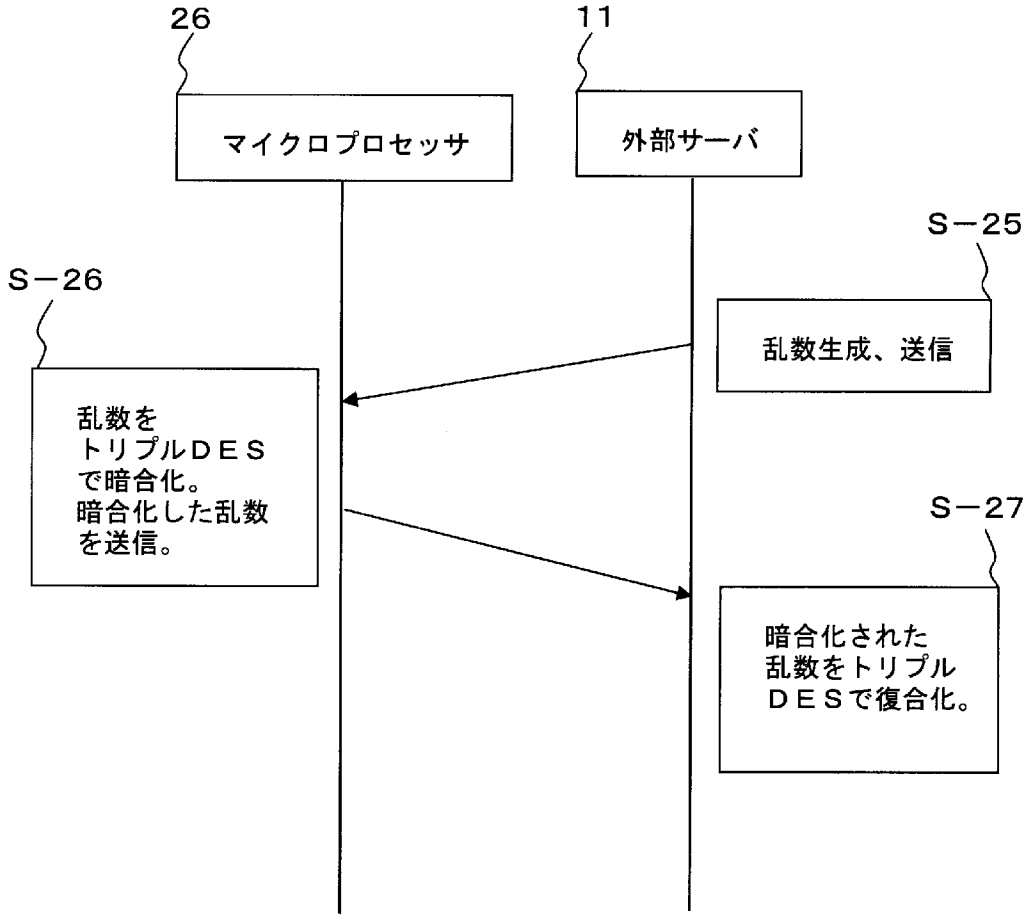
[図5]


スタート
初期テスト
メモリーテキスト
S−10
コードサイニング
S−11
相互認証
外部認証
S−12
内部認証
S−13
ダウンロード処理
S−14
エンド

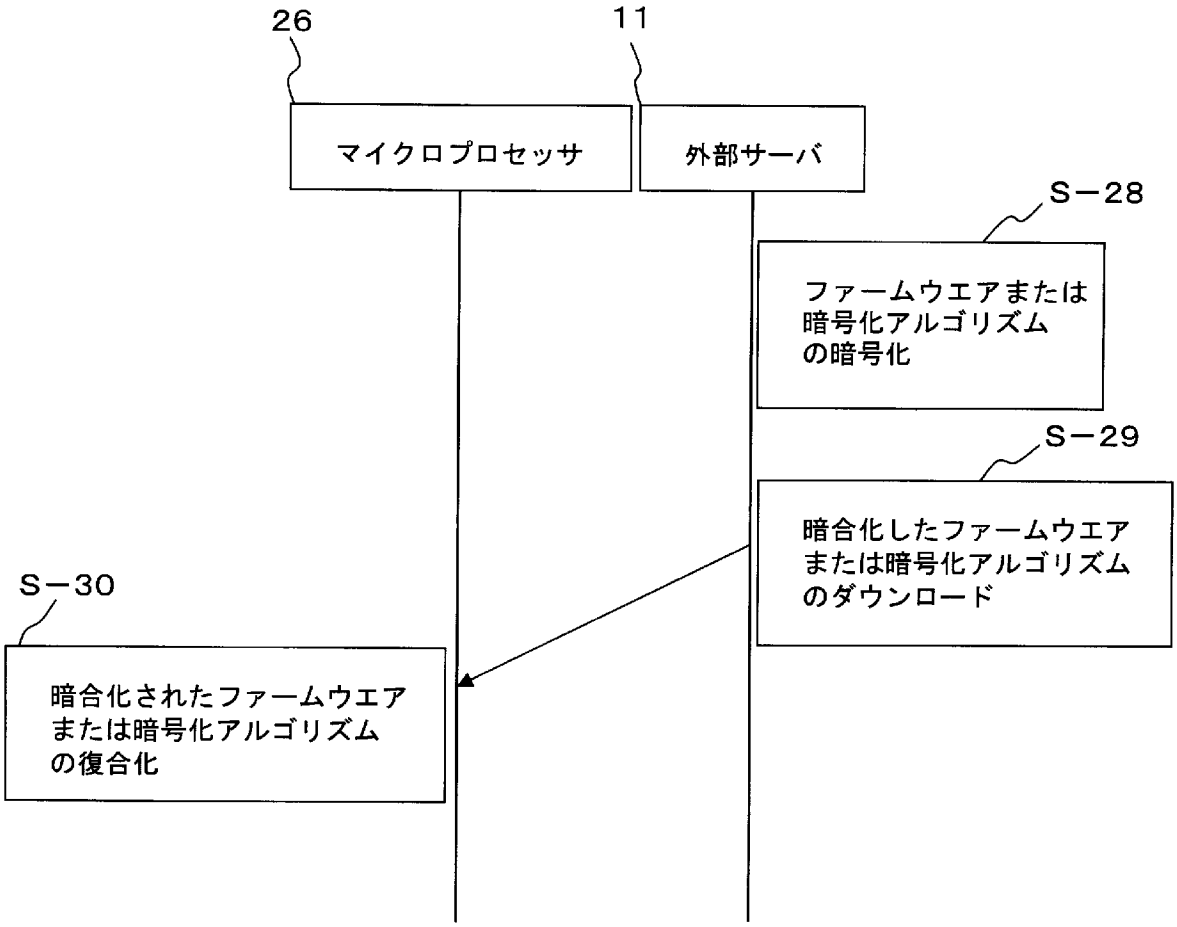
[図6]


26
マイクロプロセッサ
11
外部サーバ
S－20
乱数送信要求
S－21
乱数送信
S－22
乱数を
トリプルＤＥＳ
で暗合化。
暗号化した乱数表
を送信。
S－23
暗号化された
乱数をトリプル
ＤＥＣで復合化。
承認結果送信
S－24
外部認証結果取得

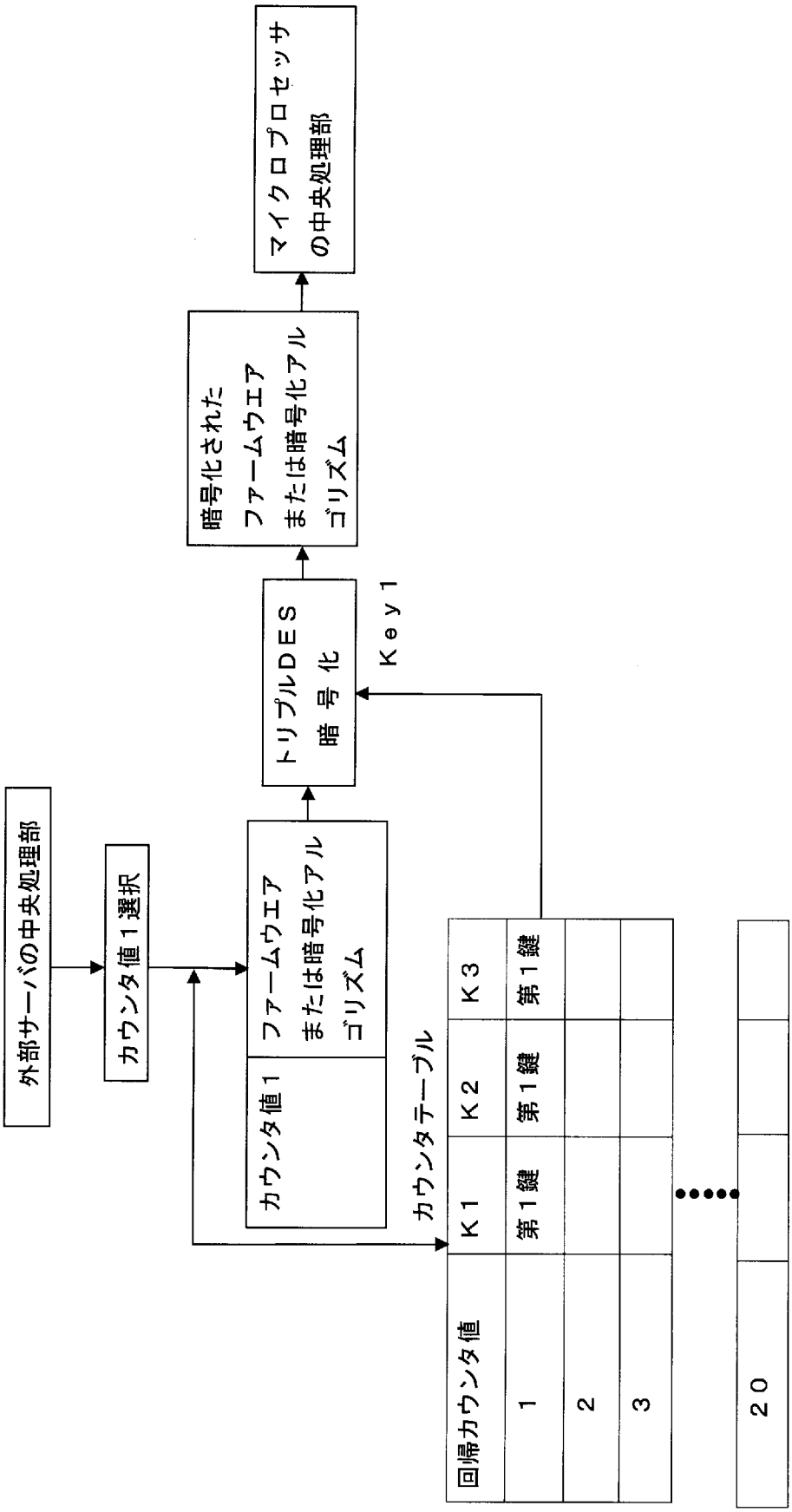
[図7]


