(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
2007 年6 月28 日(28.06.2007)

PCT

(10)
WO 2007/072793 A1

(51) 国際特許分類:
*G06K 19/10* (2006.01) *G06F 21/24* (2006.01)
*B42D 15/00* (2006.01) *G06K 17/00* (2006.01)
*G06F 21/20* (2006.01) ***G06K 19/06*** (2006.01)

(21) 国際出願番号: PCT/JP2006/325224

(22) 国際出願日: 2006 年12 月19 日(19.12.2006)

(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2005-365416
2005 年12 月19 日(19.12.2005) JP
特願2006-200823
2006 年7 月24 日(24.07.2006) JP
特願2006-287714
2006 年10 月23 日(23.10.2006) JP

(71) 出願人(米国を除く全ての指定国について): 国際先端技術総合研究所株式会社 **(INTERNATIONAL FRONTIER TECHNOLOGY LABORATORY, INC.)** [JP/JP]; 〒1000014 東京都千代田区永田町二丁目10番2号 秀和永田町TBRビル Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人(米国についてのみ): 小松信明(KOMATSU, Nobuaki) [JP/JP]; 〒1050001 東京都港区虎ノ門二丁目6番1O号 Tokyo (JP). 南條眞一郎(NANJO, **Shin-ichiro)** [JP/JP]; 〒1740064 東京都板橋区中台三丁目27f B610 Tokyo (JP).

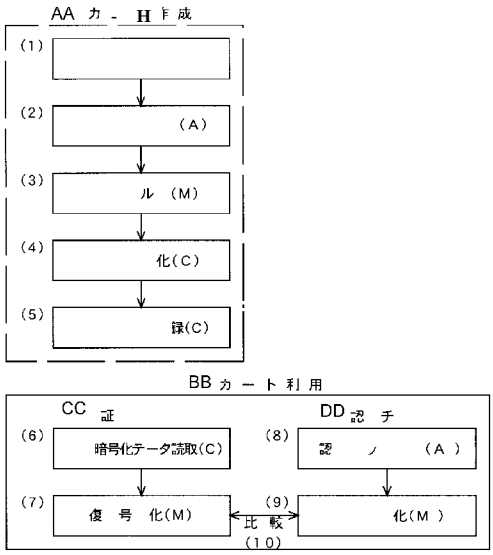
(74) 代理人: 南條眞一郎 **(NANJO, Shin-ichiro);** 〒1010053 東京都千代田区神田美土代町7番地 クボビル 南條特許事務所 Tokyo (JP).

(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, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,

/続葉有/

**(54) Title:** CARD CAPABLE OF AUTHENTICATION

**(54)** 発明の名称: 真贋判別可能なカード




AA CARD FABRICATION
(1) CREATE AUTHENTICATION CHIP
(2) READ AUTHENTICATION CHIP (A)
(3) DIGITIZATION (M)
(4) ENCRYPTION (C)
(5) ENCRYPTED DATA RECORDING (C)
B CARD USE
CC CERTIFYING CHIP
DD AUTHENTICATION CHIP
(6) ENCRYPTED DATA READ (C)
(7) DECRYPTION (M)
(8) AUTHENTICATION CHIP READ (A)
(9) DIGITIZATION (M)
(10) COMPARISON

(57) Abstract: It is possible to prevent use of a forged card. An authentication chip describing information which cannot be copied or difficult to be copied is attached to a card and a card processing device includes a card authentication processing device. The information described in the authentication chip is digitized and encrypted to obtain encrypted data which is described on an authentication certifying chip. The authentication certifying chip is attached to the card. The authentication certifying chip checks the validity of the authentication chip. Before a specific operation such as entry of a password is started, it is judged whether the card is true so as to exclude a forged card.

**(57)** 要約: 偽造カードの使用を防止する。カードに複写不能あるいは複写困難な情報が記載された真贋認証チップを取り付け、カードを処理する装置内にカード真贋認証処理装置を付加する。カードに真贋認証チップに記載された情報を子ジタル化した子ータを暗号化した暗号化子ータが記載された真贋証明チップを取り付け、真贋証明チップによって真贋認証チップの正当性を確認する。暗証番号入力等の具体的な操作が開始される前に、カードの真贋を判定し、偽造カードを排除する。

WO 2007/072793 1

OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, 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), -xーラシT (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, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, Rの, 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
— 補正書

2文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノートJ を参照。

# 明 細 書

## 真贋判別可能なカード

## 技術分野

[0001] この出願に係る発明は、カード、紙幣、証券類等偽造されやすく、真贋認証を必要とする対象物の構造及びその対象物の真贋を判別する方法に係るものである。

## 背景技術

[0002] カード社会と呼ばれる今日、数多くのカードが出回っており、銀行のキャッシュカード、クレジットカード会社のクレジットカード等所有者の財産に関わるカード、有価証券であるプリペイドカード及び運転免許証,健康保険証,パスポート等身分証明に関わるカードが使用されている。

[0003] 財産に関わるカード及び有価証券であるカードの多くは、表面あるいは裏面に設けられた磁気ストライプに必要な情報を書込、ATM(Automatic Teller's Machine)等の自動機械あるいは手動読み取り装置を用いて、磁気ストライプから磁気情報を読み取り、各種の処理を実行している。

[0004] 図1に示すのは、現行のキャッシュカード処理フローの例である。

(1)カード所有者がATM等の端末装置のカード挿入口にキャッシュカードを挿入すると、カード挿入口のセンサがそのことを感知し、カードを装置内に取り込む。

[0005] (2)カードを取り込む際に、端末装置はカードの磁気記録部からカード情報を読み込む。キャッシュカードの場合には、銀行コード,支店コード,口座種別,口座番号等のカード情報を読み込む。なお、クレジットカードの場合には、カード識別番号,有効期限,口座種別,口座番号がカード情報として、磁気記録部に記録されている。また、キャッシュカードあるいはクレジットカードに暗証番号が記録されている場合があるが、その場合には暗証番号も読み込まれる。

[0006] (3)端末装置は、挿入されたカードがその端末装置で取り扱うことが可能なカードであるか否かを判断する。

[0007] (4)読み込んだカード情報から、取扱いが可能であることを示す情報が確認されなかった場合、あるいは正規のカードであっても破損あるいは汚損等によりカードの情

報が読みとれなかった場合には、端末装置はそのカードが取り扱うことが出来ない不適正なカードであるとして排出する。

[0008] (5) カードが正規のものであり、磁気記録部の情報が正しく読みとれた場合には、ホストコンピュータとの通信が開始される。

[0009] (6) ホストコンピュータから暗証番号の入力要求がなされる。

[0010] (7) ホストコンピュータからの要求に対応して、カード利用者が暗証番号を入力する。

[0011] (8) ホストコンピュータからの要求に対応して、カード利用者が暗証番号を入力すると、ホストコンピュータは入力された暗証番号をホストコンピュータに格納されている読み込まれたカード情報に対応する暗証番号と比較する。

[0012] (9) 合致しなかった場合には、カードの磁気記録部にそのことを記録して、再度暗証番号の入力を求め、再度入力された暗証番号が正当なものであったときはその後の手続きを行い、合致しなかった場合には同様にして再々度暗証番号の入力を求め、暗証番号の誤入力の累計が3回になると、カードを無効にし端末装置内に取り込む等の無効処分を行う。

[0013] (10) 合致した場合には、ホストコンピュータはカード利用者が正しいカード所有者であると判断して、引出金額の入力を要求する。

[0014] (11) 利用者が引出要求金額を入力する。

[0015] (12) 引出要求金額が適正であれば、その金額を出金し、キャッシュカードが端末装置から排出され、通帳への記帳あるいは取扱明細書の発行が行われて、取引は終了する。

なお、暗証番号がキャッシュカードに記録されていた場合にはその暗証番号が正しいものとして取引が行われるが、その後磁気記録部からその暗証番号は消去される。

[0016] 図2 (a) に示すのは、図1に示した現行のキャッシュカード処理フローで使用されるキャッシュカードの例である。この図において、1はプラスティック等からなるキャッシュカード本体であり、その表側には情報が記録された磁気ストライプ2及びキャッシュカードの挿入方向を示す矢印3が形成されている。なお、図示は省略したが、所要事項がエンボス文字として掲載されている。

[0017] 磁気ストライプに書き込まれた情報はスキマーと呼ばれる装置を用いて容易に読み取ることが可能なため、偽造カードが作成され、しばしば偽造カードが使用される被害が生じている。

[0018] その対策として、半導体メモリを内蔵したICカードが使用されて来ており、磁気カードに代わるものとして、銀行等は普及を計っている。

[0019] しかしながら、このICカードといえども、メモリに保存された情報を読み取ることは可能であり、手間暇をかけた偽造が行われた場合には、絶対に安全とレづことはできない。その上、ICカードは磁気カードに比べて非常に高価であり、早急な普及は期待できない。

[0020] 銀行のキャッシュカードの場合は、1つの国の中だけで使用可能であれば済むが、クレがットカードの場合は外国でも使用可能である必要があり、世界中で使用されている全ての磁気カードであるクレがットカードを規格を統一したICカードに置き換えることは、事実上不可能である。

[0021] さらに、キャッシュカードとクレがットカードには所有者名等の情報がエンボス加工されて設けられており、これらの情報は磁気情報にも用いられているため、エンボス情報は偽造カード作成の手掛かりとなっている。

[0022] これらの磁気カードあるいはICカードが紛失あるいは盗難に遭った場合には、所有者がその事実に気がつきやすいが、盗難の役に手元に戻った場合、特に盗難に気がつかずに戻った場合には、偽造カードの使用による被害が発生しやすい。

[0023] カードの偽造を防止することによる不正使用防止ではなく、カード使用者の適否を判定するための手段として、これまで4桁の数字で構成された暗証番号が用いられてきた。この暗証番号にはしばしば類推可能な番号が使用され、これまでに多くの被害が生じてきた。最近は類推だけでなく盗撮等の手段による暗証番号の盗視までも行われており、暗証番号による不正使用防止は、きわめて困難となってきている。

[0024] 偽造カードによる被害防止のために、パターン認識技術を利用した生体判別(バイオメトリックス)技術が、一部で採用されている。生体判別技術の代表的なものとして、虹彩判別、指紋判別、掌紋判別、指静脈判別、手掌静脈判別、手甲静脈判別があり、この内虹彩判別以外の判別には接触型と非接触型があるが、何れも予めパターン

を登録する必要があり、パターンの登録に手間がかかり、判別にも時間がかかるため、運用コストが大きくなる。

[0025] 接触型の場合には検出装置に直接触れる必要があるため、衛生上あるいは生理的嫌悪感の問題がある。また、判別部分に負傷した場合、あるいは最悪の場合は判別部分が失われて地場合には、生体判別は不可能である。また、判別過程において部分的な判別しか行っていないため、万全のものとはいえない。

[0026] また、カード所有者本人しか使用することが出来ない生体判別システムは、カードを使用する時間あるいはカード処理装置が身近にないため代理人にカードの取扱を依頼しようとしても、不可能であり、この点でも使用者にとっては不便である。

[0027] 偽造防止の一つの手段として、クレジットカード、紙幣、証券類等にプラスチックに凹凸を形成したエンボスホログラムが取り付けられている。このエンボスホログラムは複製することが非常に困難であるため、エンボスホログラムが付されたカード類を偽造することは事実上不可能であるが、現在の使用形態では人間がそれも一瞥で読み取っているため、類似したエンボスホログラムを使用してカード等を偽造して使用することは可能である。

[0028] 図2(b)に示すのは、官能によるカード真贋認証が行われるホログラム付きクレジットカードの例である。この図において、1はプラスティック等からなるクレジットカード本体であり、その表側には情報が記録された磁気ストライプ2及びキャッシュカードの挿入方向を示す矢印3が形成されている。なお、図示は省略したが、所要事項がエンボス文字として掲載されている。

[0029] このキャッシュカード1は矢印3が記された部分を先にして端末装置に挿入されるが、その先端部付近に例えばエンボスホログラムで構成された真贋認証チップ4が取り付けられている。

[0030] クレジットカードの場合には、キャッシュカードと異なり、磁気ストライプはカードの裏面に設けられているが、カードの端末装置への挿入方向は同じなので、結果としてクレジットカードの磁気情報の読み取り方向はキャッシュカードとは逆となる。

[0031] 真贋認証チップ4はカードを端末装置に挿入する操作者によって、例示したパターン「A」が、目視すなわち官能によって確認され、カード端末装置によって読み取られ

ることはない。

[0032] 官能による真贋認証は、判別をする個人の能力にばらつきがあること、及び同一人であっても判別環境及び心理状態、体調などによるばらつきがあることにより、1次的スクリーニングには大きな効果を発揮するが、信頼性は低い。

[0033] 補助器具による真贋認証は、微細画線、特殊画線、マイクロ文字、特殊形状スクリーン等、ルーペ等の拡大器具を用いることによって、あるいは光学的干渉を発生する特殊フィルタを用いることによって、真贋認証を行う。

[0034] 具体的には、発光基材、発光ラミネートフィルム、発光インキ、サーモクロミックインキ、フォトクロミックインキ等、特殊な光学特性を示す材料を基材・ラミネートフィルム・インキ等に混入し、特殊フィルタ、紫外線ランプ等の補助器具を用いるものがあるが、これらも最終的な判別は人間の官能に頼るため、信頼性は低い。

[0035] 機械処理による真贋認証には、材料の持つ特性を機械的に検出して真贋認証を行うものであり、検出の対象としては磁気、光学特性等の検出がある。

[0036] 具体的には、発光材料,磁性材料を基材・ラミネートフィルム・インキ等に混入し、検出機器を用いるもの、コード化した特定の情報をOCR文字,磁気バーコードにより磁気的あるいは光学的に付与し、磁気・光学検出機器を用いるなものがある。

[0037] 機械処理による真贋認証技術として、生体固有の情報に代えて媒体中にランダム配置された再現性のない人工物を利用する人工物メトリクス・システム(artifact-metric system)が、「金融業務と人工物メトリクス」日本銀行金融研究所(http://www.imes.boj.or.jp/japanese/jdps/2004/04-J-12.pdf)及び「第6回情報セキュリティ・シンポジウム「金融分野における人工物メトリクス」の模様」(http://www.imes.boj.or.jp/japanese/kinyu/2004/kk23-2-6.pdf)に示されている。

[0038] 人工物メトリクスでは、粒状物の光反射パターン、光ファイバの透過光パターン、ポリマファイバの視差画像パターン、ファイバの画像パターン、磁性ファイバの磁気パターン、ランダム記録された磁気パターン、磁気ストライプのランダム磁気パターン、メモリセルのランダム電荷量パターン、導電性ファイバの共振パターン,振動シールの共鳴パターン等偶然によって形成されるパターンを不利用する。

[0039] カードの不正使用や偽造の対象となる事項には、カードが利用者に発給される時

に付与される「カード記載情報」と、カードの製造工程で付与される「カード本体情報」がある。(「連携IC カード券面の偽造防止技術ハンドブック」財務省印刷局(http://www.npb.go.jp/ja/info/ichb.pdf)参照)

[0040] カード記載情報は、カード本体に対してカード発給時に印字・付与される情報であり、所持人情報、有効期限等の発給に関する情報が該当する。不正使用の代表的形態である改竄は、カード記載情報の全部、又は一部の記載情報を書き換える行為であり、正規の情報を消去し、不正な情報を加筆することで行われる。

[0041] カード本体情報は、発給されたカードからカード記載情報を除いたカード自体が有する情報であり、カードの物理的形状、主にプレ印刷工程で付与される背景模様、下地の印刷層及び保護ラミネート層等、カード基体に付随する情報である。

[0042] 偽造は、カード本体について行われる不正行為であり、カード本体に付随する情報である図柄や模様等を複写又は模倣して、外観上近似したカードを作製することで行われ、具体的には真正なカード券面に付与されている図柄や模様等をスキャナ等で読み取り、加工、修正等を加え、プリンタ等を使用して行われる。

[0043] カード本体に対する偽造対策技術は、印刷技術に限っても、印刷方式、インク、印刷模様の組み合わせにより、多数存在するが、決定的なものは現存しない。

[0044] 偽造を判別する真贋認証方法は、大きく分けて、官能によるもの、補助器具によるもの、機械処理によるものがある。

[0045] 官能による真贋認証は、視覚、触覚等の人間の官能で真贋を判別するものであり、視覚によるものには本体の色彩、透かし、見る角度を変化させることによって付与した模様や色彩等が変化するホログラム等があり、触覚によるものには、付与された凹凸形状の検知、カード本体の質感の検知等がある。

[0046] 具体的には、ロゴマーク、特殊フォント、複写防止画線、特色インキ、ホログラム、光学的変化材料、潜像模様等、複製・複写が困難であり、視覚的に容易に真贋判別が可能なもの、エンボス加工、凹凸付与、穿孔等、指感的、視覚的に真贋判別を行なうのがある。

[0047] 図3に、特開平10-44650号公報に開示された金属粒による人工物メトリクス・チップが取り付けられたカードの従来例を示すが、この図において(a)は全体図、(b)

は断面図、(c) は真贋認証チップの拡大図である。

[0048] このカード1は、識別用の開口8が形成された光不透過性であるカード基体7の上に金属粒5が混入された光透過性樹脂である薄板状の人工物メトリクス・チップ4が積層され、その上にカード基体7に形成された開口と同ツ立置に開口が形成され、磁気ストライプ2と矢印3が形成された不透明なカード表面板6が積層されている。

[0049] 金属粒5は、可視らの規則性を有することなく3次元的に光透過性樹脂中に混入されているため、開口を経由して観測される金属粒5の配置パターンは人工物メトリクス・チップ4各々に固有のものである。