26
11
マイクロプロセッサ
外部サーバ
S－25
S－26
乱数生成、送信
乱数を
トリプルＤＥＳ
で暗合化。
暗合化した乱数
を送信。
S－27
暗合化された
乱数をトリプル
ＤＥＳで復合化。

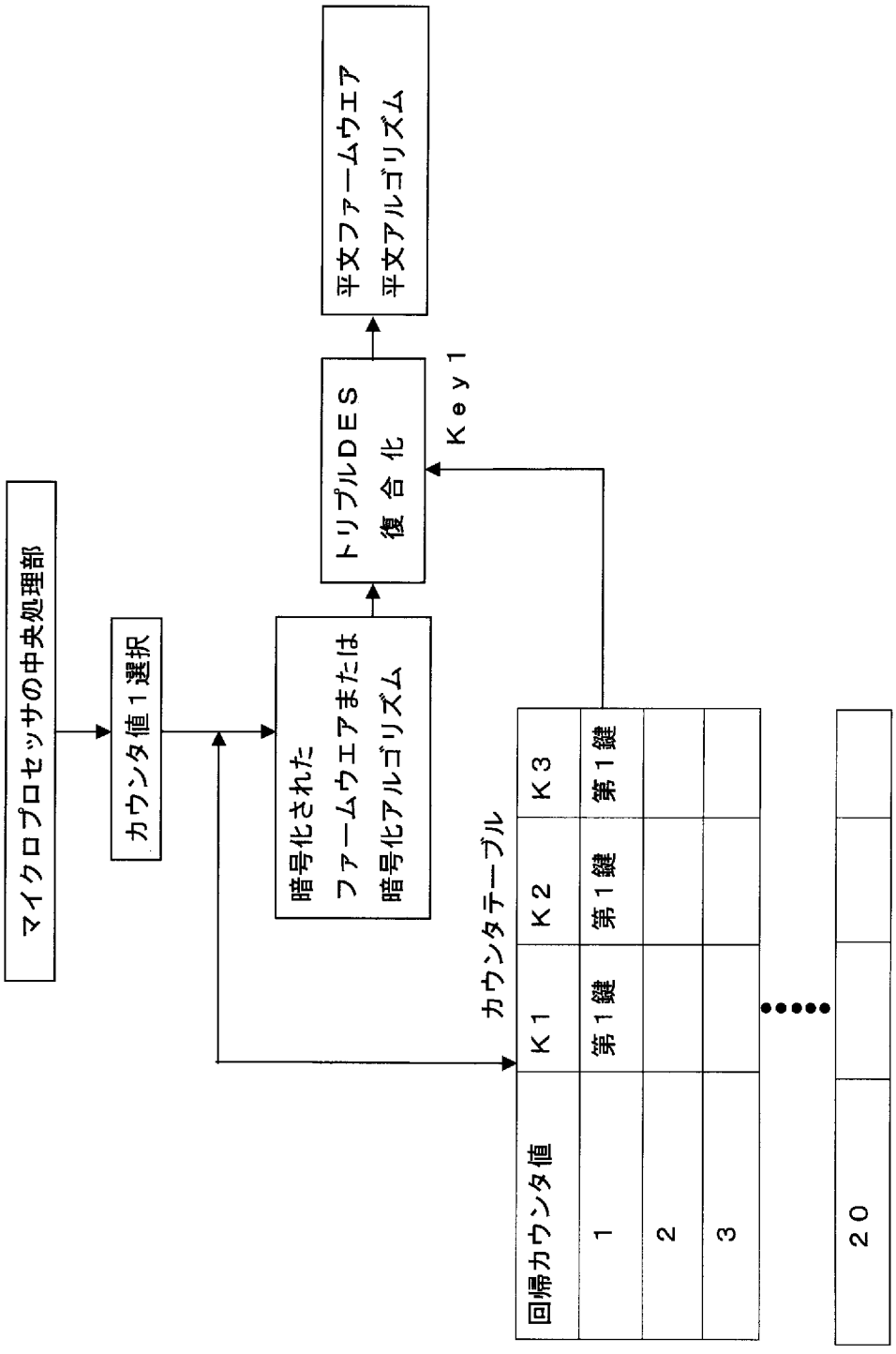
[図8]


26
11
マイクロプロセッサ
外部サーバ
S－28
ファームウエアまたは
暗号化アルゴリズム
の暗号化
S－29
暗合化したファームウエア
または暗号化アルゴリズム
のダウンロード
S－30
暗合化されたファームウエア
または暗号化アルゴリズム
の復合化

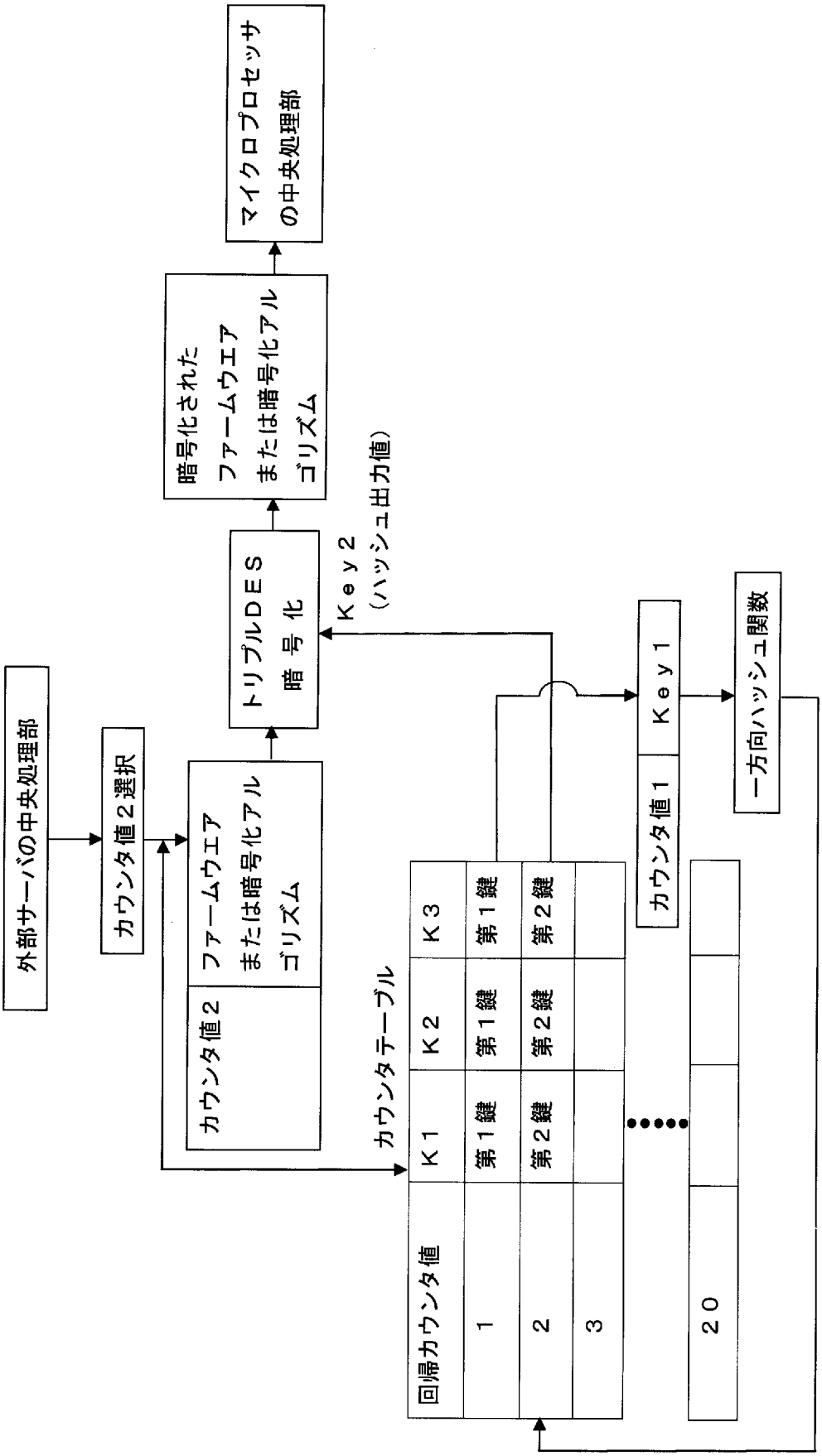
[図9]


外部サーバの中央処理部
カウンタ値１選択
カウンタ値１
ファームウエア
または暗号化アル
ゴリズム
トリプルＤＥＳ
暗 号 化
Ｋｅｙ１
暗号化された
ファームウエア
または暗号化アル
ゴリズム
マイクロプロセッサ
の中央処理部
カウンタテーブル
回帰カウンタ値
Ｋ１
Ｋ２
Ｋ３
第１鍵
第１鍵
第１鍵
１
２
３
２０

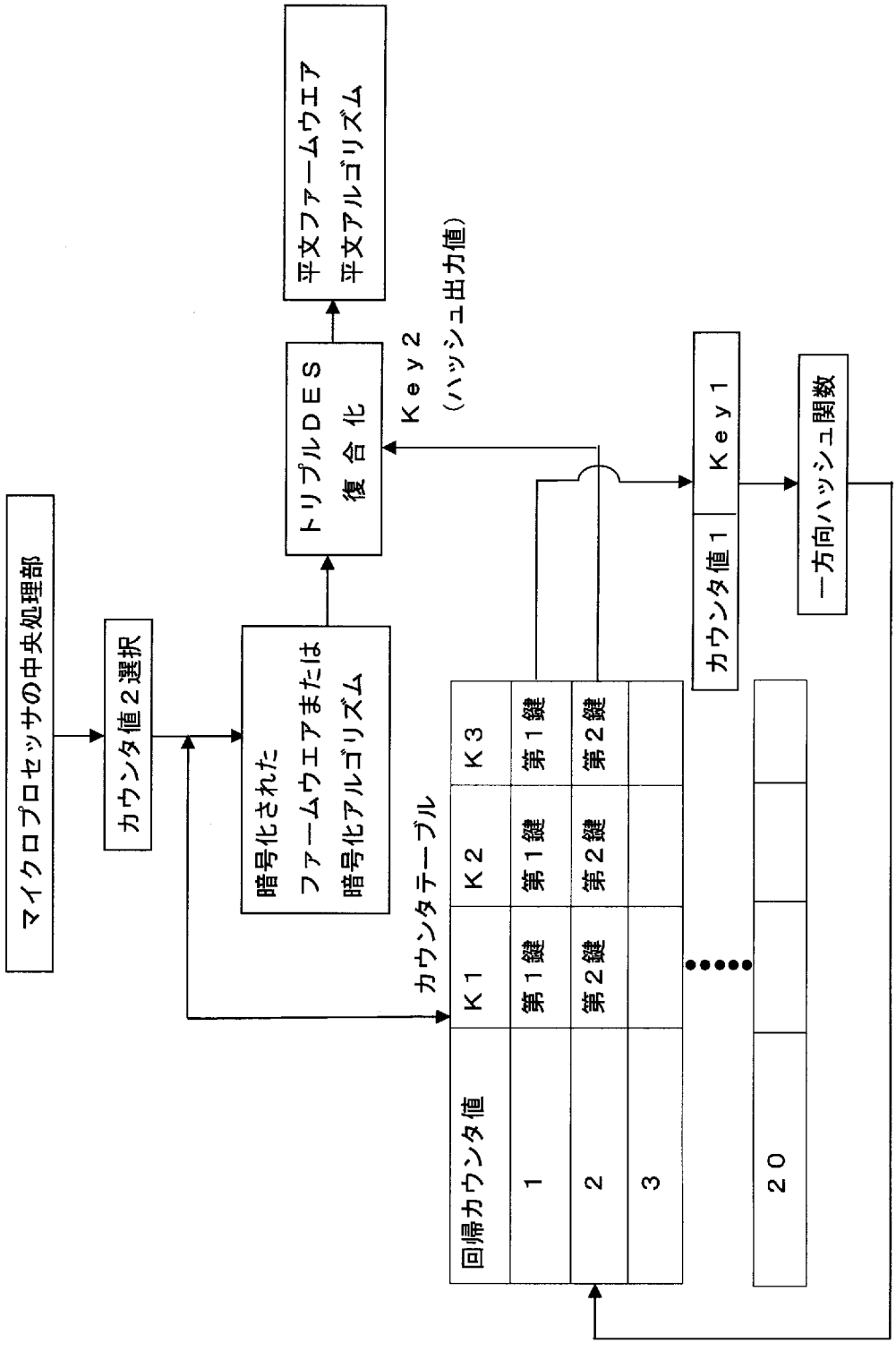
[図10]


マイクロプロセッサの中央処理部
カウンタ値１選択
暗号化された
ファームウエアまたは
暗号化アルゴリズム
トリプルＤＥＳ
復 合 化
Ｋｅｙ１
平文ファームウエア
平文アルゴリズム
カウンタテーブル
回帰カウンタ値
Ｋ１
Ｋ２
Ｋ３
１
２
３
２０
第１鍵
第１鍵
第１鍵

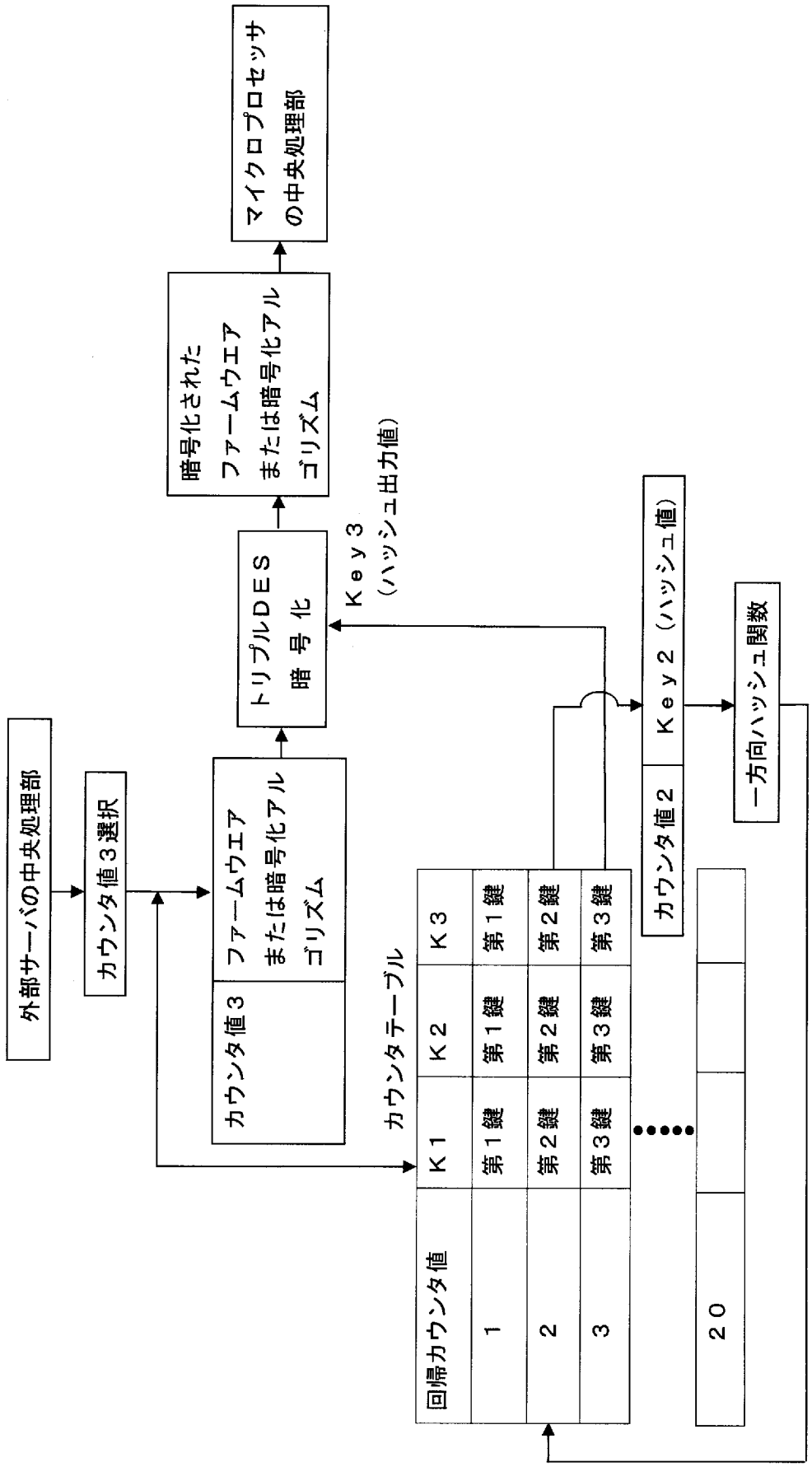
[図11]