[0050] このことを利用して、人工物メトリクス・チップ4を透過する光を開口を経由して撮影することにより金属粒5の配置パターンを観察し、個々の人工物メトリクス・チップ4、すなわちカードを識別する。

[0051] 図4に、特開2003—29636号公報に開示された繊維による人工物メトリクス・チップが取り付けられた真贋識別カードの他の従来例を示す。この図において(a)は全体図、(b)は断面図、(c) は人工物メトリクス・チップの拡大図である。

[0052] このカードは、光不透過性であるカード基体1の開口に、透明樹脂中に網目部材9と短小繊維10が3次元的に混入されて構成された人工物メトリクス・チップ8が嵌入され、カード基体1の表面には磁気ストライプ2と矢印3が形成されている。人工物メトリクス・チップ8には、網目部材9のパターンと短小繊維10とにより干渉パターンが発生する。

[0053] この干渉パターンは、人工物メトリクス・チップ8、すなわちカード各々に固有のものであり、このことを利用して、真贋認証チップの人工物メトリクス・チップ8の識別パターンを透過光あるいは反射光により撮影し、カードを識別する。

[0054] バイオメトイリクスあるいは人工物メトリクスのようなパターンの機械読み取りは、撮像装置で読み取ってパターン認識技術によって判別するのが一般的である。そのため、複写技術による偽造の可能性がある。

[0055] 人工物メトリクス・チップはイメージではない実体物によって構成されているから、偽造の対象となる人工物メトリクス・チップを構成する要素を真正なものと同一形態に配置することは不可能である。しかし、偶々ではあっても同じ構成要素によって同じパタ

ーンが出現する可能性は否定できず、このようにして偶然に得られた贋物は真正なものとして通用する。そのため、人工物メトリクス・チップのみによってカード等が真正であるか否かを確認するのは危険である。

[0056] このように、カード自体の真贋を判定する技術は確立されておらず、偽造することが出来ないカードは実現されていない。したがって、偽造カードの使用を不可能にする技術も実現されていない。

特許文献1:特開平10-44650号公報

特許文献2:特開2003-29636号公報

非特許文献1:「金融業務と人工物メトリクス」日本銀行金融研究所(http://www.imes.boj.or.jp/japanese/jdps/2004/04-J-12.pdf)

非特許文献2:「第6回情報セキュリティシンポジウム「金融分野における人工物メトリクス」の模様」(http://www.imes.boj.or.jp/japanese/kinyu/2004/kk23-2-6.pdf)

非特許文献3:「連携ICカード券面の偽造防止技術ハンドブック」財務省印刷局(http://www.npb.go.jp/jp/info/ichb.pdf)

## 発明の開示

## 発明が解決しようとする課題

[0057] 本出願においては、従来汎用されているキャッシュカードあるいはクレジットカードに基本的な変更を加えることなく、安全性を高めることのできるカード,カード処理方法の発明を提供する。

[0058] 本件出願に係る発明は、真贋認証作業の負担を軽減するとともに、偶然に得られた贋物が真正なものとして通用する可能性を排除することを課題とする。

## 課題を解決するための手段

[0059] そのために、本出願に係る発明では、カードの真贋認証のために偽造することが困難な真贋認証チップを固着するとともに、カードを処理する装置内に真贋認証装置を付加する。

[0060] 真贋認証チップには、透明媒体中に分散された金属等の粒子、透明媒体中に分散された繊維片、透明媒体中に配置された規則性を有するパターンとその透明媒体中に分散された繊維片による干渉パターン、エンボスホログラム、透明媒体中に分散

された蛍光体粒子、任意の媒体中に分散された放射性物質粒子が採用可能である。

[0061] さらに、真贋認証チップに加えてもう一つのチップを設け、そのチップに真贋認証チップに記載された情報をデジタル化し、デジタル化されたデータを暗号化した暗号化データを記載し、真贋証明チップとする。

[0062] カード利用時にはカード上の真贋認証チップのイメージが読み取られデジタル化され、同時に同じカード上に付されている真贋証明チップの暗号化データが復号化され、真贋証明チップから復号化されたデータと真贋認証チップのデータとが対照され、一致すればそのカードは真正なものであるとされ、一致しなければそのカードは偽造されたと判断される。

[0063] 暗号鍵システムにおいて、最も簡便にはカード発行者のみが知っている秘密鍵システムを用いるが、暗号化と複合化に異なる鍵を用いる公開鍵システムも使用可能である。共通鍵システムでは、公開鍵と専用鍵が使用されるが暗号化と復号化にはどちらの鍵を用いることも可能である。

[0064] 暗号化／復号化の負担を軽減するために、MD5(Message Digest 5), SAH－1(Secure Hash Algorithm－1), SAH－2等のハッシュアルゴリズムを使用する。

[0065] デジタル化されたデータにカード等のID,所有者の情報を付加あるいは混入させ、その全体を暗号化する。さらに、デジタル化されたデータにデジタル透かしを挿入する。デジタルデータのハッシュ値化、ID,所有者の情報付加、デジタル透かしの挿入はいずれかのみの使用、幾つかを組み合わせて使用する。

[0066] カードを処理する装置は、暗証番号入力等の具体的な操作が開始される前に、カードの真贋を判別し、偽造カードを排出するか、警報を発するか、偽造カードを処理装置内に取り込む。

## 発明の効果

[0067] 透明媒体中に分散された金属等の粒子、透明媒体中に分散された繊維片、透明媒体中に配置された規則性を有するパターンとその透明媒体中に分散された繊維片による干渉パターン、透明媒体中に分散された蛍光体粒子、任意の媒体中に分散された放射性物質粒子は、偶然のみによって得られるものであるため、複写するこ

とは不可能である。また、エンボスホログラムは立体構造を有しているため、原型から直接にレプリカを製造する以外にコピーすることは不可能である。

[0068] また、磁気記録データあるいはICチップ内のデータをコピーした偽造カードが、排除され、使用が不可能になる。

[0069] さらに、不正使用がなされようとした場合に使用を拒否して、被害を未然に防止することができ、あるいは不正カード使用をある程度容認し、最終的には不正カードを確保することにより、不正使用者を特定することが容易に可能となる。

[0070] 真贋認証チップとそれを証明する真贋証明チップとが一枚のカード上に共存している場合には、暗号鍵がATM等の端末装置に与えられていれば、ホストサーバによることなくカードの真贋を確認することが可能である。

[0071] また、偶然により同じ人工物メトリクスが得られ、同じハッシュ値が得られたとしても、そのハッシュ値にさらに付加あるいは混入させた、カード等のID,所有者の情報の付加あるいは混入のアルゴリズムを知らなければ、暗号化に使用された暗号鍵を知ることはできないため、安全性は高い。

## 図面の簡単な説明

[0072] [図1]現行のキャッシュカード処理フロー図。

[図2]従来のキャッシュカードの説明図。

[図3]人工物メトリクスを使用する従来のカードの例。

[図4]人工物メトリクスを使用する従来のカードの他の例。

[図5]真贋認証チップを取り付けたカードの例。

[図6]真贋認証チップを取り付けたカードの他の例。

[図7]真贋認証チップを取り付けたカードのさらに他の例。

[図8]真贋認証チップ取り付け位置の例の説明図。

[図9]真贋認証チップ取り付け位置の他の例の説明図。

[図10]位置合わせ用マークの説明図。

[図11]乱数に基づいて作成した真贋認証チップの例。

[図12]真贋認証チップに使用する乱数の例。

[図13]真贋認証チップに使用する乱数の配列例。

[図14]真贋認証チップに使用する乱数を2進数とした例。

[図15]真贋認証チップに使用する乱数を2進数として配列した例。

[図16]真贋認証チップに使用する乱数の追加例。

[図17]真贋認証チップに使用する追加乱数を2進数とした例。

[図18]真贋認証チップに使用する追加乱数を4進数とした例。

[図19]真贋認証チップに使用する乱数を4進数として配列した例。

[図20]乱数に基づいて作成した真贋認証チップから、別の真贋認証チップを得る例。

[図21]真贋認証チップと真贋証明チップを取り付けたカードの例。

[図22]図21のカードの真贋証明フロー。

[図23]真贋認証チップと真贋証明チップを取り付けたカードの他の例。

[図24]図23のカードの真贋証明フロー。

[図25]真贋認証チップと真贋証明チップを取り付けたカードのさらに他の例。

[図26]図25のカードの真贋証明フロー。

[図27]真贋認証チップと真贋証明チップを取り付けたカードのまたさらに他の例。

[図28]図27のカードの真贋証明フロー。

[図29]本件出願発明のキャッシュカード処理フロー図。

[図30]本件出願発明の他のキャッシュカード処理フロー図。

[図31]本件出願発明のさらに他のキャッシュカード処理フロー図。

## 符号の説明

[0073] 1 カード

2 磁気ストライプ

3 矢印

4 ,8, 12, 15, 18, 21, 22, 32, 42, 46, 61 真贋認証チップ

5 金属粒

6, 14, 34, 44 表面板

7 ,44 カード基板

9 網目部材

10 短小繊維

11 ,31, 41 真贋認証カード

16, 19, 22, 23, 25 ピット

17, 20, 24 反射ピット

33 蛍光体粒子

43 放射性物質粒子

44, 49, 54, 59 証明チップ

47 ICチップ

48 位置合わせ用マーク

49 移動方向読み取り開始線

50 移動方向読み取り終了線

51, 52 端部指示線

62, 64, 66, 68 真贋証明チップ

60, 63, 65, 67 真贋証明カード

## 発明を実施するための最良の形態

[0074] 以下、図面を参照して発明を実施するための最良の形態を示す。

初めに、カード真贋認証チップについて説明する。

[真贋認証チップ実施例1]

図5に示したのは、真贋認証チップとしてエンボスホログラムチップが取り付けられたカードの基本的構成の実施例1である。この図において(a)は全体図、(b)は断面図、(c)～(e)はエンボスホログラムチップの拡大図である。

[0075] このカード皿は、光不透過性であるカード基体13の上に開口が形成された表面板14が取り付けられ、その開口にエンボスホログラムチップ12が嵌入されている。また、表面板14アには磁気ストライプ2と矢印3が形成されている。

[0076] エンボスホログラムは、使用するレーザ光の1／4波長の深さの孔と孔が形成されていない部分で構成されており、孔の在る部分では出射レーザ光が入射レーザ光に打ち消されることにより出射レーザ光が検出されず、孔のない部分では出射レーザ光が入射レーザ光に打ち消されずに出射レーザ光が検出される。

[0077] 使用されるレーザ光はCDの場合はλ=780nmの赤外レーザであり、λ/4=195nmである。DVDの場合にはλ=650nmの赤色レーザが使用されλ/4=151.25nmである。次世代DVDの場合にはλ=405nmの青紫レーザ、λ=351nmの紫外レーザ、λ=266nmの遠紫外レーザの使用が検討されており、λ/4は各々101.25nm、87.75nm、66.5nmである。

[0078] (c)に示したのは、最も基本的な構造であり、ホログラムチップ15に適宜な間隔で使用レーザ光の1/4波長の深さの孔16と孔が形成されていない部分17とが配置されている。この図に示した例の場合、双方向矢印で示した実線は入射光と出射光がともにあることを表しており、片方向矢印で示した破線は入射光はあるが出射光がないことを表している。

[0079] (d)に示したのは、レーザ光の方向を傾斜させた例であり、傾斜角の情報がなければ書き込まれたデータの読み取りは困難である。この例ではホログラムチップ18に適宜な間隔で使用レーザ光の1/4波長の深さの傾斜した孔19と孔が形成されていない傾斜した部分20とが配置されている。この図に示した例の場合も、双方向矢印で示した実線は入射光と出射光がともにあることを表しており、片方向矢印で示した破線は入射光はあるが出射光がないことを表している。この構造の複製を得ることは、不可能に近い。なお、(c)に示された構造と(d)に示された構造とを共存させることも可能である。

[0080] (e)に示したのは、複数の波長のレーザ光を利用する例であり、使用されるレーザ光全ての波長の情報がなければ書き込まれたデータの読み取りは困難である。この例ではホログラムチップ21に赤色(R)レーザ光の1/4波長の深さの孔22と、緑色(G)レーザ光の1/4波長の深さの孔23と、青色(B)レーザ光の1/4波長の深さの孔25と孔が形成されていない部分24とが適宜な間隔で配置されている。

[0081] この図に示した例の場合にも、双方向矢印で示した実線は入射光と出射光がともにあることを表しており、片方向矢印で示した破線は入射光はあるが出射光がないことを表している。この構造の複製を得ることは、さらに不可能に近い。なお、(d)に示された構造と(e)に示された構造とを共存させることも可能である。

[0082] [真贋認証チップ実施例2]

図6に、真贋認証チップの実施例2を示す。この図において、(a) はカードを上から見た図、(b) はその断面図、(c) は断面図の拡大図である。このカード31は、光不透過性であるカード基体35の上に開口が形成された表面板34が取り付けられ、その開口に樹脂中に蛍光物質粒33が混入されて構成された真贋認証チップ32が嵌入されている。なお、真贋認証チップ32と表面板34の上にさらに他の表面板を積層することも可能である。

[0083] カード基板35は従来から多用されているキャッシュカード等に使用される合成樹脂厚板あるいはプリペイドカード等で使用される合成樹脂薄板である。真贋認証チップ32は、表面板34の開口に嵌合する面積及び厚さを有しており、蛍光物質粒33が混入されている。

[0084] 表面板35の材料はカードの入射光及び出射光に対して透明な合成樹脂でも、カードの入射光及び／又は出射光に対して不透明でありその他の可視光線に対して不透明な合成樹脂のどちらも使用可能である。なお、合成樹脂から構成された真贋認証チップ32と表面板34の上にさらに積層された表面板には人射光及び出射光に対して透明な合成樹脂が用いられる。

[0085] [真贋認証チップ実施例3]

図7に、真贋認証チップの実施例3を示す。この図において、(a)はカードを上から見た図、(b) はその断面図、(c) は断面図の拡大図である。このカード41は、光不透過性であるカード基体45の上に開口が形成された表面板44が取り付けられ、その開口に樹脂中に放射性物質粒20が混入されて構成された真贋認証チップ42が嵌入されている。また、表面板44上には磁気ストライプ2と矢印3が形成されている。

[0086] この混入された放射性物質粒の配置パターンは、その真贋認証チップ42、すなわちカード41に固有のものであり、このことを利用して、カードを識別する。

[0087] [真贋認証チップ取付位置実施例]

図8に、これらの構造を有する真贋認証チップのカードへの取付位置の実施例を示す。真贋認証チップ46の取付位置は図5～図7に示したカード本体のほぼ中央以外の位置の他に、図8 (a) に示す中段先頭位置、(b) に示す中段中央位置の他に、(c) に示す中段後部位置、(d) に示す下段先頭位置、(e) に示す下段中央位置、㈲ に

示す下段後部位置が可能である。上段位置も可能であるが、磁気ストライプからの情報読み取りに影響する可能性がある場合には、上段位置に配置することは避けることが望ましい。

[0088] [真贋認証チップ取付位置実施例2]

カードのセキュリティ強化、あるいは利便性の強化の観点から情報記憶媒体にICチップを用いることが進められている。このICチップは内部に半導体メモリを有しており、この半導体メモリは放射線特に電子線であるほ線に照射されるとメモリが書き換えられてしまうことがある。

[0089] 放射線の中cc線は1枚の紙でも遮蔽することができるため、半導体メモリに対する影響は殆ど考慮する必要はない。しかし、ほ線の遮蔽には1mm厚のアルミニウム板あるいは10mm厚のアクリル板が必要とされる。そこで、ほ線を放射する放射性物質粒を使用する場合には、図9(a), (c), (d)および(有)に示すように、真贋認証チップ36とICチップ80とを10mm以上の間隔を開けて配置することによりほ線による影響を回避することができる。

[0090] [真贋認証チップ読取位置]

キャッシュカード及びクレジットカードの物理的規格は汎用性の観点から厳格に規定されているため、その上に設けられるものも当然にその物理的規格は厳格である。しかし、過酷な使用により変形が生じる可能性は否定できない。

[0091] そのような場合に備えて、真贋認証チップに図10に示す位置合わせ用マーク48を形成しておくことが望ましい。位置合わせ用マークは、最も単純には1個でよいが、より確実に位置合わせを行うためには複数個設ける。

[0092] 読み取りをより確実に行うために、位置合わせ用マークと兼用して、真贋認証チップの読み取り開始位置及び読み取り終了位置に何らかのマーク例えば、図10に示す移動方向読み取り開始線49及び移動方向読み取り終了線50、さらには端部指示線51, 52を設けておく。

[0093] 真贋認証チップ上の情報の読み取りは、真贋認証チップと読み取り装置の相対運動で行うため、確実な読み取りを行うためには真贋認証チップと読み取り装置の運動を同期させる必要がある。そのために真贋認証チップ上に同期信号用のマーク87を

形成しておけば、マークに読み込みに読み取り装置の運動を同期させることができる。

[0094] 読み取り開始・終了線及び／又は同期信号用のマークを信号処理の際の信号正規化に利用することも出来る。これらの位置合わせ用マーク、読み取り開始・終了線及び／又は同期信号用のマークは、何れも蛍光体で構成され、例えばインクジェットプリンタのような適宜な印刷手段で形成することができる。

[0095] [真贋認証チップ実施例4]

図6～図7に示したカード真贋認証チップは人工物メトリクスである。人工物メトリクスは偽造することが不可能である反面、製造する際にパターンを制御することも不可能である。図8～図20により、機械読み取りに適した2値データであるコンピュータによって作成される真贋認証チップの構成例を示す。