外部サーバの中央処理部
カウンタ値２選択
カウンタ値２
ファームウエア
または暗号化アル
ゴリズム
トリプルＤＥＳ
暗号化
Ｋｅｙ２
（ハッシュ出力値）
暗号化された
ファームウエア
または暗号化アル
ゴリズム
マイクロプロセッサ
の中央処理部
カウンタテーブル
回帰カウンタ値
Ｋ１
Ｋ２
Ｋ３
１
２
３
２０
第１鍵
第２鍵
カウンタ値１
Ｋｅｙ１
一方向ハッシュ関数

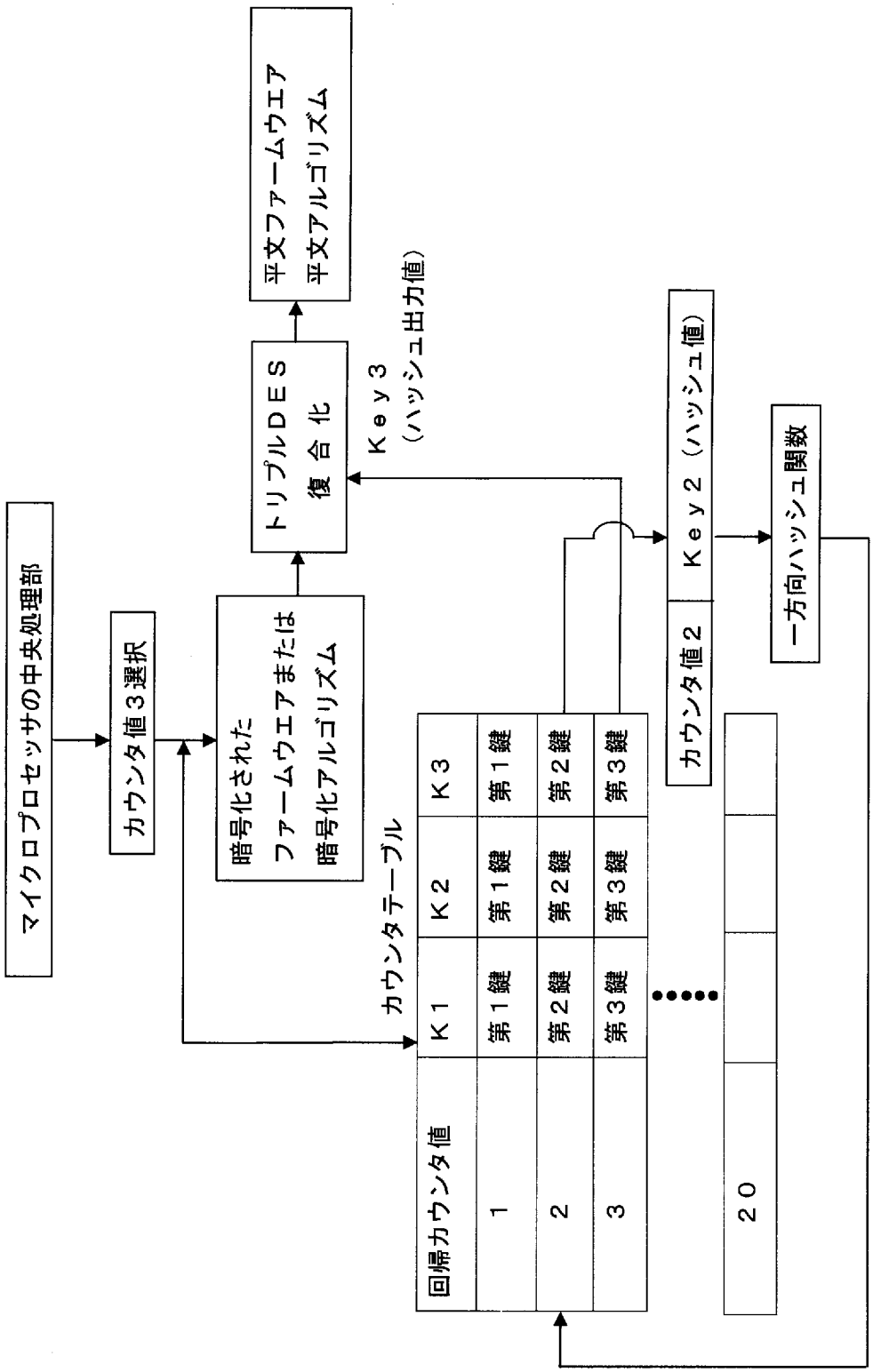
[図12]


マイクロプロセッサの中央処理部
カウンタ値２選択
暗号化されたファームウエアまたは暗号化アルゴリズム
トリプルＤＥＳ復合化
平文ファームウエア平文アルゴリズム
Ｋｅｙ２（ハッシュ出力値）
カウンタテーブル
回帰カウンタ値
Ｋ１
Ｋ２
Ｋ３
第１鍵
第２鍵
１
２
３
２０
カウンタ値１
Ｋｅｙ１
一方向ハッシュ関数

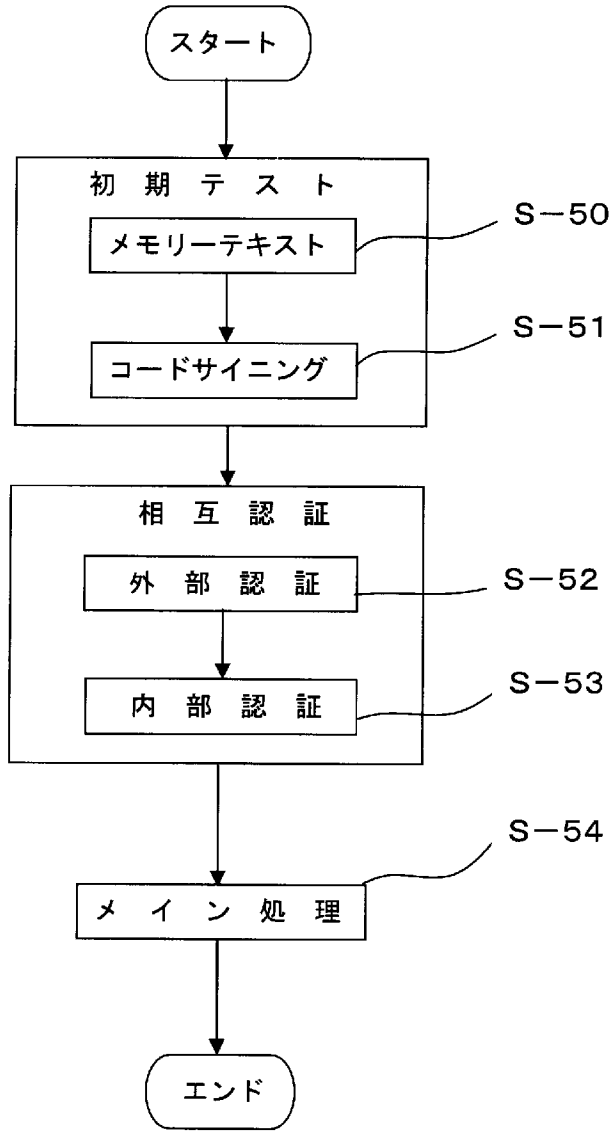
[図13]


外部サーバの中央処理部
カウンタ値３選択
カウンタ値３
ファームウエア
または暗号化アル
ゴリズム
トリプルＤＥＳ
暗号化
Ｋｅｙ３
（ハッシュ出力値）
暗号化された
ファームウエア
または暗号化アル
ゴリズム
マイクロプロセッサ
の中央処理部
カウンタテーブル
回帰カウンタ値
Ｋ１
Ｋ２
Ｋ３
１
２
３
２０
第１鍵
第２鍵
第３鍵
カウンタ値２
Ｋｅｙ２（ハッシュ値）
一方向ハッシュ関数

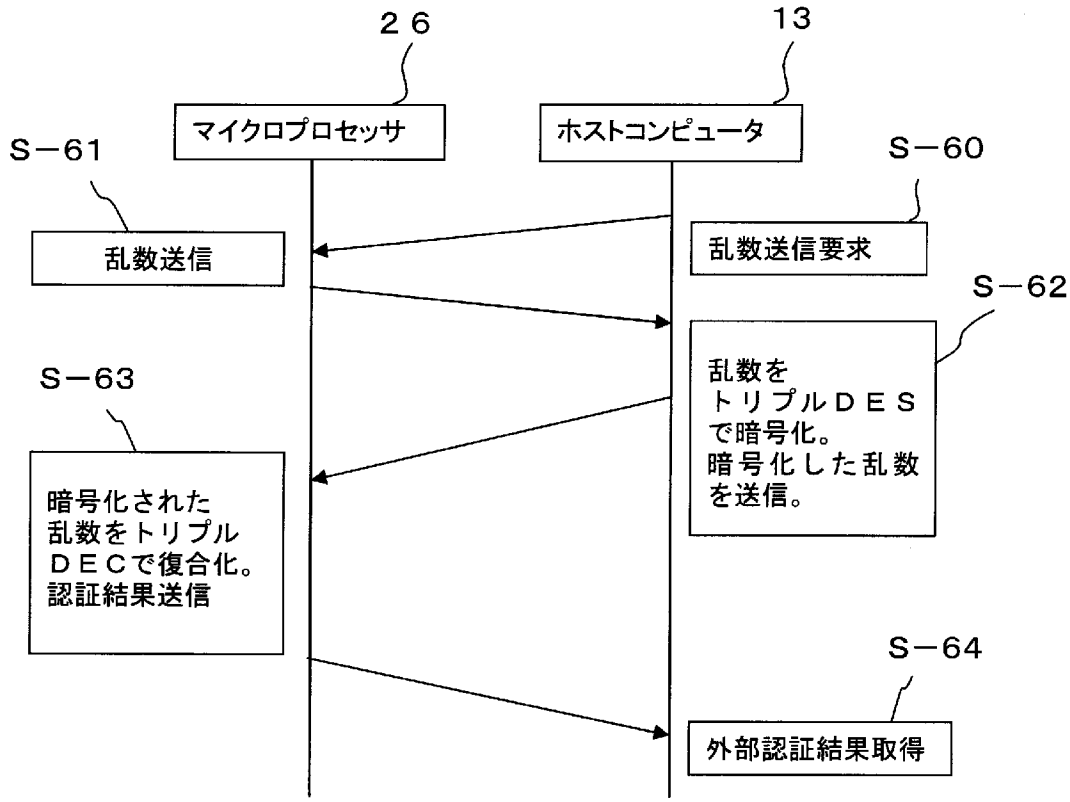
[図14]


マイクロプロセッサの中央処理部
カウンタ値３選択
暗号化された
ファームウエアまたは
暗号化アルゴリズム
トリプルＤＥＳ
復 合 化
平文ファームウエア
平文アルゴリズム
Ｋｅｙ３
（ハッシュ出力値）
カウンタテーブル
回帰カウンタ値
Ｋ１
Ｋ２
Ｋ３
１
２
３
２０
第１鍵
第２鍵
第３鍵
カウンタ値２
Ｋｅｙ２（ハッシュ値）
一方向ハッシュ関数

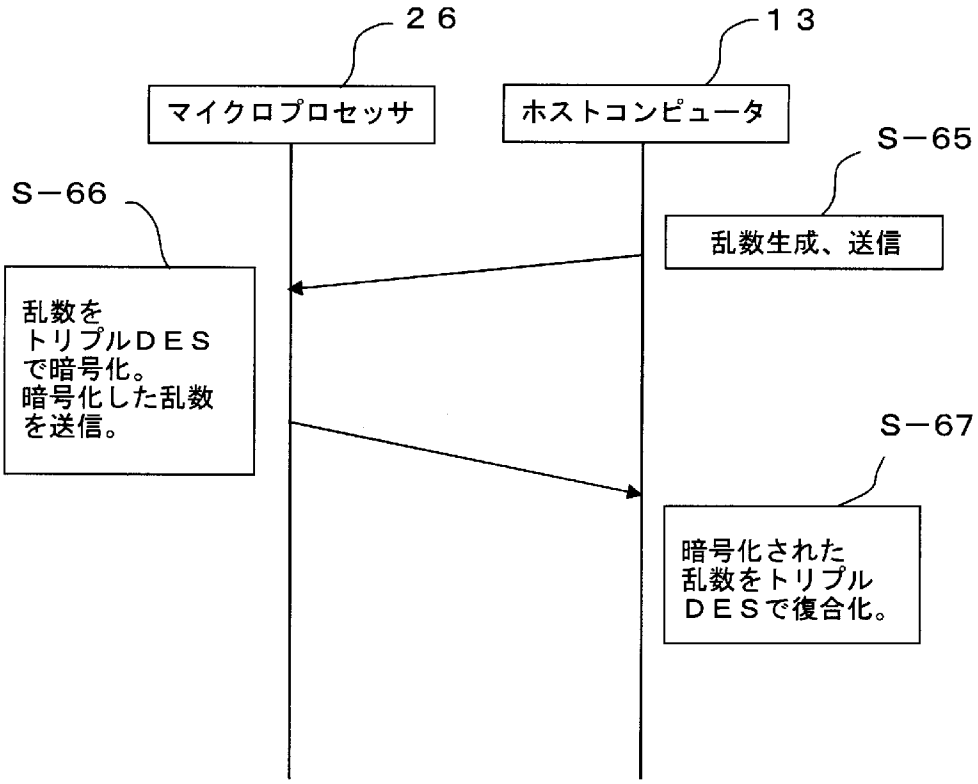
[図15]


スタート
初期テスト
メモリーテキスト
S−50
コードサイニング
S−51
相互認証
外部認証
S−52
内部認証
S−53
S−54
メイン処理
エンド

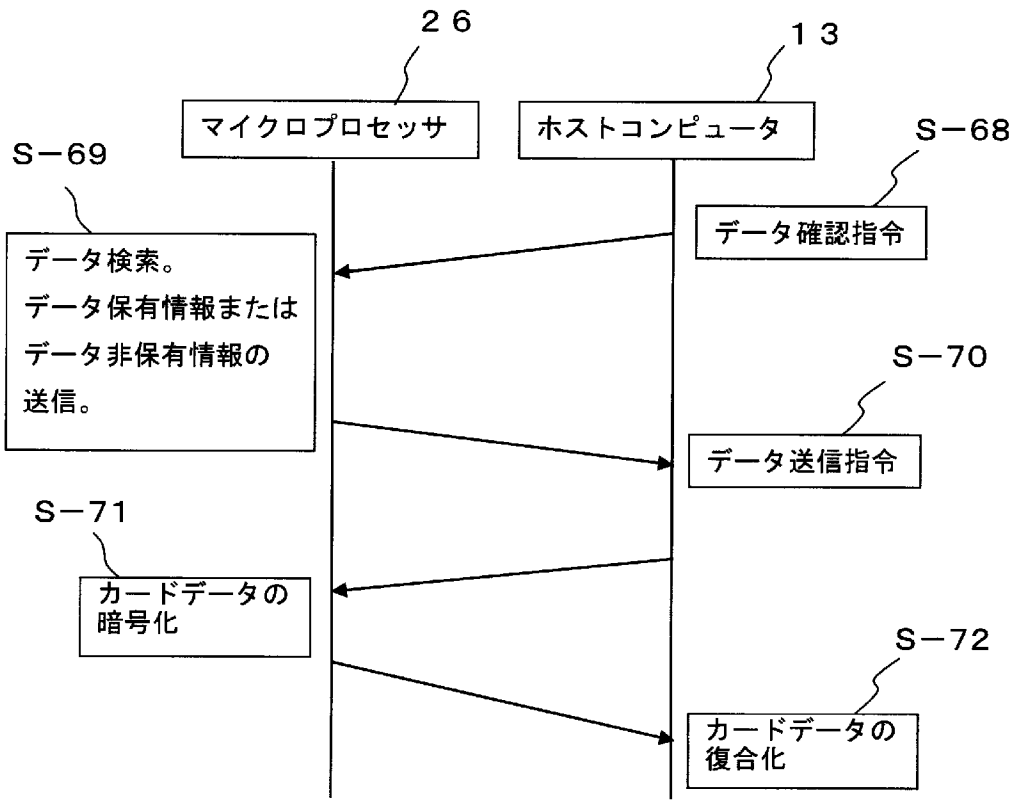
[図16]


２６
１３
マイクロプロセッサ
ホストコンピュータ
Ｓ－６１
Ｓ－６０
乱数送信
乱数送信要求
Ｓ－６２
乱数を
トリプルＤＥＳ
で暗号化。
暗号化した乱数
を送信。
Ｓ－６３
暗号化された
乱数をトリプル
ＤＥＣで復合化。
認証結果送信
Ｓ－６４
外部認証結果取得