[0096] 図8に示した真贋認証チップは、1024個の2値データが32X32のマトリクスに配置されており、この図において、2値データ「0」が書き込まれた箇所は空白で表示され、2値データ「1」が書き込まれた箇所は「木」で表示されている。

[0097] この2値データを得る方法について説明する。図12に示したのは、放射性物質の核崩壊によって放射される放射線を検出することによって得られる、16進数256桁の真性乱数の実例であり、暗号鍵等に使用される乱数は、通常はこのような16進数として供給される。図13に、図12に示した16進乱数を8列32行のマトリクスに配列したものを示す。

[0098] この16進数は、4桁の2進数に置き換えて表現することができる。すなわち、16進数の「0」は2進数の「0000」で、同様に「1」は「0001」で、「2」は「0010」で、「3」は「0011」で、「4」は「0100」で、「5」は「0101」で、「6」は「0110」で、「7」は「0111」で、「8」は「1000」で、「9」は「1001」で、「A」は「1010」で、「B」は「1011」で、「C」は「1100」で、「D」は「1101」で、「E」は「1110」で、「F」は「1111」で、各々表現される。

[0099] このことに基づき、図12に示した256桁の16進乱数を2進乱数に置き換えたものは、図14に示すようになる。1桁の16進数は4桁の2進数に置き換えられるから、256桁の16進数は256桁X4桁＝1024桁の2進数となる。これらの2進数は乱数発生装置

では直接に得られるものであるから、その場合にはこの置き換え操作は不要である。

[0100] これを図13に示した8列32行のマトリクスに配列し、さらに2進数の桁単位に32列32行のマトリクスに配列したものを図15に示す。

[0101] 最後に、図15のマトリクス中の2進数の0に相当する箇所を情報を書き込むことなくそのままとし、1に相当する「ホ」が表示されている箇所に情報を書き込むことにより、図皿に示した真贋認証チップの配列を得ることができる。このように形成された真贋認証チップは32列×32行X1ビットニ1024ビットの真贋認証情報、すなわち1024ビットの真贋認証鍵を有している。

[0102] 図5(c)に示したエンボスホログラム及び図6に示した蛍光物質は、複数波長の光を使用することができる。次に、2値データである機械読み取りに適した、コンピュータによって作成される、一般的にいう赤(R) ,緑(G)及び青(B)の光を利用するカード真贋認証チップのピット構成例を示す。

[0103] これらの、「R」,「G」,「B」はデータが書き込まれていない状態である「0」も含めて合計4つの状態を表現することができる。いいかえれば、これらは4進数として扱うことが可能であり、4進数は4つの2ビット数すなわち「00」,「01」,「10」,「11」で表現することができる。

[0104] 図16に示すのは、図12に示した256桁の16進乱数に先立つさらに256桁の16進乱数を併せて表示したものである。ここで、「16進乱数列a」とあるのは図12に示したのと同じ乱数列であり、「16進乱数列b」とあるのは「16進乱数列a」に先立つ乱数列である。

[0105] この16進乱数列を2進乱数列に変換し、O ,R ,G ,Bと表現される4進数に変換するために2ビット毎に区分した乱数列を図17に示す。

[0106] さらに、2進数「00」を4進数「0」に、2進数「01」を4進数「R」に、2進数「10」を4進数「G」に、2進数「11」を4進数「B」に変換したものを、図18に示す。

[0107] このようにして得られた4進数を図皿あるいは図15に示した2進数と同様に32列X32行のマトリクスに配列したものを、図19に示す。このように形成された真贋認証チップは32列×32行マV2ビットニ2048ビットの真贋認証情報、いいかえれば2048ビットの真贋認証鍵を有している。

[0108] 図20により、1つの乱数列から複数の真贋認証チップを得る方法を説明する。この図において、(a)，(b)，(c)，(d)は各々図11に示した32 X 32のマトリクスパターンに基づいて16 X 16のマトリクスパターンを得たものであり、各々(a)は座標(0，0)を原点とし、(a)は座標(0，0)を原点とし、(b)は座標(1，0)を原点とし、(c)は座標(0，1)を原点とし、(d)は座標(1，1)を起点としている。

このように、図12に示した乱数列から得られた1つのマトリクスパターンから複数のマトリクスパターンを得ることができる。

[0109] 1つの乱数列から複数のマトリクスパターンを得るにはこの他に、図12に示した乱数列の使用開始位置を変化させる、あるいは図13に示したマトリクスパターンの作成開始位置を変化させる等種々の方法が利用可能である。

[0110] このようにすることにより、カード発行者が1つの乱数列をマスター乱数列として秘密に保管し、そのマスター乱数列に基づいて複数のマトリクスパターンを得ることが可能になる。また、複数のマトリクスパターンは原点情報によって自動的に管理することができる。

[0111] 図14及び図15に示した実施例は1ビットで表現される2進数により真贋認証情報を記録し、図19に示した実施例は2ビットで表現される4進数により真贋認証情報を記録している。これらの延長として、3ビットで表現される8進数，4ビットで表現される16進数も使用可能である。

[0112] [証明チップ実施例1]

図21及び図22に、カード自身を証明するカードの実施例を示す。図21にカードを示し、図22に真贋認証チップと真贋証明チップの機能を示す。

[0113] カード60には、人工物メトリクス等のカード真贋認証情報「A」(Authentication)が格納された真贋認証チップ61と、真贋認証情報「A」のデジタル化データ「M」(Message)を暗号化して暗号化データ「C」とし、暗号化データ「C」が格納された真贋証明チップ62が、カード本体と分離不可能な構造で取り付けられている。また、カード60の表面の上部には磁気ストライプ2と矢印3が形成されている。

[0114] 磁気ストライプ2に代えて、あるいはともにICチップを使用することも可能である。また、真贋認証チップ61と真贋証明チップ62とは、図21に示されたように別々の位置

に配置してもよいが、隣接してあるいは一体化して配置してもよい。

[0115] 図22により、図21に示したカード60上の真贋認証チップ61と真贋証明チップ62の機能について、基本的な実施例を説明する。この図において、(1)～(5)はカード発行者によるカード作成するときについての説明であり、(6)～(10)は利用者がATM等の端末装置を用いてカードを利用するときについての説明である。

[0116] (1)人工物メトリクスあるいはエンボスホログラムであるカード真贋認証情報「A」が格納された真贋認証チップ61を作成する。人工物メトリクスは各々が全て異なっているから、人工物メトリクスを有する真贋認証チップ61は全て異なっている。

[0117] また、図面～図20に示した方法により32ビット×32ビット=1024ビット(10進数で307桁)のデータあるいはそれ以上のビット数のデータを使用して図5～図7に示した真贋認証チップを作成すれば、同じ真贋認証チップが存在する確率は無視できる程小さい。また、エンボスホログラムは3次元的構造を有しているから、光学的なコピーは不可能であり、偽造することはきわめて困難である。

[0118] (2)真贋認証チップ61の情報を、アナログ的あるいはデジタル的に読み取る。カードを利用する際の読み取りを正確に行うためには、真贋認証チップ61をカード60に取り付けた後に読み取りを行うことが望ましい。

[0119] (3)読み取られた真贋認証チップ61のアナログイメージをデジタルデータ「M」にデジタル化する。なお、読み取られる真贋認証チップ61に格納されるのがデジタルデータである場合にはデジタル化は不要である。

[0120] (4)デジタルデータ「M」を暗号化し、暗号化データ「C」を得る。

暗号化システムとしては、秘密鍵暗号システム(Secret-key Cryptosystem)、公開鍵暗号システム(Public-key Cryptosystem)が利用可能である。

[0121] 秘密鍵暗号システム(Secret-key Cryptosystem)において使用する暗号鍵は秘密鍵(Secret-key)と呼ばれるが、近年は公開鍵暗号システムが普及するに伴い公開鍵暗号システムで使用する専用鍵(Private-key)を秘密鍵(Secret-key)と呼ぶ人が増えたため、混乱を避けて共通鍵(Common-key)と呼ぶこともある。

[0122] 電子情報通信学会刊「現代暗号理論」によれば、メッセージM(Message)を暗号鍵K(Key)を用いて暗号化(Encryption)して暗号化データ(encrypted-data)Cを得る過程

を、C＝E(K, M)と表現し、暗号化データCを暗号鍵Kを用いて復号化(Decryption)して復号化データを得る過程を、M＝D(K, C)と表現する。

[0123] ここではこれに倣って、デジタルデータ「M」を秘密鍵暗号システムの秘密鍵$K_s$で暗号化して暗号化データ「Cs」を得る過程を、Cs＝E($K_S$, M)と、暗号化データ「Cs」を秘密鍵$K_S$で復号化してデジタルデータ「M」を得る過程をM＝D($K_S$, Cs)と表現する。

[0124] デジタルデータ「M」を公開鍵暗号システムの公開鍵$K_p$で暗号化して暗号化データ「Cp」を得る過程を、Cp＝E($K_p$, M)と、暗号化データ「Cp」を専用鍵$K_V$で復号化してデジタル・イメージ・データMを得る過程をM＝D($K_V$, Cp)と表現する。暗号鍵の配送はこのようにして行われる。

[0125] デジタルデータ「M」を公開鍵暗号システムの専用鍵$K_V$で暗号化して暗号化データCvを得る過程を、Cv＝E($K_V$, M)と、暗号化データ「Cv」を専用鍵$K_p$で復号化してデジタルデータ「A」を得る過程をA＝D($K_p$, Cv)と表現する。デジタル署名はこのようにして行われる。

[0126] (5) 暗号化データ「Cs」, 「Cp」または「Cv」を、証明チップ44に記録・保存し、カード本体60と分離不可能な構造で取り付ける。暗号化データの記録・保存にはバーコード、2次元バーコード等の光学的読み取り記録方法、磁気記録等適宜なものが採用可能である。

[0127] カード60がICチップが搭載されたICカードである場合には、暗号化データをICチップに格納することも可能である。分離不可能な構造として一体構造とする、あるいは溶着等の方法を採用する。また、真贋証明チップをカードに取り付けるのではなく暗号化データをカード自体に記録してもよい。

[0128] (6) カードを利用するときには、真贋証明チップ62に格納された暗号化データ「C」を読み取る。

[0129] (7) 暗号化データ「C」を所定の暗号アルゴリズムと暗号鍵を用いて復号化し、復号化データ「M」を得る。

[0130] (8) 同時に、真贋認証チップ61の情報「A'」を読み取る。読み取り手段はカメラを使用するのが最も一般的であるが、カメラ以外の読み取りヘッドあるいはスキャナ等を

使用することも可能である。

[0131] (9) 読み取られた認証チップの情報「A'」をデジタル化し、デジタルデータ「M'」を得る。

[0132] (10)復号化されたデータ「M」とデジタル化されたデータ「M'」を比較する。同一であれば、真贋認証チップ61と真贋証明チップ62との組合せは正当であると判断され、異なっていれば、真贋認証チップ61と真贋証明チップ62との組合せは正当ではないと判断され、カードは不正であると判断される。このようにして、真贋認証チップ61の正当性はともにカード上に存在する真贋証明チップ62によって証明される。

[0133] この実施例では真贋認証チップ61から読み取られたデータ「M'」と真贋証明チップ62から復号されたデータ「M」とを比較しているが、逆に真贋認証チップ61から読み取られたデータ「M'」を暗号化した暗号化データ「C'」と真贋証明チップ62から読み取られた暗号化データ「C」とを比較するように構成することも可能である。

[0134] 真贋証明チップ62のデータは暗号化されている。その暗号システムは単一の暗号鍵を使用する秘密鍵(あるいは共通鍵)暗号システム及び2つ暗号鍵を使用する公開鍵方式のどちらでも採用可能である。公開鍵システムにおいて暗号化及び復号化に用いる鍵は公開鍵と専用鍵(秘密鍵)の組合せあるいは専用鍵と公開鍵の組合せのどちらの組合せも採用可能である。

[0135] 利用者が端末装置によってカードを利用するときには復号用の暗号鍵が使用されるが、暗号鍵の保管場所として、サーバ内と端末装置内とがある。暗号鍵をサーバ内に保管し、カードの真贋認証が必要になったときに必要な暗号鍵をその都度端末装置に配信する構成にすればオンラインによる安全性の高い方法が可能となる。暗号鍵が端末装置内に保管されていれば、カードの真贋認証はオフラインで端末装置のみによって行うことができる。しかし、端末装置が盗難に遭うと暗号鍵も盗まれることになる。そのようなことを防止するために暗号鍵を端末装置内のDRAMに保管しておき、端末装置が破壊あるいは盗まれたりすることにより電源が切断された場合には、DRAMに保管されていた暗号鍵が失われるように構成すれば、暗号鍵の盗難は防止できる。

[0136] [証明チップ実施例2]

カードの真贋を確認するために保存されたデータをホストのサーバから端末装置に送信して端末装置側で真贋を認証し、あるいは読み取ったカードのデータをサーバに送信してサーバ側で真贋を認証する場合、真贋認証チップ61からのデジタルデータは大きいため、サーバの保存データ量及び通信データ量は大きなものとなる。

[0137] その対策として、例えば代表的なハッシュアルゴリズムであるMD5(Message Digest 5), SAH－1(Secure Hash Algorithm－1), SAH－2等のハッシュアルゴリズムを用いれば、どのように大きなデータであっても16バイトのハッシュ値に変換することができ、元のデータの改竄は必ずハッシュ値に反映される。このことを利用すれば、サーバの保存データ量及び通信データ量は大きならなくてすむ。暗号化／復号化の負担を軽減するために、ハッシュアルゴリズムを使用する。

[0138] 図23及び図24に、ハッシュアルゴリズムを用いたカードの実施例を示す。図23にカードを示し、図24に真贋認証チップと真贋証明チップの機能を示す。

[0139] このカード63は、人工物メトリクス等のカード真贋認証情報「A」(Authentication)が格納された真贋認証チップ61と、認証情報「A」のデジタル化データ「M」(Message)和ッシュ値化してハッシュ値「1」とし、ハッシュ値「1」を暗号化して暗号化データ「Ch」とし、暗号化データ「Ch」が格納された真贋証明チップ64が、カード本体と分離不可能な構造で取り付けられている。また、カード63の表面の上部には磁気ストライプ2と矢印3が形成されている。磁気ストライプ2に代えて、あるいはともにICチップを使用することも可能である。また、真贋認証チップ61と真贋証明チップ64とは、図23に示されたように別々の位置に配置してもよいが、隣接してあるいは一体化して配置してもよい。

[0140] 図24により、図23に示したカード63上の真贋認証チップ61と真贋証明チップ64の機能について説明する。この図において、(1) ～(6) はカード発行者によるカード作成するときについての説明であり、(7) ～(11)は利用者がATM等の端末装置を用いてカードの利用するときについての説明である。

[0141] (1) 人工物メトリクスあるいはエンボスホログラムであるカード真贋認証情報「A」が格納された真贋認証チップ61を作成する。人工物メトリクスは各々が全て異なっているから、人工物メトリクスを有する真贋認証チップ61は全て異なっている。特に3次元

的配置を有する人工物メトリクスのコピーは不可能であるから、偽造することはできない。

[0142] また、図皿～図20に示した方法により32ビット×32ビット=1024ビット(10進数で307桁)のデータあるいはそれ以上のビット数のデータを使用して図5～図7に示した真贋認証チップを作成すれば、同じ真贋認証チップが存在する確率は無視できる程小さい。また、エンボスホログラムは3次元的構造を有しているから、光学的なコピーは不可能であり、偽造することはきわめて困難である。

[0143] (2) 真贋認証チップ61の情報を、アナログ的あるいはデジタル的に読み取る。カードを利用する際の読み取りを正確に行うためには、真贋認証チップ61をカード63に取り付けた後に読み取りを行うことが望ましい。

[0144] (3) 読み取られた真贋認証チップ61のアナログイメージをデジタルデータ「M」にデジタル化する。なお、読み取られる真贋認証チップ61に格納されるのがデジタルデータである場合にはデジタル化は不要である。

[0145] (4)デジタルデータ「M」をハッシュし、ハッシュ値「H」を得る。汎用されているMD5アルゴリズムによりハッシュ他場合に得られるハッシュ値は16バイト(=128ビット)である。

[0146] (5) ハッシュ値「H」を暗号化し、暗号化データ「Ch」を得る。暗号化システムとしては、秘密鍵暗号システム(Secret-key Cryptosystem)、公開鍵暗号システム(Public-key Cryptosystem)が利用可能である。

[0147] (6) 暗号化データ「Ch」を、真贋証明チップ64に記録・保存し、カード本体63と分離不可能な構造で取り付ける。暗号化データの記録・保存にはバーコード、2次元バーコード等の光学的読み取り記録方法、磁気記録等適宜なものが採用可能である。

[0148] カード63がICチップが搭載されたICカードである場合には、暗号化データをICチップに格納することも可能である。分離不可能な構造として一体構造とする、あるいは溶着等の方法を採用する。また、チップを取り付けるのではなくカード自体に記録してもよい。

[0149] (7) カードを利用するときには、真贋証明チップ64に格納された暗号化データ「Ch」を読み取る。

[0150] (8) 暗号化データ「Ch」を所定の暗号アルゴリズムと暗号鍵を用いて復号化し、復号化データ「H」を得る。

[0151] (9) 同時に、真贋認証チップ61の情報「A'」を読み取る。

読み取り手段はカメラを使用するのが最も一般的であるが、カメラ以外の読み取りヘッドあるいはスキャナ等を使用することも可能である。

[0152] (10) 読み取られた認証チップの情報「A'」をデジタル化し、デジタルデータ「M'」を得る。

[0153] (11) デジタルデータ「M'」をハッシュし、ハッシュ値「H'」を得る。

[0154] (12) 復号化データ「H」とハッシュ値「H'」を比較する。

同一であれば、真贋認証チップ61と真贋証明チップ64との組合せは正当であると判断され、異なっていれば、真贋認証チップ61と真贋証明チップ64との組合せは正当ではないと判断され、カードは不正であると判断される。このようにして、真贋認証チップ61の正当性は、真贋認証チップ61とともにカード上に存在する真贋証明チップ64によって証明される。