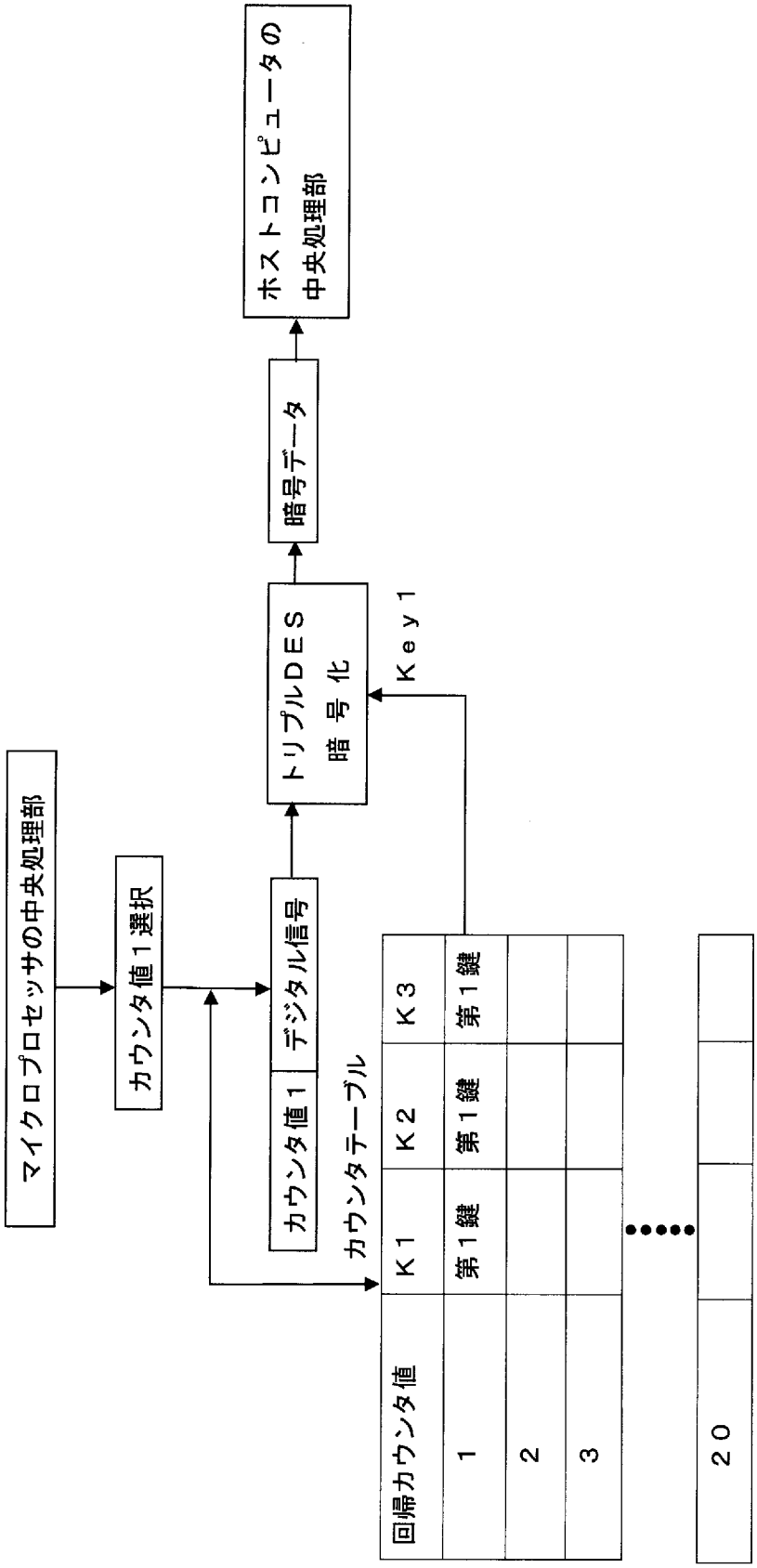
[図17]


２６
１３
マイクロプロセッサ
ホストコンピュータ
S－65
S－66
乱数生成、送信
乱数を
トリプルＤＥＳ
で暗号化。
暗号化した乱数
を送信。
S－67
暗号化された
乱数をトリプル
ＤＥＳで復合化。

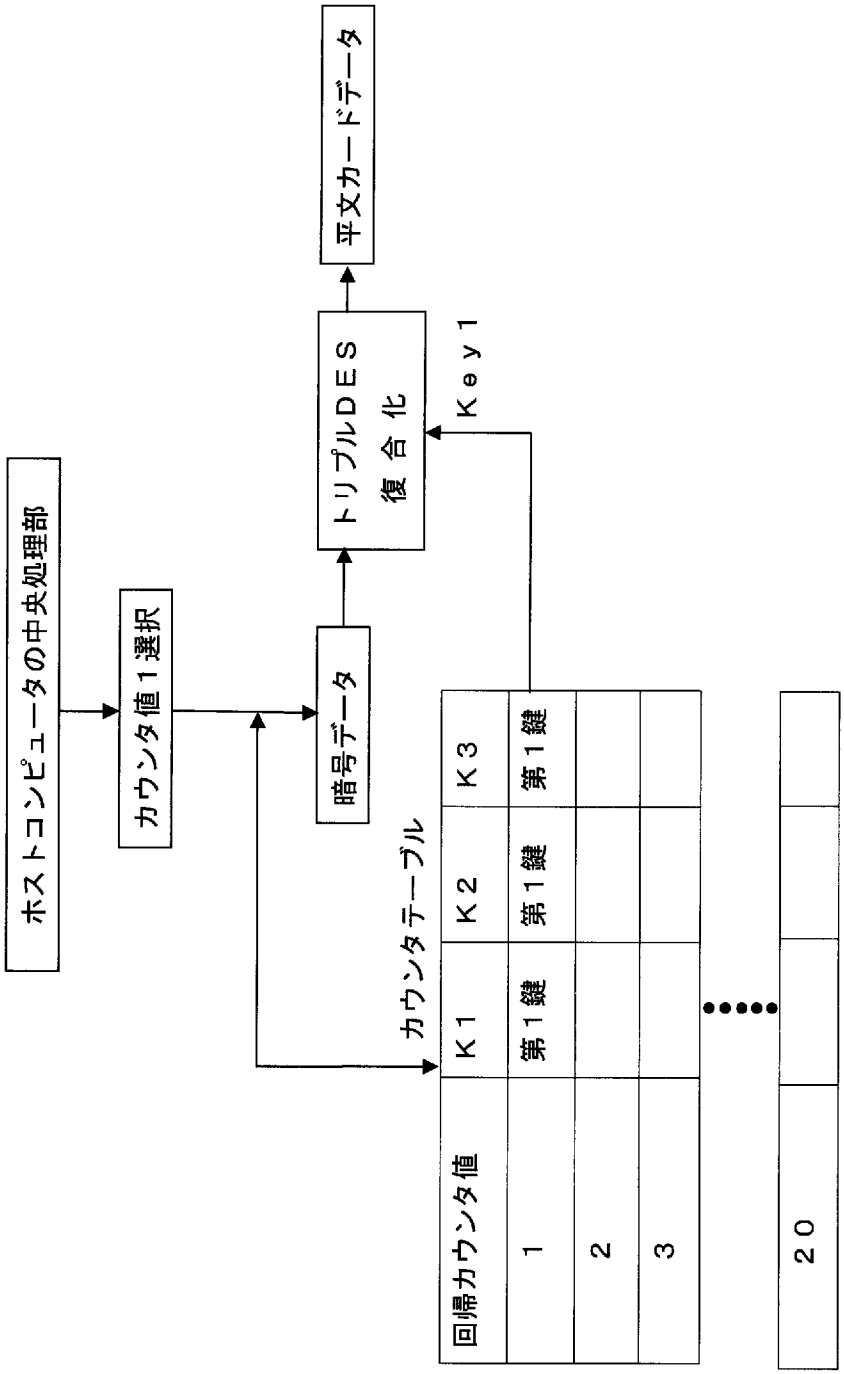
[図18]


２６
１３
マイクロプロセッサ
ホストコンピュータ
S－68
S－69
データ確認指令
データ検索。
データ保有情報または
データ非保有情報の
送信。
S－70
データ送信指令
S－71
カードデータの
暗号化
S－72
カードデータの
復合化