[0155] この実施例では真贋認証チップ61から読み取られたデータ「M'」をハッシュしたハッシュ値「H'」と真贋証明チップ64から読み取られた暗号化ハッシュ値「Ch」から復号されたハッシュ値「H」とを比較しているが、逆に真贋認証チップ61から読み取られたデータ「M'」をハッシュしたハッシュ値「H'」を暗号化した暗号化ハッシュ値「Ch'」と真贋証明チップ64から読み取られた暗号化データ「Ch」とを比較するように構成することも可能である。

[0156] なお、この実施例における使用する暗号システム、暗号鍵の使用法及び管理方法は、証明チップの実施例2の場合と変わるところはないので、新たな説明は省略した。

[0157] [証明チップ実施例3]

認証チップが破損あるいは汚損され、認証情報の読み取りが不可能になることがあり得る。そうすると、そのカードが正当なものであっても、使用することはできなくなる。そのような事態に備えるための構成を説明する。

[0158] 図25及び図26に、カードのIDを用いたカードの実施例を示す。図25にカードを示

し、図26に図25に示した真贋認証チップと真贋証明チップの機能を示す。

[0159] このカード65は、人工物メトリクス等のカード真贋認証情報「A」(Authentication)が格納された真贋認証チップ61と、真贋認証情報「A」のデジタル化データ「M」(Message)にカードのID等の情報を付加してID付加データ「i」とし、ID付加データ「i」を暗号化して暗号化データ「Ci」とし、暗号化データ「Ci」が格納された真贋証明チップ66が、カード本体と分離不可能な構造で取り付けられている。また、カード65の表面の上部には磁気ストライプ2と矢印3が形成されている。磁気ストライプ2に代えて、あるいはともにICチップを使用することも可能である。また、真贋認証チップ61と真贋証明チップ66とは、図25に示されたように別々の位置に配置してもよいが、隣接してあるいは一体化して配置してもよい。

[0160] 図26により、図25に示したカード65上の真贋認証チップ61と真贋証明チップ66の機能について説明する。この図において、(1)～(6)はカード発行者によるカード作成するときについての説明であり、(7)～(11)は利用者がATM等の端末装置を用いてカードを利用するときについての説明である。

[0161] (1)人工物メトリクスあるいはエンボスホログラムであるカード真贋認証情報「A」が格納された真贋認証チップ61を作成する。

[0162] 人工物メトリクスは各々が全て異なっているから、人工物メトリクスを有する真贋認証チップ61は全て異なっている。特に3次元的配置を有する人工物メトリクスのコピーは不可能であるから、偽造することはできない。

[0163] また、図皿～図20に示した方法により32ビット×32ビット＝1024ビット(10進数で307桁)のデータあるいはそれ以上のビット数のデータを使用して図5～図7に示した真贋認証チップを作成すれば、同じ真贋認証チップが存在する確率は無視できる程小さい。また、エンボスホログラムは3次元的構造を有しているから、光学的なコピーは不可能であり、偽造することはきわめて困難である。

[0164] (2)真贋認証チップ61の情報を、アナログ的あるいはデジタル的に読み取る。カードを利用する際の読み取りを正確に行うためには、真贋認証チップ61をカード65に取り付けた後に読み取りを行うことが望ましい。

[0165] (3)読み取られた真贋認証チップ61のアナログイメージをデジタルデータ「M」にデ

ジタル化する。なお、読み取られる真贋認証チップ61に格納されるのがデジタルデータである場合にはデジタル化は不要である。

[0166] (4)デジタルデータ「M」にカードのID等のデータを付加し、ID付加データ「I」を得る。

[0167] (5) ID付加データ「I」を暗号化し、暗号化データ「Ci」を得る。暗号化システムとしては、秘密鍵暗号システム(Secret-key Cryptosystem)、公開鍵暗号システム(Public-key Cryptosystem)が利用可能である。

[0168] (6) 暗号化データ「Ci」を、真贋証明チップ66に記録・保存し、カード本体65と分離不可能な構造で取り付ける。暗号化データの記録・保存にはバーコード、2次元バーコード等の光学的読み取り記録方法、磁気記録等適宜なものが採用可能である。

[0169] カード65がICチップが搭載されたICカードである場合には、暗号化データをICチップに格納することも可能である。分離不可能な構造として一体構造とする、あるいは溶着等の方法を採用する。また、チップを取り付けるのではなくカード自体に記録してもよい。

[0170] (7) カードを利用するときには、真贋証明チップ66に格納された暗号化データ「Ci」を読み取る。

[0171] (8) 暗号化データ「Ci」を所定の暗号アルゴリズムと暗号鍵を用いて復号化し、復号化データ「I」を得る。

[0172] (9) 同時に、真贋認証チップ61の情報「A'」を読み取る。読み取り手段はカメラを使用するのが最も一般的であるが、カメラ以外の読み取りヘッドあるいはスキャナ等を使用することも可能である。

[0173] (10)読み取られた真贋認証チップ61の情報「A'」をデジタル化し、デジタルデータ「M'」を得る。

[0174] (11)デジタルデータ「M'」にカードのID等のデータを付加し、ID付加データ「I'」を得る。

[0175] (12)復号化データ「I」とID付加データ「I'」を比較する。同一であれば、真贋認証チップ61と真贋証明チップ66との組合せは正当であると判断され、異なっていれば、真贋認証チップ61と真贋証明チップ66との組合せは正当ではないと判断され、カ

ードは不正であると判断される。

[0176] このようにして、真贋認証チップ61の正当性は、ともにカード上に存在する真贋証明チップ66によって証明される。

[0177] 真贋証明チップ66に記録されたデータは真贋認証チップ61の情報に基づくデータにIDを付加したデータを暗号化したものである。真贋認証チップ61の正当性を確認するためにはデータを比較する前に真贋認証チップ66から得られたデータにIDを付加する必要がある。このIDを秘密にしておくことにより、IDを知らない者が暗号解読を行って暗号鍵を知ることは不可能である。

[0178] この実施例では真贋認証チップ61から読み取られた情報「A'」をデジタル化してデジタルデータ「M'」とし、カード情報を付加したデータ「i'」と、真贋証明チップ66から読み取られた暗号化データ「Ci」を復号化したデータ「i」とを比較している。これは、逆に真贋証明チップ66から読み取られたデータ「Ci」を復号したデータ「i」からカード情報を除去して得られたデジタルデータ「M」と、真贋認証チップ61から読み取られた情報「A'」をデジタル化したデジタルデータ「M'」とを比較するように構成することも可能である。

[0179] なお、この実施例における使用する暗号システム、暗号鍵の使用法及び管理方法は、証明チップの実施例Ⅰの場合と変わるところはないので、新たな説明は省略した。

[0180] 真贋認証チップと真贋証明チップが共存したカードは利用者が管理している。また、真贋認証チップには暗号化の対象となる真贋認証情報が裸の状態で存在しており、真贋証明チップには真贋認証情報の暗号化データが存在している。このような状況において、カードが悪意を持つ者の手中に落ちた場合、あるいは利用者が悪意ある者であった場合には、暗号が解読され、暗号鍵が知られてしまう。そのような事態を防止するための構成を説明する。

[0181] 図27及び図28に、電子透かしを用いたカードの実施例を示す。図27にカードを示し、図28に図27に示した真贋認証チップと真贋証明チップの機能を示す。

[0182] このカード67は、人工物メトリクス等のカード真贋認証情報「A」(Authentication)が格納された真贋認証チップ61と、真贋認証情報「A」のデジタル化データ「M」(Messa

9o)に電子透かし(Watar Marking)を付加して電子透かし付データ「W」とし、電子透かし付データ「W」を暗号化して暗号化データ「Cw」とし、暗号化データ「Cw」が格納された真贋証明チップ68が、カード本体と分離不可能な構造で取り付けられている。また、カード67の表面の上部には磁気ストライプ2と矢印3が形成されている。磁気ストライプ2に代えて、あるいはともにICチップを使用することも可能である。また、真贋認証チップ61と真贋証明チップ68とは、図27に示されたように別々の位置に配置してもよいが、隣接してあるいは一体化して配置してもよい。

[0183] 図28により、図27に示したカード67上の真贋認証チップ61と真贋証明チップ68の機能について説明する。この図において、(1)～(6)はカード発行者によるカード作成についての説明であり、(7)～(11)は利用者がATM等の端末装置を用いてカードの利用するときについての説明である。

[0184] (1)人工物メトリクスあるいはエンボスホログラムであるカード真贋真贋認証情報「A」が格納された真贋認証チップ61を作成する。

[0185] 人工物メトリクスは各々が全て異なっているから、人工物メトリクスを有する真贋認証チップ61は全て異なっている。特に3次元的配置を有する人工物メトリクスのコピーは不可能であるから、偽造することはできない。また、図皿～図20に示した方法により32ビット×32ビット=1024ビット(10進数で307桁)のデータあるいはそれ以上のビット数のデータを使用して図5～図7に示した真贋認証チップを作成すれば、同じ真贋認証チップが存在する確率は無視できる程小刮、。また、エンボスホログラムは3次元的構造を有しているから、光学的なコピーは不可能であり、偽造することはきわめて困難である。

[0186] (2)真贋認証チップ61の情報を、アナログ的あるいはデジタル的に読み取る。カードを利用する際の読み取りを正確に行うためには、真贋認証チップ61をカード67に取り付けた後に読み取りを行うことが望ましい、。

[0187] (3)読み取られた真贋認証チップ61のアナログイメージをデジタルデータ「M」にデジタル化する。なお、読み取られる真贋認証チップ61に格納されるのがデジタルデータである場合にはデジタル化は不要である。

[0188] (4)デジタルデータ「M」に電子透かしを付加し、電子透かし付データ「W」を得る。

[0189] (5) 電子透かし付データ「W」を暗号化し、暗号化データ「Cw」を得る。

[0190] (6) 暗号化データ「Cw」を、真贋証明チップ68に記録・保存し、カード本体55と分離不可能な構造で取り付ける。暗号化データの記録・保存にはバーコード、2次元バーコード等の光学的読み取り記録方法、磁気記録等適宜なものが採用可能である。

[0191] カード67がICチップが搭載されたICカードである場合には、暗号化データをICチップに格納することも可能である。分離不可能な構造として一体構造とする、あるいは溶着等の方法を採用する。また、チップを取り付けるのではなくカード自体に記録してもよい。

[0192] (7) カードを利用するときには、真贋証明チップ68に格納された暗号化データ「Cw」を読み取る。

[0193] (8) 暗号化データ「Cw」を所定の暗号アルゴリズムと暗号鍵を用いて復号化し、復号化データ「W」を得る。

[0194] (9) 同時に、真贋認証チップ61の情報「A'」を読み取る。読み取り手段はカメラを使用するのが最も一般的であるが、カメラ以外の読み取りヘッドあるいはスキャナ等を使用することも可能である。

[0195] (10) 読み取られた真贋認証チップの情報「A'」をデジタル化し、デジタルデータ「M'」を得る。

[0196] (11) デジタルデータ「M'」に電子透かしを付加し、電子透かし付加データ「W'」を得る。

[0197] 復号化データ「W」とハッシュ値「W'」を比較する。同一であれば、真贋認証チップ61と真贋証明チップ68との組合せは正当であると判断され、異なっていれば、真贋認証チップ61と真贋証明チップ68との組合せは正当ではないと判断される。

[0198] このようにして、真贋認証チップ61の正当性は、ともにカード上に存在する真贋証明チップ68によって証明される。

[0199] 真贋証明チップ68に記録されたデータは真贋認証チップ61の情報に基づくデータに電子透かしを付加したデータを暗号化したものである。真贋認証チップ61の正当性を確認するためにはデータを比較する前に真贋認証チップ61から得られたデータに電子透かしを付加する必要がある。この電子透かしを秘密にしておくことにより

、電子透かしを知らない者が暗号解読を行って暗号鍵を知ることは不可能である。

[0200] この実施例では真贋認証チップ61から読み取られた情報「A'」をデジタル化してデジタルデータ「M'」とし、電子透かしを付加したデータ「W'」と、真贋証明チップ68から読み取られた暗号化データ「Cw」を復号化したデータ「W」とを比較している。これは、逆に真贋証明チップ68から読み取られたデータ「Cw」を復号したデータ「W」からカード情報を除去して得られたデジタルデータ「M」と、真贋認証チップ61から読み取られた情報「A'」をデジタル化したデジタルデータ「M'」とを比較するように構成することも可能である。

[0201] なお、この実施例における使用する暗号システム、暗号鍵の使用法及び管理方法は、証明チップの実施例Eの場合と変わるところはないので、新たな説明は省略した。

[証明チップ実施例5]

以上説明した証明チップ例は、証明チップの実施例1に示された基本的な構成に証明チップの実施例2ではハッシュアルゴリズムを、証明チップの実施例3ではカード等のIDを、証明チップの実施例4では電子透かしを、各々付加することによって、偽造を困難にしている。

これらの付加された技術は、単にそれのみが付加されるのではなく、幾つかを組合わせる、すなわち、ハッシュアルゴリズムとカード等のIDを、ハッシュアルゴリズムと電子透かしを、カード等のIDと電子透かしを、さらにはハッシュアルゴリズムとカード等のIDと電子透かしを組み合わせることも可能である。

[0202] カード真贋認証処理フローを説明する。

[処理フロー実施例1]。

図29により、カード真贋認証処理フローの実施例1を説明する。

(1)カード利用者がATM等の端末装置のカード挿入口に矢印部を先頭にしてキャッシュカードを挿入すると、カード挿入口のセンサがそのことを感知し、カードを装置内に取り込む。

[0203] (2)カードを取り込む際に、端末装置はカードの磁気記録部からカード情報を読み込む。

[0204] (3)端末装置は、挿入されたカードがその端末装置で取り扱うことが可能なカードであるか否かを判断する。

[0205] (4)読み込んだカード情報から、取扱が可能であることを示す情報が確認されなかった場合、あるいは正規のカードであっても破損あるいは汚損等により カードの情報が読みとれなかった場合には、端末装置はそのカードが取り扱うことが出来ない不適正なカードであるとして排出する。

[0206] (5)端末装置は、カード取り込み時のカードの移動を利用する機械的走査、あるいはカードが取り込まれた停止した状態で真贋認証チップから真贋認証情報を読み取る。

[0207] (6)端末装置は、読み込まれたカード真贋認証情報が正しいか否かを判断する。

[0208] (7)端末装置がカード真贋認証情報が正しくないと判断したときには、挿入されたカードが正規のものではないと判断し、カードを端末装置から排出し、処理を終了する。

[0209] (8)端末装置が、カード真贋認証情報が正規のものであると判断したときには、出金額等のさらなる入力操作をユーザに要求する。

[0210] (9)ユーザが要求に従い、出金額等の入力操作を行う。

[0211] (10)ホストコンピュータは、出金額等の入力操作の内容が適切であるか否かを判断する。

[0212] (11)ホストコンピュータは、出金額等の入力操作の内容が残高不足等の理由により適切でないと判断したときには、カードを端末装置から排出し、処理を終了する。

[0213] (12)ホストコンピュータは、出金額等の入力操作の内容が適切であると判断したときには、出金等により出力し、カードを端末装置から排出し、処理を終了する。

[0214] [処理フロー実施例2]

図30により、カード真贋認証処理フローの実施例2を説明する。

このカード真贋認証処理フローの実施例2は、カード真贋認証処理フローの実施例1では、カード真贋認証情報が正しくないときには、カードを端末装置から排出するのに対し、真贋認証情報が正しくないときには、カードを端末装置に取り込み、警報を発する。このようにすることにより、不正カードの摘発が容易になる。

[0215] (1)カード利用者がATM等の端末装置のカード挿入口に矢印部を先頭にしてキャッシュカードを挿入すると、カード挿入口のセンサがそのことを感知し、カードを装置内に取り込む。

[0216] (2) カードを取り込む際に、端末装置はカードの磁気記録部からカード情報を読み込む。

[0217] (3) 端末装置は、挿入されたカードがその端末装置で取り扱うことが可能なカードであるか否かを判断する。

[0218] (4)読み込んだカード情報から、取扱が可能であることを示す情報が確認されなかった場合、あるいは正規のカードであっても破損あるいは汚損等によりカードの情報が読みとれなかった場合には、端末装置はそのカードが取り扱うことが出来ない不適正なカードであるとして排出する。

[0219] (5) 端末装置は、カード取り込み時のカードの移動を利用する機械的走査、あるいはカードが取り込まれた停止した状態で真贋認証チップから真贋認証情報を読み取る。

[0220] (6)端末装置は、読み込まれたカード真贋認証情報が正しいか否かを判断する。

[0221] (7) 端末装置がカード真贋認証情報が正しくないと判断したときには、挿入されたカードが正規のものではないと判断し、カードを端末装置内に収納するとともに警報を発する。