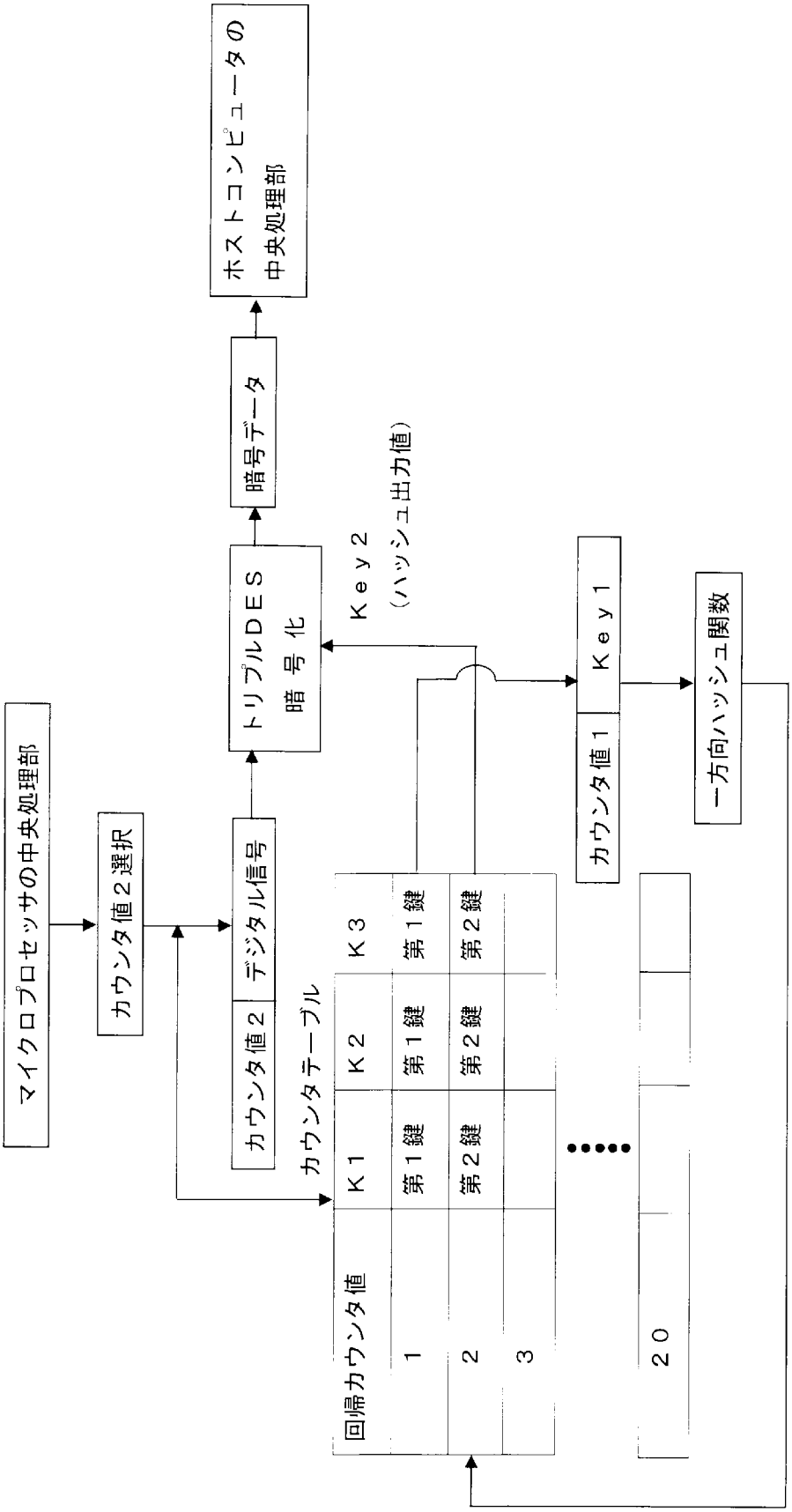
[図19]


マイクロプロセッサの中央処理部
カウンタ値１選択
カウンタ値１
デジタル信号
トリプルＤＥＳ
暗号化
Ｋｅｙ１
暗号データ
ホストコンピュータの
中央処理部
カウンタテーブル
回帰カウンタ値
Ｋ１
Ｋ２
Ｋ３
第１鍵
第１鍵
第１鍵
１
２
３
２０

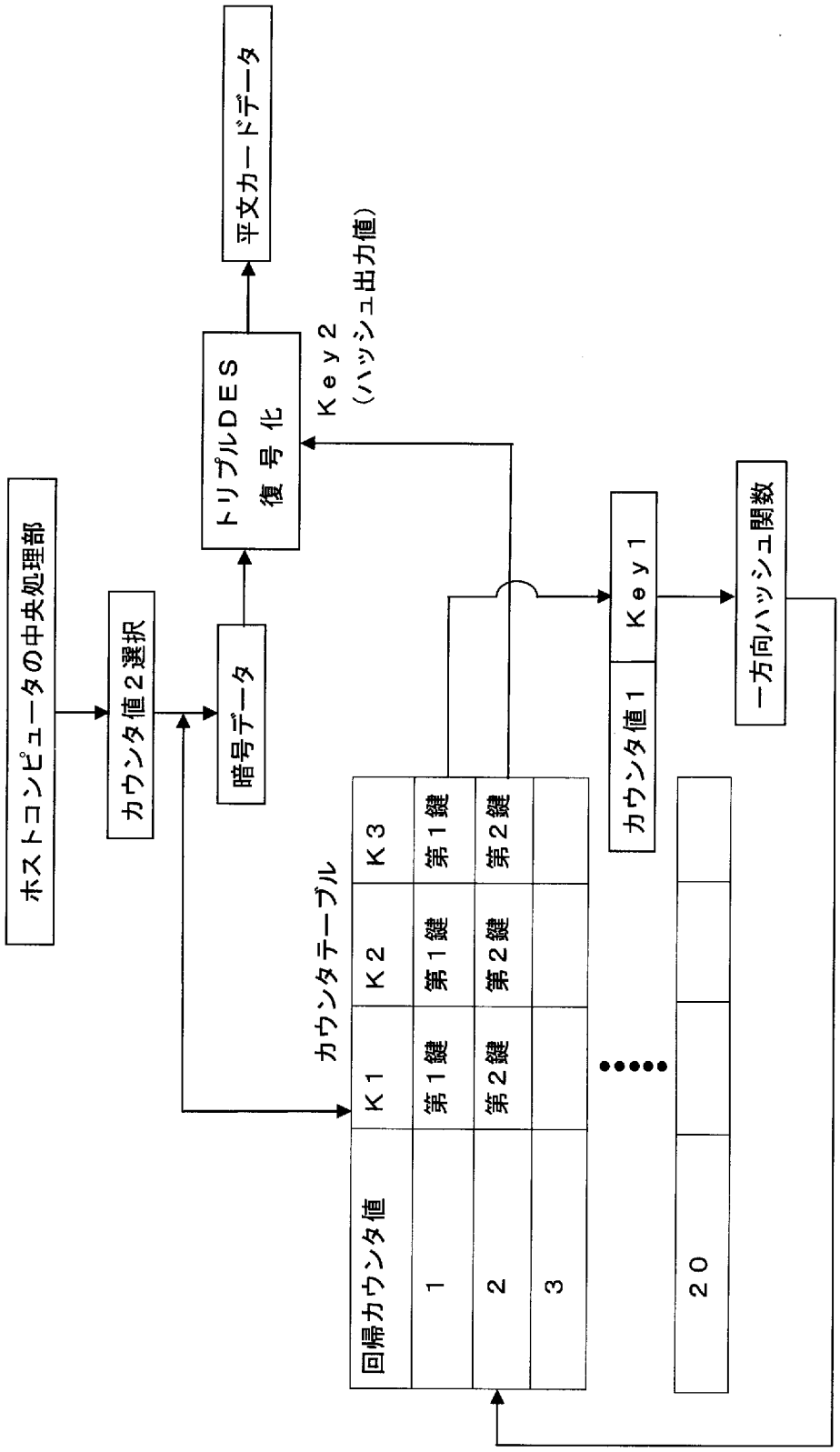
[図20]


ホストコンピュータの中央処理部
カウンタ値１選択
暗号データ
トリプルＤＥＳ
復合化
Ｋｅｙ１
平文カードデータ
カウンタテーブル
回帰カウンタ値
Ｋ１
Ｋ２
Ｋ３
第１鍵
第１鍵
第１鍵
１
２
３
２０

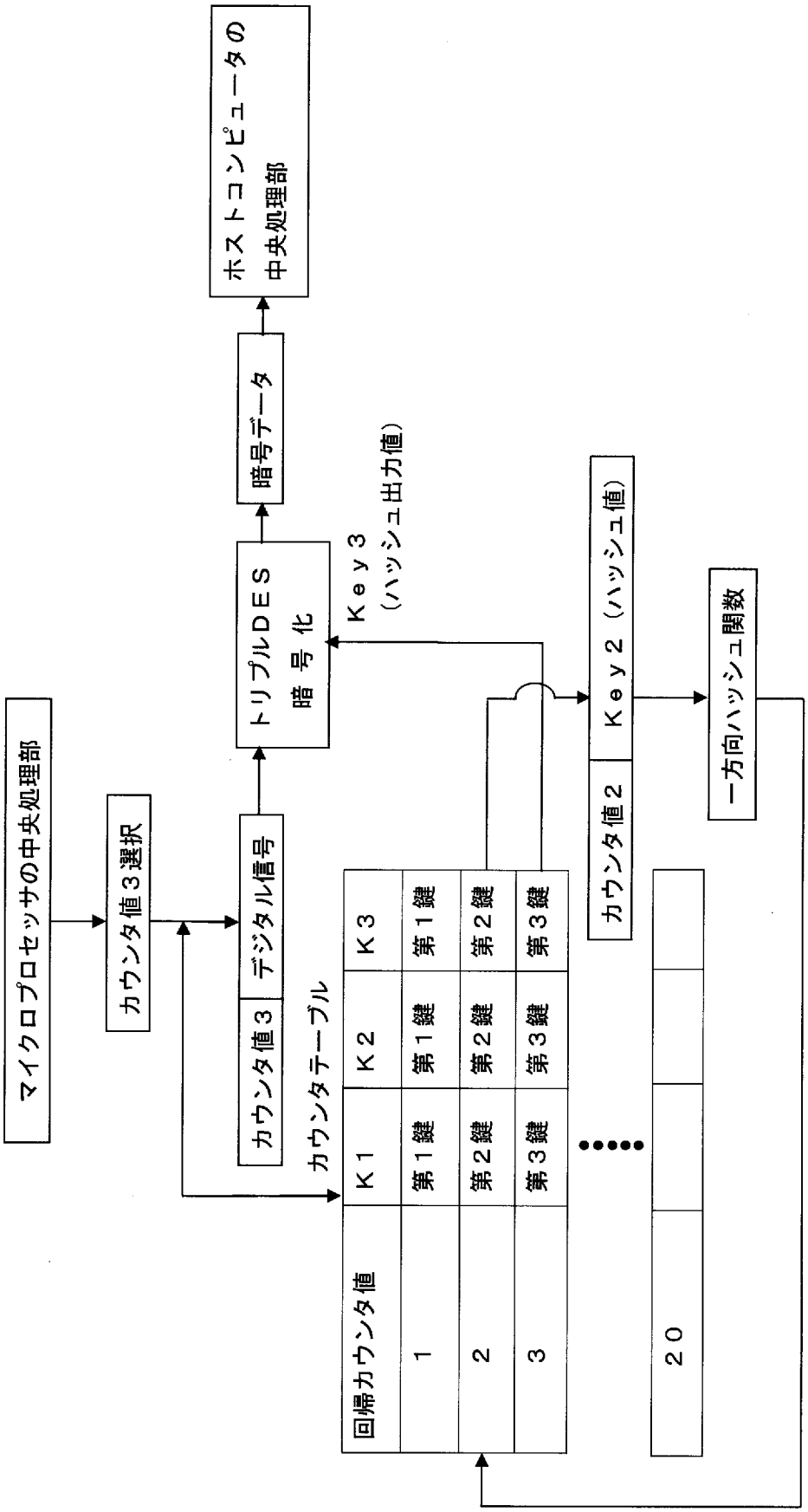
[図21]