[0222] この警報は端末機から離隔した場所でのみ発するようにし、端末機には故障表示をするようにすれば不正規カード使用者の身柄確保が容易になる。

[0223] (8)端末装置が、カード真贋認証情報が正規のものであると判断したときには、出金額等のさらなる入力操作をユーザに要求する。

[0224] (9) ユーザが要求に従い、出金額等の入力操作を行う。

[0225] (10)ホストコンピュータは、出金額等の入力操作の内容が適切であるか否かを判断する。

[0226] (11)ホストコンピュータは、出金額等の入力操作の内容が残高不足等の理由により適切でないと判断したときには、カードを端末装置から排出し、処理を終了する。

[0227] (12)ホストコンピュータは、出金額等の入力操作の内容が適切であると判断したと

きには、出金等により出力し、カードを端末装置から排出し、処理を終了する。

[0228] [処理フロー実施例3]

図31により、カード真贋認証処理フローの実施例3を説明する。

このカード真贋認証処理フローの実施例3は、カード真贋認証処理フローの実施例2では、カード真贋認証情報が正しくないときには、直ちにカードを端末装置に取り込み、警報を発するのみ対し、カード利用者に操作を行わせる。

このようにすることにより、不正カードの摘発が確実になる。

[0229] (1)カード利用者がATM等の端末装置のカード挿入口に矢印部を先頭にしてキャッシュカードを挿入すると、カード挿入口のセンサがそのことを感知し、カードを装置内に取り込む。

[0230] (2)カードを取り込む際に、端末装置はカードの磁気記録部からカード情報を読み込む。

[0231] (3)端末装置は、挿入されたカードがその端末装置で取り扱うことが可能なカードであるか否かを判断する。

[0232] (4)読み込んだカード情報から、取扱が可能であることを示す情報が確認されなかった場合、あるいは正規のカードであっても破損あるいは汚損等によりカードの情報が読みとれなかった場合には、端末装置はそのカードが取り扱うことが出来ない不適正なカードであるとして排出する。

[0233] (5)端末装置は、カード取り込み時のカードの移動を利用する機械的走査、あるいはカードが取り込まれた停止した状態で真贋認証チップから真贋認証情報を読み取る。

[0234] (6)端末装置は、読み込まれたカード真贋認証情報が正しいか否かを判断する。

[0235] (7)端末装置がカード真贋認証情報が正しくないと判断したときには、出金額等のさらなる入力操作をユーザに要求する。

[0236] (8)ユーザが要求に従い、出金額等の入力操作を行う。

[0237] (9)カードを端末装置内に収納するとともに警報を発する。

[0238] この警報は端末機から離隔した場所でのみ発するようにし、端末機には故障表示をするようにすれば不正規カード使用者の確保が容易になる。

[0239] (10)端末装置が、カード真贋認証情報が正規のものであると判断したときには、出金額等のさらなる入力操作をユーザに要求する。

[0240] (11)ユーザが要求に従い、出金額等の入力操作を行う。

[0241] (12)ホストコンピュータは、出金額等の入力操作の内容が適切であるか否かを判断する。

[0242] (14)ホストコンピュータは、出金額等の入力操作の内容が残高不足等の理由により適切でないと判断したときには、カードを端末装置から排出し、処理を終了する。

[0243] このような構成にすることにより、不正規カード使用者が端末装置を使用する時間が長くなり身柄確保のための時間が長くなるだけでなく、操作を行わせることにより、指紋等の証拠の採取が可能になる。

その際、接触型のタッチスイッチを採用すると指紋の採取がより確実になる。

## 産業上の利用可能性

[0244] 以上説明したカード真贋認証チップ、カード真贋証明チップを有するカードは、銀行キャッシュカード、クレジットカード、プリペイドカード、ポイントカード、証券、IDカード、入構証、証明書等に採用可能である。

# 請求の範囲

[1] 真贋認証が必要となる対象物であって、前記対象物には前記対象物を特定する固有の複写不能な情報が、前記対象物から分離不可能に付与された、真贋認証対象物。

[2] 前記対象物を特定する固有の複写不能な情報が人工物メトリクスパターンである、請求項1の真贋認証対象物。

[3] 前記対象物を特定する固有の複写不能な情報が人為的パターンである、請求項1の真贋認証対象物。

[4] 真贋認証が必要となる対象物であって、前記対象物には前記対象物を特定する固有の複写不能な情報と、前記対象物の真贋を証明するための情報が、
前記対象物から分離不可能に付与された、真贋認証対象物。

[5] 前記対象物を特定する固有の複写不能な情報と、前記対象物の真贋を証明するための情報が、異なる位置に付与された、請求項4の真贋認証対象物。

[6] 前記対象物を特定する固有の複写不能な情報と、前記対象物の真贋を証明するための情報が、同一位置に付与された、請求項4の真贋認証対象物。

[7] 前記対象物を特定する固有の複写不能な情報が人工物メトリクスパターンである、請求項4,請求項5又は請求項6の真贋認証対象物。

[8] 前記対象物を特定する固有の複写不能な情報が人為的パターンである、請求項4,請求項5又は請求項6の真贋認証対象物。

[9] 前記人為的パターンが、マトリクス状に配置されたデジタルデータであり、前記デジタルデータは2進乱数に基づいて決定されている、請求項8の真贋認証対象物。

[10] 前記人為的パターンが、より大きなマトリクス状に配置されたデジタルデータの一部分である、請求項9の真贋認証対象物。

[11] 前記対象物の真贋を証明するための情報が、前記対象物を特定する固有の複写不能な情報に基づいて得られた暗号化データである、請求項6,請求項7,請求項8,請求項9又は請求項10の真贋認証対象物。

[12] 前記暗号化データが前記対象物を特定する固有の複写不能な情報を暗号化して得られた暗号化データである、請求項皿の真贋認証対象物。

[13] 前記暗号化データが前記対象物を特定する固有の複写不能な情報のハッシュ値を暗号化して得られた暗号化データである、請求項1乃至12の真贋認証対象物。

[14] 前記暗号化データが前記対象物を特定する固有の複写不能な情報と前記対象物の識別情報からなる情報を暗号化して得られた暗号化データである、請求項1乃至12の真贋認証対象物。

[15] 前記暗号化データが前記対象物を特定する固有の複写不能な情報と電子透かしからなる情報を暗号化して得られた暗号化データである、請求項11の真贋認証対象物。

[16] 前記暗号化データが前記真贋認証対象物の発行者が管理する共通鍵システムの共通鍵を用いて暗号化されている、請求項1乃至10,請求項12,請求項13,請求項14又は請求項15の真贋認証対象物。

[17] 前記暗号化データが前記真贋認証対象物の発行者が管理する公開鍵システムの公開鍵を用いて暗号化されている、請求項1乃至10,請求項12,請求項13,請求項14又は請求項15の真贋認証対象物。

[18] 前記暗号化データが前記真贋認証対象物の発行者が管理する公開鍵システムの秘密鍵を用いて暗号化されている、請求項1乃至10,請求項12,請求項13,請求項14又は請求項15の真贋認証対象物。

[19] 対象物の真贋認証をインフラシステムであって、前記対象物には前記対象物を特定する固有の複写不能な情報と、前記対象物の真贋を判別するための情報が、前記対象物から分離不可能に付与されており、対象物を特定する情報と前記対象物の真贋を判別するための情報により、前記真贋認証対象物の真贋を判定する真贋認証システム。

[20] 前記対象物を特定する固有の複写不能な情報が人工物メトリクスパターンである、請求項19の真贋認証システム。

[21] 前記対象物を特定する固有の複写不能な情報が複数の人為的パターンである、請求項19の真贋認証システム。

[22] 前記対象物の真贋を証明するための情報が、前記対象物を特定する固有の複写不能な情報に基づいて得られた暗号化データである、請求項19の真贋認証システム。

[23] 前記暗号ｲﾋﾞデータが前記対象物を特定する固有の複写不能な情報を暗号化して得られた暗号ｲﾋﾞデータである、請求項22の真贋認証システム。

[24] 前記暗号ｲﾋﾞデータが前記対象物を特定する固有の複写不能な情報のﾊｯｼｭ値を暗号ｲﾋﾞして得られた暗号ｲﾋﾞデータである、請求項22の真贋認証システム。

[25] 前記暗号ｲﾋﾞデータが前記対象物を特定する固有の複写不能な情報と前記対象物の識別情報からなる情報を暗号ｲﾋﾞして得られた暗号ｲﾋﾞデータである、請求項22の真贋認証システム。

[26] 前記暗号ｲﾋﾞデータが前記対象物を特定する固有の複写不能な情報と電子透かしからなる情報を暗号ｲﾋﾞして得られた暗号ｲﾋﾞデータである、請求項22の真贋認証システム。

[27] 前記暗号ｲﾋﾞデータが前記真贋認証対象物の発行者が管理する共通鍵システムの共通鍵を用いて暗号ｲﾋﾞされている、請求項22 ,請求項23 ,請求項24 ,請求項25又は請求項26の真贋認証システム。

[28] 前記暗号ｲﾋﾞデータが前記真贋認証対象物の発行者が管理する公開鍵システムの公開鍵を用いて暗号ｲﾋﾞされている、請求項２０,請求項21 ,請求項22 ,請求項23 ,請求項24 ,請求項25又は請求項26の真贋認証システム。

[29] 前記暗号ｲﾋﾞデータが前記真贋認証対象物の発行者が管理する公開鍵システムの公開鍵を用いて暗号ｲﾋﾞされている、請求項２０,請求項21 ,請求項22 ,請求項23 ,請求項24 ,請求項25又は請求項26の真贋認証システム。

[30] 真贋認証情報が記載されたカードを処理する方法であって、前記カードにはカード真贋認証情報が記録されており、前記真贋認証情報と前記カード真贋認証情報を比較し、前記真贋認証情報と前記カード真贋認証情報とが合致した場合にのみカード挿入者の希望する取引を行う、カード処理方法。

[31] 前記真贋認証情報と前記カード真贋認証情報とが一致しなかったときに、前記カードを没収する、請求項３０のカード処理方法。

[32] 前記真贋認証情報と前記カード真贋認証情報とが一致しなかったときに、取引を継続しながら警報を出す、請求項３０のカード処理方法。

# 補正書の請求の範囲

[2007年5月25日 (25. 05. 2007) 国際事務局受理]

1．(補正後) 真贋認証が必要となる対象物であって、前記対象物には前記対象物を特定する固有の複写不能な情報と読み取り位置合わせ用マークが設けられた真贋認証チップが、前記対象物から分離不可能に付与された、真贋認証対象物。

2．前記対象物を特定する固有の複写不能な情報が、人工物メトリクスパターンである、請求の範囲第1項の真贋認証対象物。

3．前記対象物を特定する固有の複写不能な情報が、人為的パターンである、請求の範囲第1項の真贋認証対象物。

4．(補正後) 真贋認証が必要となる対象物であって、前記対象物には前記対象物を特定する固有の複写不能な情報と読み取り位置合わせ用マークが設けられた真贋認証チップと、前記真贋認証チップの真贋を証明するための情報とが、

前記対象物から分離不可能に付与された、真贋認証対象物。

5．(補正後) 前記対象物を特定する固有の複写不能な情報と読み取り位置合わせ用マークが設けられた真贋認証チップと、前記真贋認証チップの真贋を証明するための情報とが、異なる位置に付与された、請求の範囲第4項の真贋認証対象物。

6．(補正後) 前記対象物を特定する固有の複写不能な情報と読み取り位置合わせ用マークが設けられた真贋認証チップと、前記真贋認証チップの真贋を証明するための情報とが、同じ位置に付与された、請求の範囲第4項の真贋認証対象物。

7．前記対象物を特定する固有の複写不能な情報が、人工物メトリクスパターンである、請求の範囲第項4，請求の範囲第項5又は請求の範囲第6項の真贋認証対象物。

8．前記対象物を特定する固有の複写不能な情報が、人為的パターンである、請求の範囲第項4，請求の範囲第項5又は請求の範囲第6項の真贋認証対象物。

9．前記人為的パターンが、マトリクス状に配置されたデジタルデータであり、前記デジタルデータは2進乱数に基づいて決定されている、請求の範囲第8項の真贋認証対象物。

１０．前記人為的パターンが、より大きなマトリクス状に配置されたデジタルデータの一部分である、請求の範囲第９項の真贋認証対象物。

１１．（補正後）前記真贋認証チップの真贋を証明するための情報が、前記対象物を特定する固有の複写不能な情報に基づいて得られた暗号化データである、請求の範囲第６項，請求の範囲第７項，請求の範囲第８項，請求の範囲第９項又は請求の範囲第１０項の真贋認証対象物。

１２．前記暗号化データが、前記対象物を特定する固有の複写不能な情報を暗号化して得られた暗号化データである、請求の範囲第１１項の真贋認証対象物。

１３．前記暗号化データが、前記対象物を特定する固有の複写不能な情報のハッシュ値を暗号化して得られた暗号化データである、請求の範囲第１１項の真贋認証対象物。

１４．前記暗号化データが、前記対象物を特定する固有の複写不能な情報と前記対象物の識別情報からなる情報を暗号化して得られた暗号化データである、請求の範囲第１１項の真贋認証対象物。

１５．前記暗号化データが、前記対象物を特定する固有の複写不能な情報と電子透かしからなる情報を暗号化して得られた暗号化データである、請求の範囲第１１項の真贋認証対象物。

１６．前記暗号化データが、前記真贋認証対象物の発行者が管理する共通鍵システムの共通鍵を用いて暗号化されている、請求の範囲第１１項，請求の範囲第１２項，請求の範囲第１３項，請求の範囲第１４項又は請求の範囲第１５項の真贋認証対象物。

１７．前記暗号化データが、前記真贋認証対象物の発行者が管理する公開鍵システムの公開鍵を用いて暗号化されている、請求の範囲第１１項，請求の範囲第１２項，請求の範囲第１３項，請求の範囲第１４項又は請求の範囲第１５項の真贋認証対象物。

１８．前記暗号化データが、前記真贋認証対象物の発行者が管理する公開鍵システムの秘密鍵を用いて暗号化されている、請求の範囲第１１項，請求の範囲第１２項，請求の範囲第１３項，請求の範囲第１４項又は請求の範囲第１５項の真贋認証対象物。

１９．（補正後）対象物の真贋認証を行うシステムであって、前記対象物には前記対象物を特

定する固有の複写不能な情報と読み取り位置合わせ用マークが設けられた真贋認証チップと、前記対象物の真贋を証明するための真贋証明チップが、前記対象物から分離不可能に付与されており、真贋認証チップと前記真贋証明チップにより、前記対象物の真贋を判定する真贋認証システム。

２０．前記対象物を特定する固有の複写不能な情報が、人工物メトリクスパターンである、請求の範囲第１９項の真贋認証システム。

２１．前記対象物を特定する固有の複写不能な情報が、複数の人為的パターンである、請求の範囲第１９項の真贋認証システム。

２２．（補正後）前記真贋認証チップの真贋を証明するための情報が、前記対象物を特定する固有の複写不能な情報に基づいて得られた暗号化データである、請求の範囲第１９項の真贋認証システム。

２３．前記暗号化データが、前記対象物を特定する固有の複写不能な情報を暗号化して得られた暗号化データである、請求の範囲第２２項の真贋認証システム。

２４．前記暗号化データが、前記対象物を特定する固有の複写不能な情報のハッシュ値を暗号化して得られた暗号化データである、請求の範囲第２２項の真贋認証システム。

２５．前記暗号化データが、前記対象物を特定する固有の複写不能な情報と前記対象物の識別情報からなる情報を暗号化して得られた暗号化データである、請求の範囲第２２項の真贋認証システム。

２６．前記暗号化データが、前記対象物を特定する固有の複写不能な情報と電子透かしからなる情報を暗号化して得られた暗号化データである、請求の範囲第２２項の真贋認証システム。

２７．前記暗号化データが、前記真贋認証対象物の発行者が管理する共通鍵システムの共通鍵を用いて暗号化されている、請求の範囲第２２項，請求の範囲第２３項，請求の範囲第２４項，請求の範囲第２５項又は請求の範囲第２６項の真贋認証システム。

２８．前記暗号化データが、前記真贋認証対象物の発行者が管理する公開鍵システムの公開鍵を用いて暗号化されている、請求の範囲第２０項，請求の範囲第２１項，請求の範囲第２２項，

請求の範囲第２３項，請求の範囲第２４項，請求の範囲第２５項又は請求の範囲第２６項の真贋認証システム。

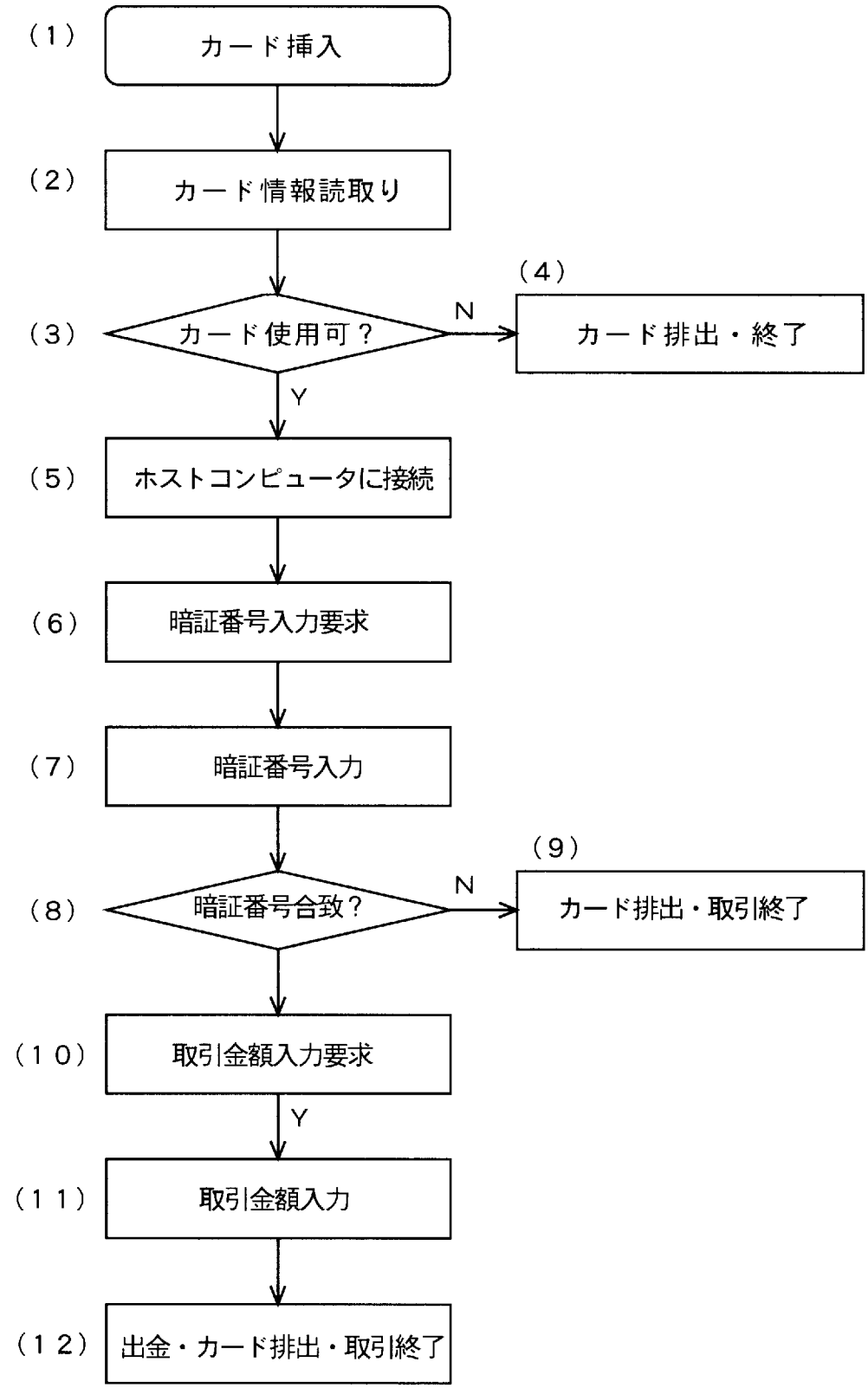
２９．（補正後）前記暗号化データが前記真贋認証対象物の発行者が管理する公開鍵システムの秘密鍵を用いて暗号化されている、請求の範囲第２０項，請求の範囲第２１項，請求の範囲第２２項，請求の範囲第２３項，請求の範囲第２４項，請求の範囲第２５項又は請求の範囲第２６項の真贋認証システム。

３０．（削除）

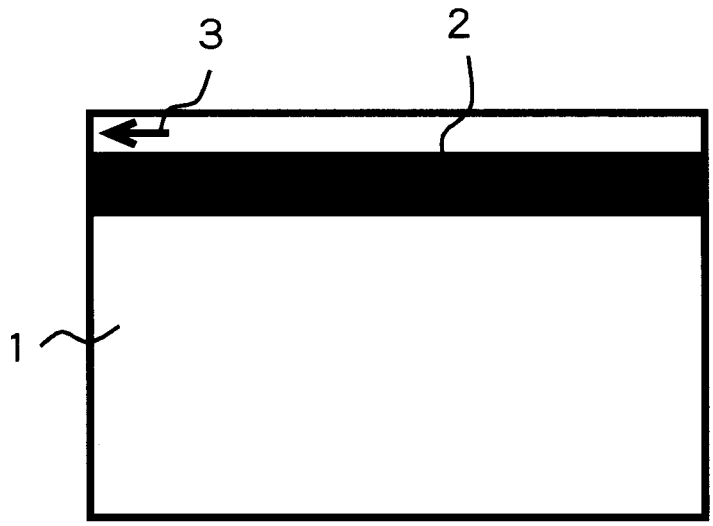
３１．（削除）

３２．（削除）

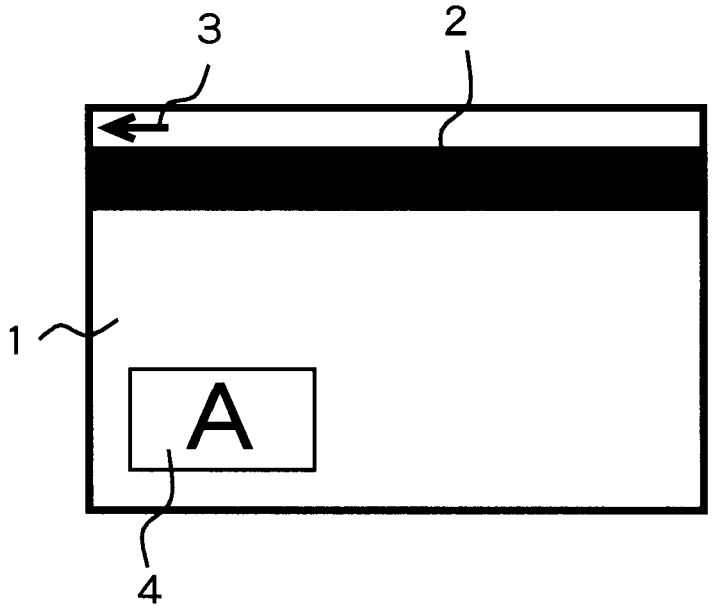
[図1]


（1）
カード挿入
（2）
カード情報読取り
（3）
カード使用可？
N
（4）
カード排出・終了
Y
（5）
ホストコンピュータに接続
（6）
暗証番号入力要求
（7）
暗証番号入力
（8）
暗証番号合致？
N
（9）
カード排出・取引終了
（１０）
取引金額入力要求
Y
（１１）
取引金額入力
（１２）
出金・カード排出・取引終了

[図2]

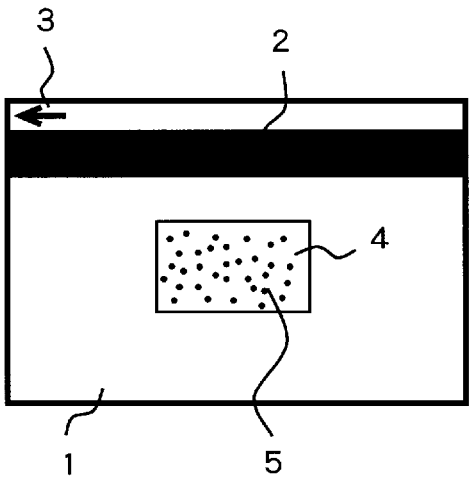



(a)

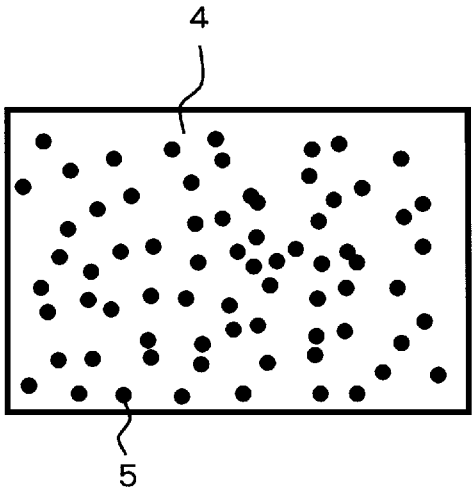



(b)

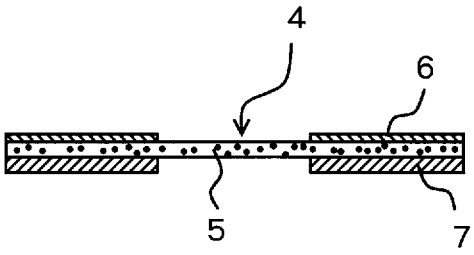
[図3]




(a)

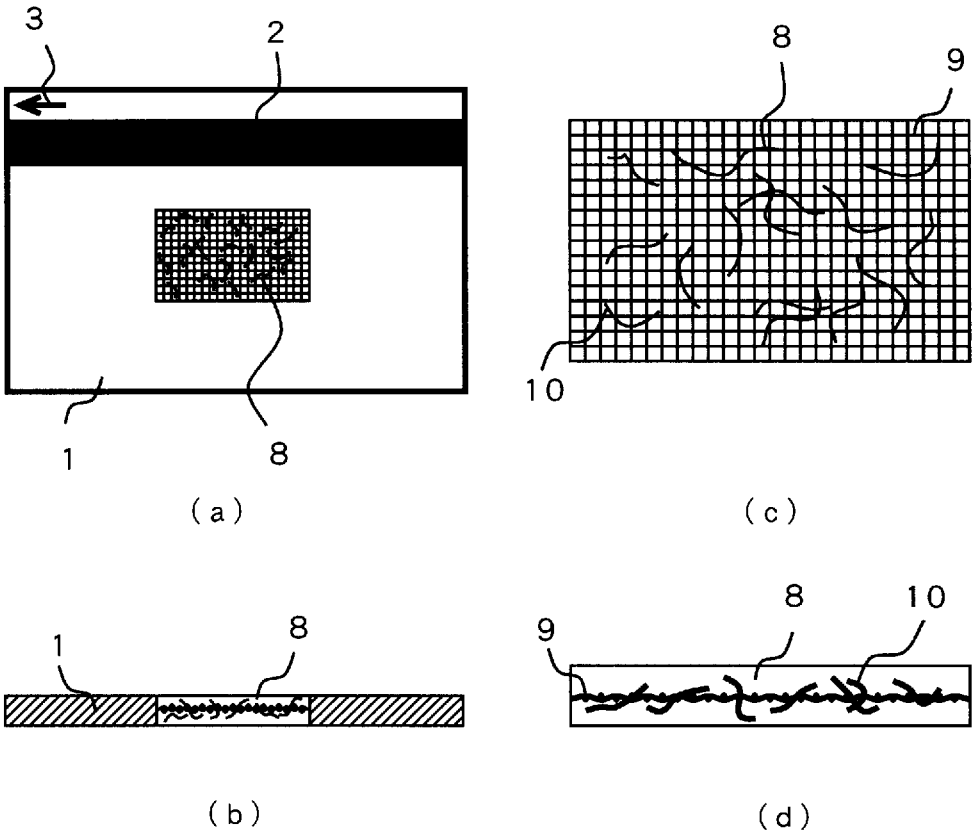



(c)

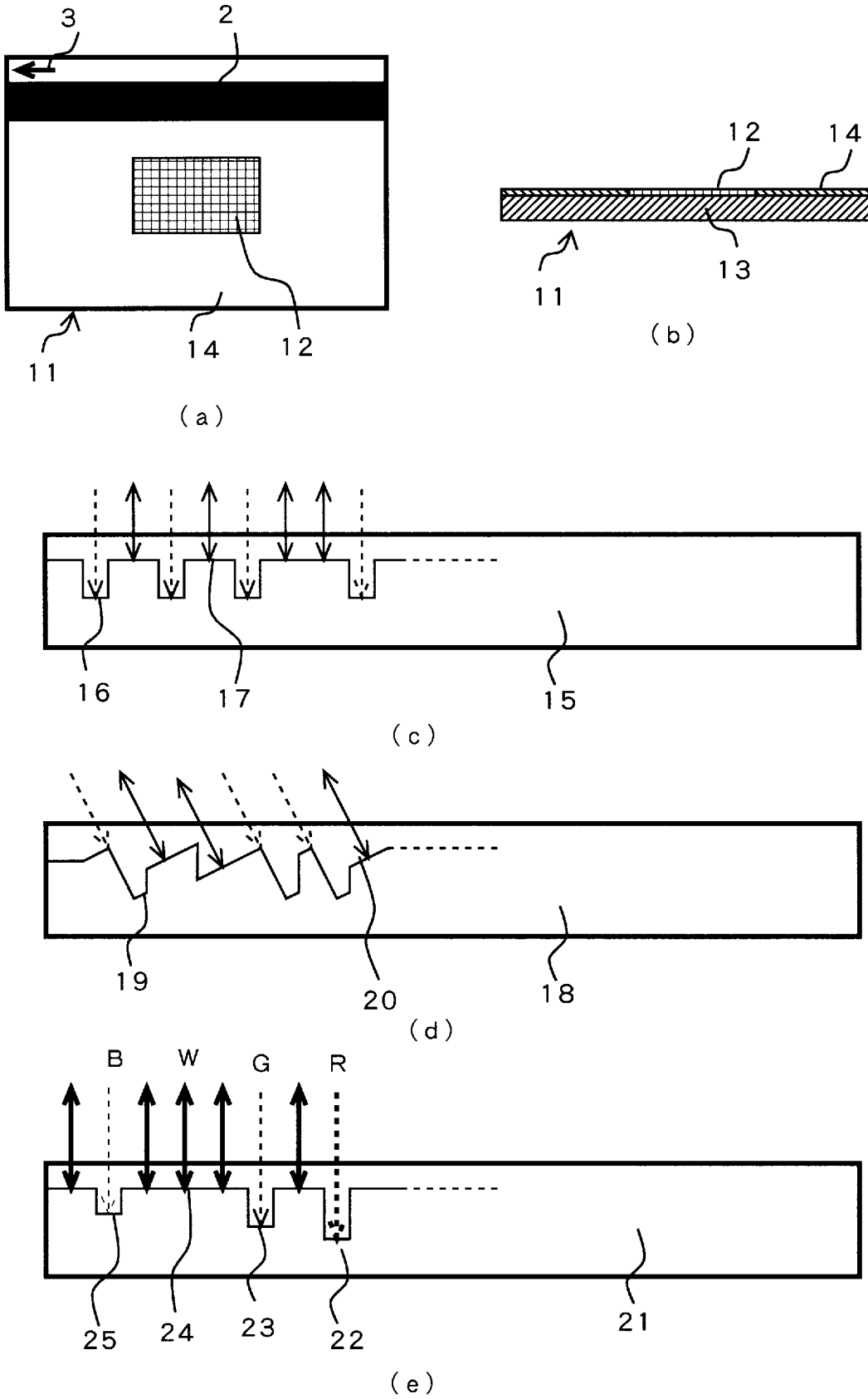



(b)

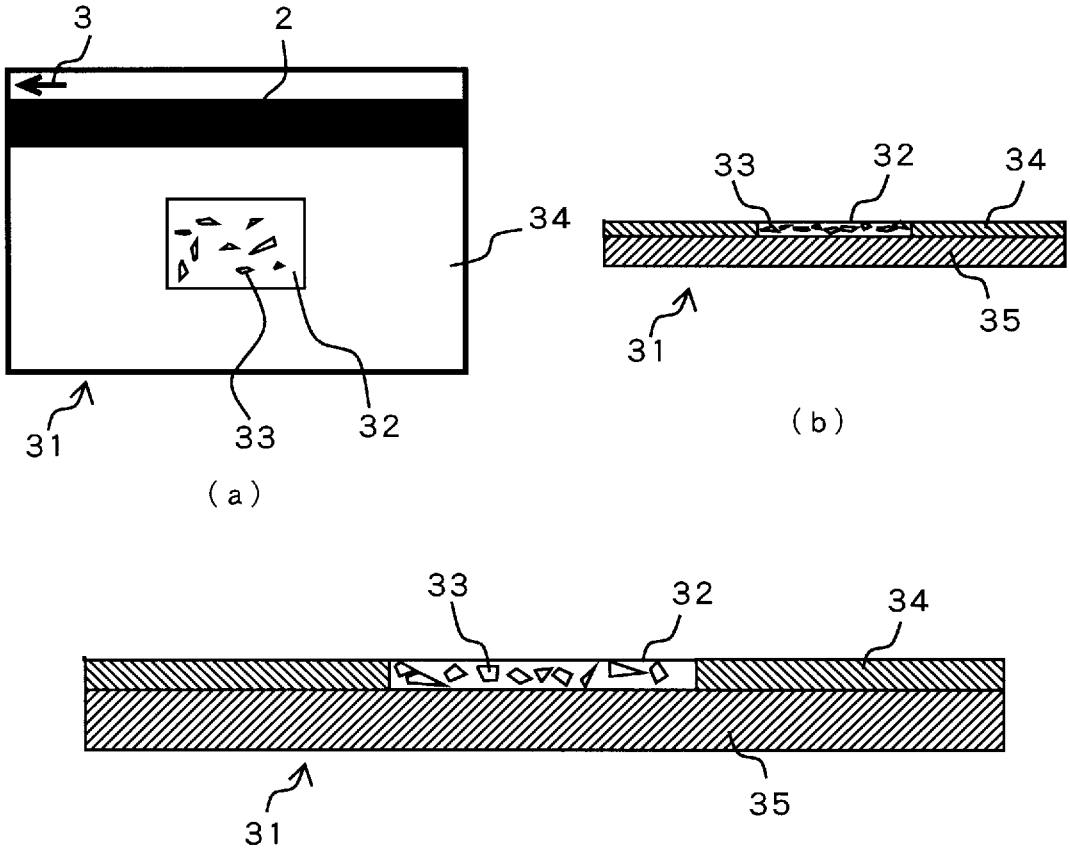
[図4]