マイクロプロセッサの中央処理部
カウンタ値２選択
カウンタ値２
デジタル信号
トリプルＤＥＳ
暗号化
暗号データ
ホストコンピュータの
中央処理部
Ｋｅｙ２
（ハッシュ出力値）
カウンタテーブル
回帰カウンタ値
Ｋ１
Ｋ２
Ｋ３
第１鍵
第２鍵
１
２
３
２０
カウンタ値１
Ｋｅｙ１
一方向ハッシュ関数

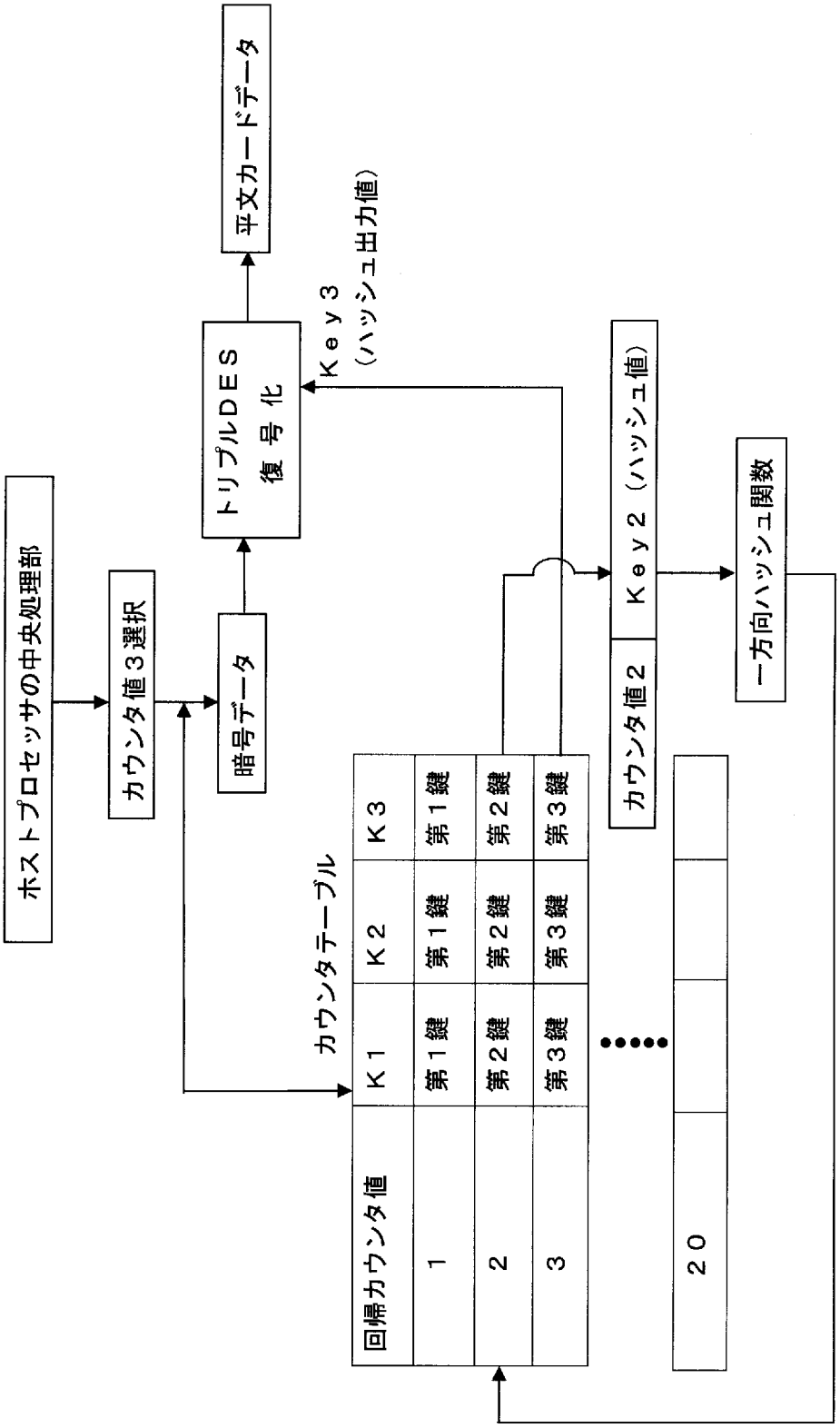
[図22]


ホストコンピュータの中央処理部
カウンタ値２選択
暗号データ
トリプルDES
復号化
平文カードデータ
Ｋｅｙ２
（ハッシュ出力値）
カウンタテーブル
回帰カウンタ値
Ｋ１
Ｋ２
Ｋ３
第１鍵
第２鍵
1
2
3
２０
カウンタ値１
Ｋｅｙ１
一方向ハッシュ関数

[図23]


マイクロプロセッサの中央処理部
カウンタ値３選択
カウンタ値３
デジタル信号
トリプルＤＥＳ
暗号化
暗号データ
ホストコンピュータの
中央処理部
Ｋｅｙ３
（ハッシュ出力値）
カウンタテーブル
回帰カウンタ値
Ｋ１
Ｋ２
Ｋ３
１
２
３
２０
第１鍵
第２鍵
第３鍵
カウンタ値２
Ｋｅｙ２（ハッシュ値）
一方向ハッシュ関数

[図24]


ホストプロセッサの中央処理部
カウンタ値３選択
暗号データ
トリプルDES
復号化
平文カードデータ
Ｋｅｙ３
（ハッシュ出力値）
カウンタテーブル
回帰カウンタ値
Ｋ１
Ｋ２
Ｋ３
第１鍵
第２鍵
第３鍵
1
2
3
２０
カウンタ値２
Ｋｅｙ２（ハッシュ値）
一方向ハッシュ関数

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/073285

A. CLASSIFICATION OF SUBJECT MATTER
G06K17/00(2006.01)i, *G11B5/09*(2006.01)i, *G11B5/10*(2006.01)i, *G11B20/10*(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)
G06K17/00, G11B5/09, G11B5/10, G11B20/10

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2009
Kokai Jitsuyo Shinan Koho	1971-2009	Toroku Jitsuyo Shinan Koho	1994-2009

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 2001-143213 A (Anritsu Corp.), 25 May, 2001 (25.05.01), Full text; all drawings (Family: none)	1-12
Y	JP 2000-90597 A (Hitachi, Ltd.), 31 March, 2000 (31.03.00), Par. No. [0008]; Fig. 2 (Family: none)	1-12
Y	JP 2003-100011 A (NEC Corp.), 04 April, 2003 (04.04.03), Par. No. [0002] (Family: none)	1-12

☐ 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 January, 2009 (16.01.09)	Date of mailing of the international search report 27 January, 2009 (27.01.09)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００８／０７３２８５

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06K17/00(2006.01)i, G11B5/09(2006.01)i, G11B5/10(2006.01)i, G11B20/10(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.　G06K17/00, G11B5/09, G11B5/10, G11B20/10

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	１９７１－２００９年
日本国実用新案登録公報	１９９６－２００９年
日本国登録実用新案公報	１９９４－２００９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	関連する請求の範囲の番号
Ｙ	JP 2001-143213 A（アンリツ株式会社）2001.05.25，全文，全図（ファミリーなし）	１－１２
Ｙ	JP 2000-90597 A（株式会社日立製作所）2000.03.31，０００８段落，図２（ファミリーなし）	１－１２
Ｙ	JP 2003-100011 A（日本電気株式会社）2003.04.04，０００２段落（ファミリーなし）	１－１２

☐　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
１６．０１．２００９	２７．０１．２００９

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）　５Ｑ　９１８６
中村　豊
電話番号　０３－３５８１－１１０１　内線　３５９１