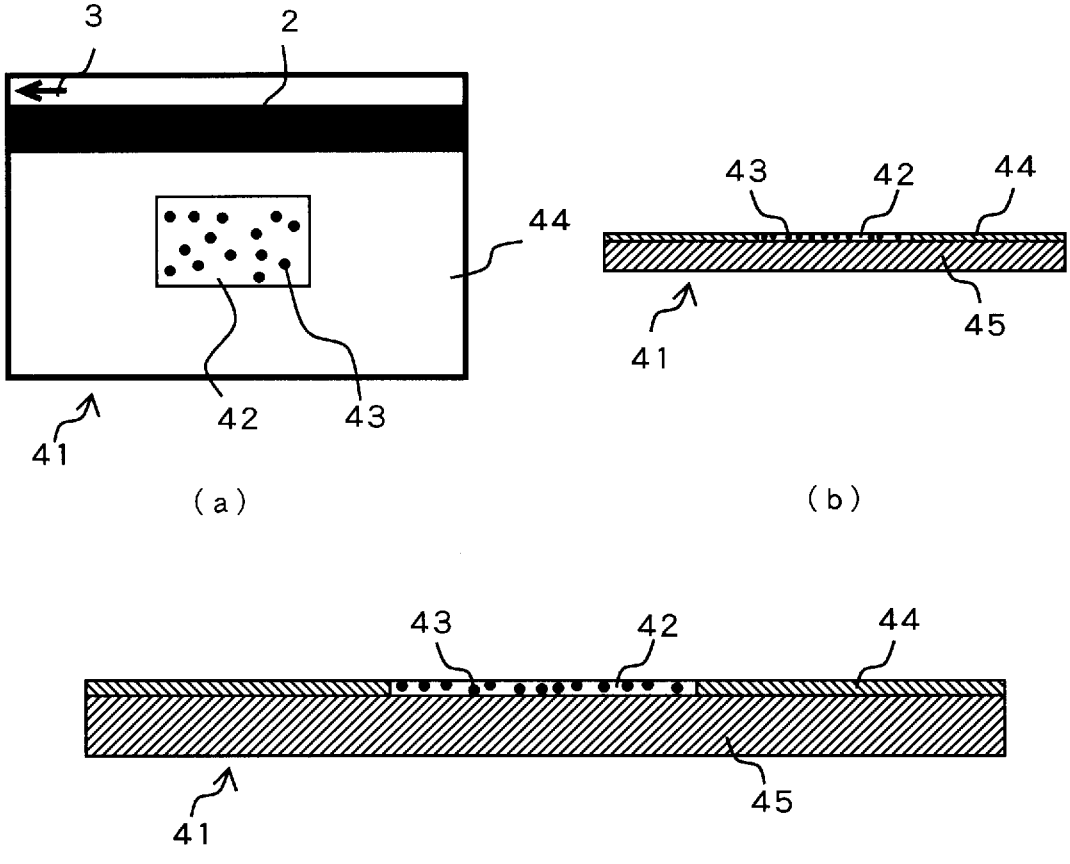
[図5]



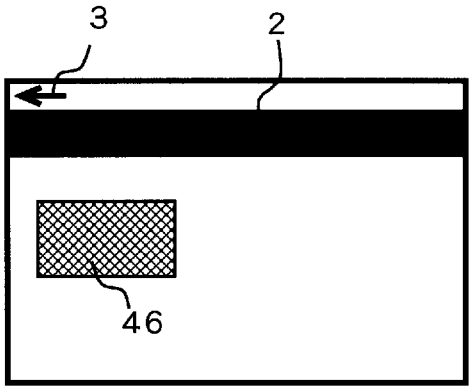
[図6]


3
2
34
33
32
31
(a)
33
32
34
35
31
(b)
33
32
34
35
31
(c)

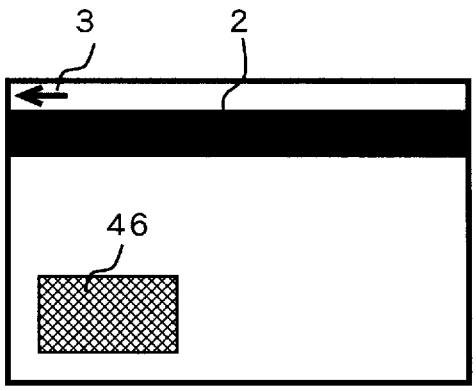
[図7]


3
2
44
42
43
41
(a)
43
42
44
45
41
(b)
43
42
44
45
41
(c)

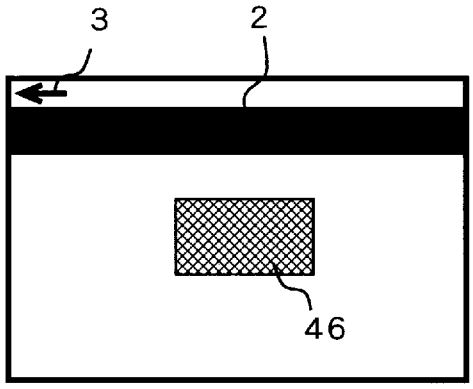
[図8]



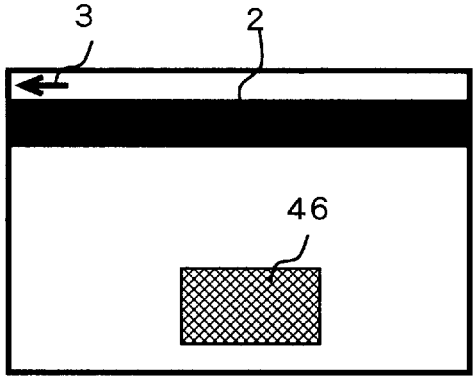

(a)



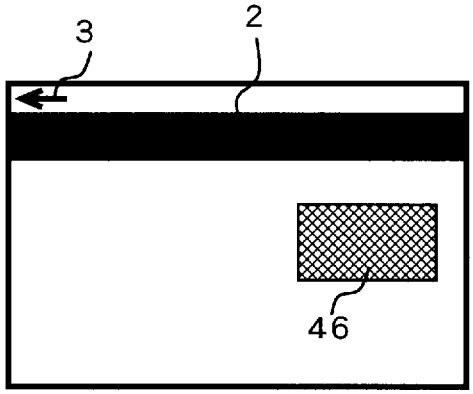

(d)



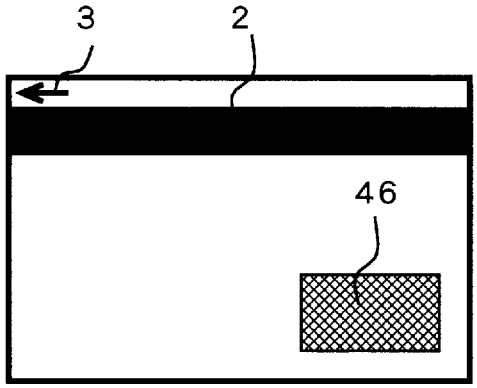

(b)




(e)

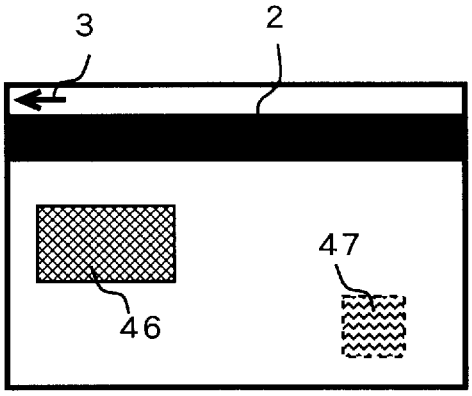



(c)

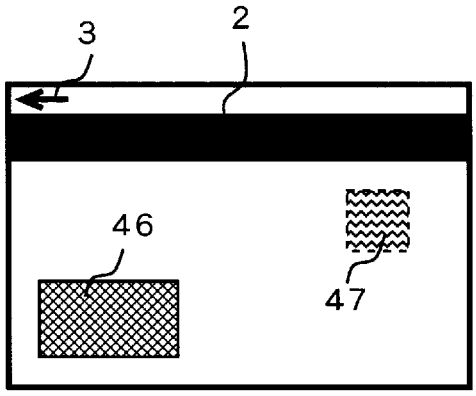



(f)

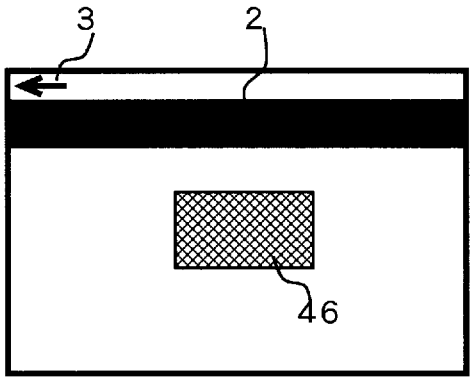
[図9]



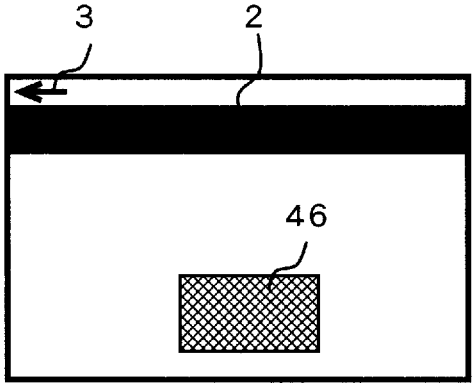

(a)



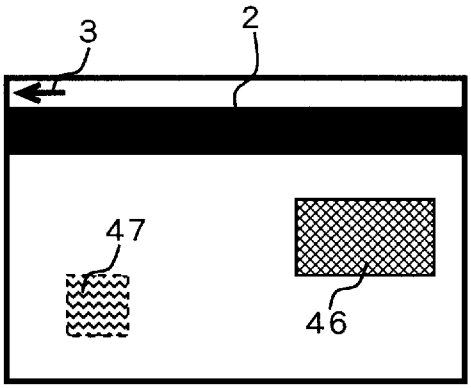

(d)



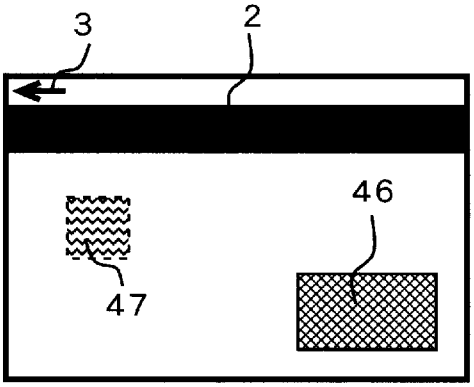

(b)




(e)

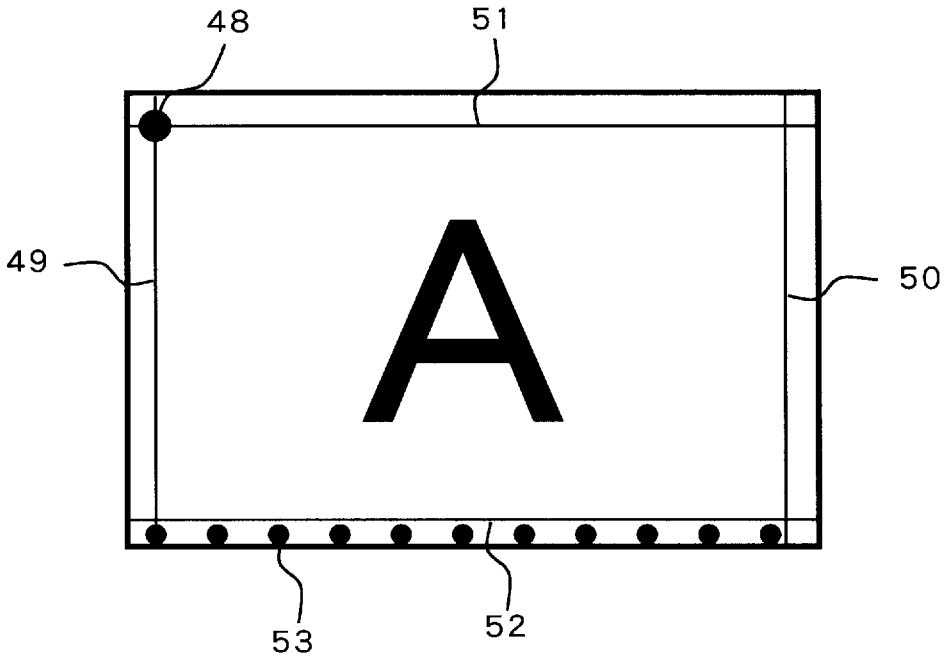



(c)

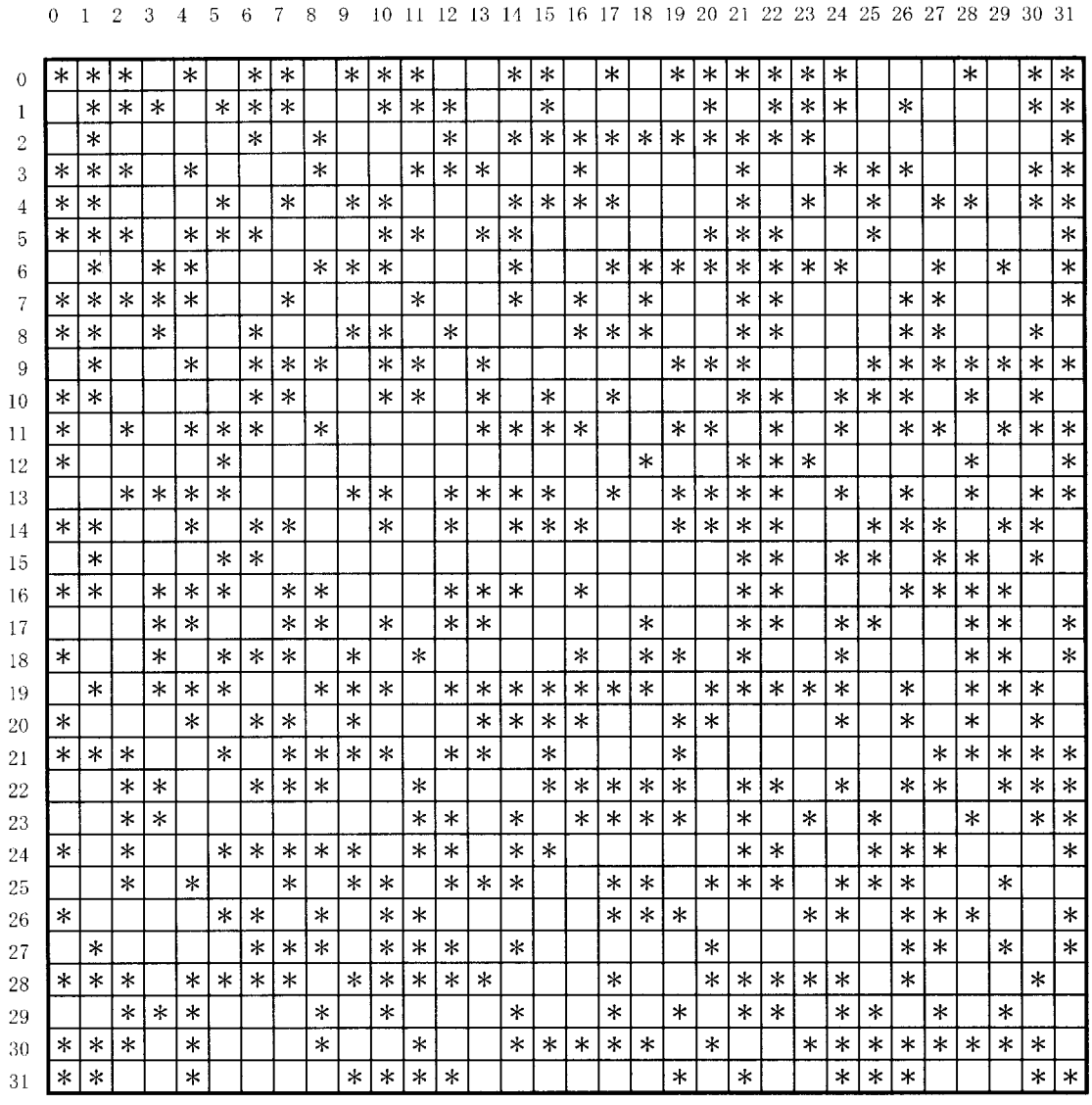



(f)

[図10]


48
51
49
A
50
53
52

[図11]


0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
0 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
1 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
2 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
3 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
4 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
5 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
6 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
7 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
8 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
9 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
10 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
11 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
12 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
13 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
14 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
15 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
16 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
17 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
18 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
19 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
20 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
21 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
22 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
23 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
24 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
25 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
26 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
27 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
28 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
29 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
30 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
31 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *

[図12]

EB735F8B773903BA3428BFF01E89C84E3
C5633C555BEE3604E41588E27F95F9125A631
D2688E63248BB41C7FC33546EAAE879AB7
8400270933C6F5EABCB2B9E76460006DA
DD8E8633C19AC26CD97503B48D5CEFEFAE
8B47988AAE5ED101F3391F6B7301AF54B
A7DB0671296E6EE4866B071B943BA0835
EF7C4FA2388A2566D4E8933E9FEC87814E3

[図13]

| E | B | 7 | 3 | 5 | F | 8 | B |
|---|---|---|---|---|---|---|---|
| 7 | 7 | 3 | 9 | 0 | B | A | 3 |
| 4 | 2 | 8 | B | F | F | 0 | 1 |
| E | B | 7 | 3 | 5 | F | 8 | B |
| 7 | 7 | 3 | 9 | 0 | B | A | 3 |
| 4 | 2 | 8 | B | F | F | 0 | 1 |
| E | 8 | 9 | C | 8 | 4 | E | 3 |
| C | 5 | 6 | 3 | C | 5 | 5 | B |
| E | E | 3 | 6 | 0 | E | 4 | 1 |
| 5 | 8 | E | 2 | 7 | F | 9 | 5 |
| F | 9 | 1 | 2 | A | 6 | 3 | 1 |
| D | 2 | 6 | 8 | E | 6 | 3 | 2 |
| 4 | B | B | 4 | 1 | C | 7 | F |
| C | 3 | 3 | 5 | 4 | 6 | E | A |
| A | E | 8 | 7 | 9 | A | B | 7 |
| 8 | 4 | 0 | 0 | 2 | 7 | 0 | 9 |
| 3 | C | 6 | F | 5 | E | A | B |
| C | B | 2 | B | 9 | E | 7 | 6 |
| 4 | 6 | 0 | 0 | 0 | 6 | D | A |
| D | D | 8 | E | 8 | 6 | 3 | C |
| 1 | 9 | A | C | 2 | 6 | C | D |
| 9 | 7 | 5 | 0 | B | 4 | 8 | D |
| 5 | C | E | F | E | F | A | E |
| 8 | B | 4 | 7 | 9 | 8 | A | A |
| E | 5 | E | D | 1 | 0 | 1 | F |
| 3 | 3 | 9 | 1 | F | 6 | B | 7 |
| 3 | 0 | 1 | A | F | 5 | 4 | B |
| A | 7 | D | B | 0 | 6 | 7 | 1 |
| 2 | 9 | 6 | E | 6 | E | E | 4 |
| 8 | 6 | B | 0 | 7 | 1 | B | 9 |
| 4 | 3 | B | A | 0 | 8 | 3 | 5 |
| E | F | 7 | C | 4 | F | A | 2 |
| 3 | 8 | A | 2 | 5 | 6 | D | 4 |
| E | 8 | 9 | 3 | E | 9 | F | E |
| C | 8 | 7 | 8 | 1 | 4 | E | 3 |

[図14]

1110, 1011, 0111, 0011, 0101, 1111, 1000, 1011,
0111, 0111, 0011, 1001, 0000, 1011, 1010, 0011,
0100, 0010, 1000, 1011, 1111, 1111, 0000, 0001,
1110, 1000, 1001, 1100, 1000, 0100, 1110, 0011,
1100, 0101, 0110, 0011, 1100, 0101, 0101, 1011,
1110, 1110, 0011, 0110, 0000, 1110, 0100, 0001,
0101, 1000, 1110, 0010, 0111, 1111, 1001, 0101,
1111, 1001, 0001, 0010, 1010, 0110, 0011, 0001,
1101, 0010, 0110, 1000, 1110, 0110, 0011, 0010,
0100, 1011, 1011, 0100, 0001, 1100, 0111, 1111,
1100, 0011, 0011, 0101, 0100, 0110, 1110, 1010,
1010, 1110, 1000, 0111, 1001, 1010, 1011, 0111,
1000, 0100, 0000, 0000, 0010, 0111, 0000, 1001,
0011, 1100, 0110, 1111, 0101, 1110, 1010, 1011,
1100, 1011, 0010, 1011, 1001, 1110, 0111, 0110,
0100, 0110, 0000, 0000, 0000, 0110, 1101, 1010,
1101, 1101, 1000, 1110, 1000, 0110, 0011, 1100,
0001, 1001, 1010, 1100, 0010, 0110, 1100, 1101,
1001, 0111, 0101, 0000, 1011, 0100, 1000, 1101,
0101, 1100, 1110, 1111, 1110, 1111, 1010, 1110,
1000, 1011, 0100, 0111, 1001, 1000, 1010, 1010,
1110, 0101, 1110, 1101, 0001, 0000, 0001, 1111,
0011, 0011, 1001, 0001, 1111, 0110, 1011, 0111,
0011, 0000, 0001, 1010, 1111, 0101, 0100, 1011,
1010, 0111, 1101, 1011, 0000, 0110, 0111, 0001,
0010, 1001, 0110, 1110, 0110, 1110, 1110, 0100,
1000, 0110, 1011, 0000, 0111, 0001, 1011, 1001,
0100, 0011, 1011, 1010, 0000, 1000, 0011, 0101,
1110, 1111, 0111, 1100, 0100, 1111, 1010, 0010,
0011, 1000, 1010, 0010, 0101, 0110, 1101, 0100,
1110, 1000, 1001, 0011, 1110, 1001, 1111, 1110,
1100, 1000, 0111, 1000, 0001, 0100, 1110, 0011,

[図15]

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| 2 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 3 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 |
| 4 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 5 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| 6 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |
| 7 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| 8 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| 9 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 10 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| 11 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 |
| 12 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| 13 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| 14 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 |
| 15 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 |
| 16 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 |
| 17 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 |
| 18 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |
| 19 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 |
| 20 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 21 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| 22 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 |
| 23 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| 24 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 |
| 25 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| 26 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 |
| 27 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |
| 28 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 29 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| 30 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |
| 31 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 |

[図16]

１６進乱数列ｂ

７ＥＤＤ７Ｅ７Ｅ７ＣＤ７ＤＦＤ９１ＡＡ５９ＣＤ３３ＥＤ１１７１８
Ａ９８２Ｄ１５７１４１９１９９ＤＥ３７Ａ９ＢＣ２Ｃ４Ｄ８８Ｄ０２
ＣＢ２０６３５６Ｄ９Ａ６２４Ｆ８５４０３Ｃ８５２５Ａ８２２ＣＢ０
２５９０Ｃ０２０ＣＢＦ７ＢＢＤＦ０２１１２Ｂ９９６６Ｂ７ＣＢＦ８
ＤＣＡＤＢ３４Ｂ１Ｄ９１２Ｄ３０４ＦＥＥ９Ｆ３Ｄ７ＦＦ８Ｄ７ＥＣ
５Ｂ５Ａ５０５２９３ＥＣ１７３２Ｅ０Ｂ１８４５ＡＥ５５Ｂ５７２０
５５ＢＣＥＡ８１２９Ｃ１Ｅ５Ｄ０４３ＡＥ３Ａ３１０７６Ｃ８Ｅ１Ａ
９ＥＢ００６３１２８５３５３Ｄ７０８Ｆ９Ｃ２Ｃ０ＦＦＥＤＣＦ７Ｅ

１６進乱数列ａ

ＥＢ７３５Ｆ８Ｂ７７３９０ＢＡ３４２８ＢＦＦ０１Ｅ８９Ｃ８４Ｅ３
Ｃ５６３Ｃ５５ＢＥＥ３６０Ｅ４１５８Ｅ２７Ｆ９５Ｆ９１２Ａ６３１
Ｄ２６８Ｅ６３２４ＢＢ４１Ｃ７ＦＣ３３５４６ＥＡＡＥ８７９ＡＢ７
８４００２７０９３Ｃ６Ｆ５ＥＡＢＣＢ２Ｂ９Ｅ７６４６０００６ＤＡ
ＤＤ８Ｅ８６３Ｃ１９ＡＣ２６ＣＤ９７５０Ｂ４８Ｄ５ＣＥＦＥＦＡＥ
８Ｂ４７９８ＡＡＥ５ＥＤ１０１Ｆ３３９１Ｆ６Ｂ７３０１ＡＦ５４Ｂ
Ａ７ＤＢ０６７１２９６Ｅ６ＥＥ４８６Ｂ０７１Ｂ９４３ＢＡ０８３５
ＥＦ７Ｃ４ＦＡ２３８Ａ２５６Ｄ４Ｅ８９３Ｅ９ＦＥＣ８７８１４Ｅ３

[図17]

2進乱数列b

01, 11, 11, 10, 11, 01, 11, 01, 01, 11, 11, 10, 01, 11, 11, 10,
01, 11, 11, 00, 11, 01, 01, 11, 11, 01, 11, 11, 11, 01, 10, 01,
00, 01, 10, 10, 10, 10, 01, 01, 10, 01, 11, 00, 11, 01, 00, 11,
00, 11, 11, 10, 11, 01, 00, 01, 00, 01, 01, 11, 00, 01, 10, 00,
10, 10, 10, 01, 10, 00, 00, 10, 11, 01, 00, 01, 01, 01, 01, 11,
00, 01, 01, 00, 00, 01, 10, 01, 00, 01, 10, 01, 10, 01, 11, 01,
11, 10, 00, 11, 01, 11, 10, 10, 10, 01, 10, 11, 11, 00, 00, 10,
11, 00, 01, 00, 11, 01, 10, 00, 10, 00, 11, 01, 00, 00, 00, 10,
11, 00, 10, 11, 00, 10, 00, 00, 01, 10, 00, 11, 01, 01, 01, 10,
11, 01, 10, 01, 10, 10, 01, 10, 00, 10, 01, 00, 11, 11, 10, 00,
01, 01, 01, 00, 00, 00, 00, 11, 11, 00, 10, 00, 01, 01, 00, 10,
01, 01, 10, 10, 10, 00, 00, 10, 00, 10, 11, 00, 10, 11, 00, 00,
00, 10, 01, 01, 10, 01, 00, 00, 11, 00, 00, 00, 00, 10, 00, 00,
11, 00, 10, 11, 11, 11, 01, 11, 10, 11, 10, 11, 11, 01, 11, 11,
00, 00, 00, 10, 00, 01, 00, 01, 00, 10, 10, 11, 10, 01, 10, 01,
01, 10, 01, 10, 10, 11, 01, 11, 11, 00, 10, 11, 11, 11, 10, 00,
11, 01, 11, 00, 10, 10, 11, 01, 10, 11, 00, 11, 01, 00, 10, 11,
00, 01, 11, 01, 10, 01, 00, 01, 00, 10, 11, 01, 00, 11, 00, 00,
01, 00, 11, 11, 11, 10, 11, 10, 10, 01, 11, 11, 00, 11, 11, 01,
01, 11, 11, 11, 11, 11, 10, 00, 11, 01, 01, 11, 11, 10, 11, 00,
01, 01, 10, 11, 01, 01, 10, 10, 01, 01, 00, 00, 01, 01, 00, 10,
10, 01, 00, 11, 11, 10, 11, 00, 00, 01, 01, 11, 00, 11, 00, 10,
11, 10, 00, 00, 10, 11, 00, 01, 10, 00, 01, 00, 01, 01, 10, 10,
11, 10, 01, 01, 01, 01, 10, 11, 01, 01, 01, 11, 00, 10, 00, 00,
01, 01, 01, 01, 10, 11, 11, 00, 11, 10, 10, 10, 10, 00, 00, 01,
00, 10, 10, 01, 11, 00, 00, 01, 11, 10, 01, 01, 11, 01, 00, 00,
01, 00, 00, 11, 10, 10, 11, 10, 00, 11, 10, 10, 00, 11, 00, 01,
00, 00, 01, 11, 01, 10, 11, 00, 10, 00, 11, 10, 00, 01, 10, 10,
10, 01, 11, 10, 10, 11, 00, 00, 00, 00, 01, 10, 00, 11, 00, 01,
00, 10, 10, 00, 01, 01, 00, 11, 01, 01, 00, 11, 11, 01, 01, 11,
00, 00, 10, 00, 11, 11, 10, 01, 11, 00, 00, 10, 11, 00, 00, 00,
11, 11, 11, 11, 11, 10, 11, 01, 11, 00, 11, 11, 01, 11, 11, 10,

2進乱数列a

11, 10, 10, 11, 01, 11, 00, 11, 01, 01, 11, 11, 10, 00, 10, 11,
01, 11, 01, 11, 00, 11, 10, 01, 00, 00, 10, 11, 10, 10, 00, 11,
01, 00, 00, 10, 10, 00, 10, 11, 11, 11, 11, 11, 00, 00, 00, 01,
11, 10, 10, 00, 10, 01, 11, 00, 10, 00, 01, 00, 11, 10, 00, 11,
11, 00, 01, 01, 01, 10, 00, 11, 11, 00, 01, 01, 01, 01, 10, 11,
11, 10, 11, 10, 00, 11, 01, 10, 00, 00, 11, 10, 01, 00, 00, 01,
01, 01, 10, 00, 11, 10, 00, 10, 01, 11, 11, 11, 10, 01, 01, 01,
11, 11, 10, 01, 00, 01, 00, 10, 10, 10, 01, 10, 00, 11, 00, 01,
11, 01, 00, 10, 01, 10, 10, 00, 11, 10, 01, 10, 00, 11, 00, 10,
01, 00, 10, 11, 10, 11, 01, 00, 00, 01, 11, 00, 01, 11, 11, 11,
11, 00, 00, 11, 00, 11, 01, 01, 01, 00, 01, 10, 11, 10, 10, 10,
10, 10, 11, 10, 10, 00, 01, 11, 10, 01, 10, 10, 10, 11, 01, 11,
10, 00, 01, 00, 00, 00, 00, 00, 00, 10, 01, 11, 00, 00, 10, 01,
00, 11, 11, 00, 01, 10, 11, 11, 01, 01, 11, 10, 10, 10, 10, 11,
11, 00, 10, 11, 00, 10, 10, 11, 10, 01, 11, 10, 01, 11, 01, 10,
01, 00, 01, 10, 00, 00, 00, 00, 00, 00, 01, 10, 11, 01, 10, 10,
11, 01, 11, 01, 10, 00, 11, 10, 10, 00, 01, 10, 00, 11, 11, 00,
00, 01, 10, 01, 10, 10, 11, 00, 00, 10, 01, 10, 11, 00, 11, 01,
10, 01, 01, 11, 01, 01, 00, 00, 10, 11, 01, 00, 10, 00, 11, 01,
01, 01, 11, 00, 11, 10, 11, 11, 11, 10, 11, 11, 10, 10, 11, 10,
10, 00, 10, 11, 01, 00, 01, 11, 10, 01, 10, 00, 10, 10, 10, 10,
11, 10, 01, 01, 11, 10, 11, 01, 00, 01, 00, 00, 00, 01, 11, 11,
00, 11, 00, 11, 10, 01, 00, 01, 11, 11, 01, 10, 10, 11, 01, 11,
00, 11, 00, 00, 00, 01, 10, 10, 11, 11, 01, 01, 01, 00, 10, 11,
10, 10, 01, 11, 11, 01, 10, 11, 00, 00, 01, 10, 01, 11, 00, 01,
00, 10, 10, 01, 01, 10, 11, 10, 01, 10, 11, 10, 11, 10, 01, 00,
10, 00, 01, 10, 10, 11, 00, 00, 01, 11, 00, 01, 10, 11, 10, 01,
01, 00, 00, 11, 10, 11, 10, 10, 00, 00, 10, 00, 00, 11, 01, 01,
11, 10, 11, 11, 01, 11, 11, 00, 01, 00, 11, 11, 10, 10, 00, 10,
00, 11, 10, 00, 10, 10, 00, 10, 01, 01, 01, 10, 11, 01, 01, 00,
11, 10, 10, 00, 10, 01, 00, 11, 11, 10, 10, 01, 11, 11, 11, 10,
11, 00, 10, 00, 01, 11, 10, 00, 00, 01, 01, 00, 11, 10, 00, 11,

[図18]

4進乱数列b

R, B, B, G, B, R, B, R, R, B, B, G, R, B, B, G,
R, B, B, 0, B, R, R, B, B, R, B, B, B, R, G, R,
0, R, G, G, G, G, R, R, G, R, B, 0, B, R, 0, B,
0, B, B, G, B, R, 0, R, 0, R, R, B, 0, R, G, 0,
G, G, G, R, G, 0, 0, G, B, R, 0, R, R, R, R, B,
0, R, R, 0, 0, R, G, R, 0, R, G, R, G, R, B, R,
B, G, 0, B, R, B, G, G, G, R, G, B, B, 0, 0, G,
B, 0, R, 0, B, R, G, 0, G, 0, B, R, 0, 0, 0, G,
B, 0, G, B, 0, G, 0, 0, R, G, 0, B, R, R, R, G,
B, R, G, R, G, G, R, G, 0, G, R, 0, B, B, G, 0,
R, R, R, 0, 0, 0, 0, B, B, 0, G, 0, R, R, 0, G,
R, R, G, G, G, 0, 0, G, 0, G, B, 0, G, B, 0, 0,
0, G, R, R, G, R, 0, 0, B, 0, 0, 0, 0, G, 0, 0,
B, 0, G, B, B, B, R, B, G, B, G, B, B, R, B, B,
0, 0, 0, G, 0, R, 0, R, 0, G, G, B, G, R, G, R,
R, G, R, G, G, B, R, B, B, 0, G, B, B, B, G, 0,
B, R, B, 0, G, G, B, R, G, B, 0, B, R, 0, G, B,
0, R, B, R, G, R, 0, R, 0, G, B, R, 0, B, 0, 0,
R, 0, B, B, B, G, B, G, G, R, B, B, 0, B, B, R,
R, B, B, B, B, B, G, 0, B, R, R, B, B, G, B, 0,
R, R, G, B, R, R, G, G, R, R, 0, 0, R, R, 0, G,
G, R, 0, B, B, G, B, 0, 0, R, R, B, 0, B, 0, G,
B, G, 0, 0, G, B, 0, R, G, 0, R, 0, R, R, G, G,
B, G, R, R, R, R, G, B, R, R, R, B, 0, G, 0, 0,
R, R, R, R, G, B, B, 0, B, G, G, G, G, 0, 0, R,
0, G, G, R, B, 0, 0, R, B, G, R, R, B, R, 0, 0,
R, 0, 0, B, G, G, B, G, 0, B, G, G, 0, B, 0, R,
0, 0, R, B, R, G, B, 0, G, 0, B, G, 0, R, G, G,
G, R, B, G, G, B, 0, 0, 0, 0, R, G, 0, B, 0, R,
0, G, G, 0, R, R, 0, B, R, R, 0, B, B, R, R, B,
0, 0, G, 0, B, B, G, R, B, 0, 0, G, B, 0, 0, 0,
B, B, B, B, B, G, B, R, B, 0, B, B, R, B, B, G,

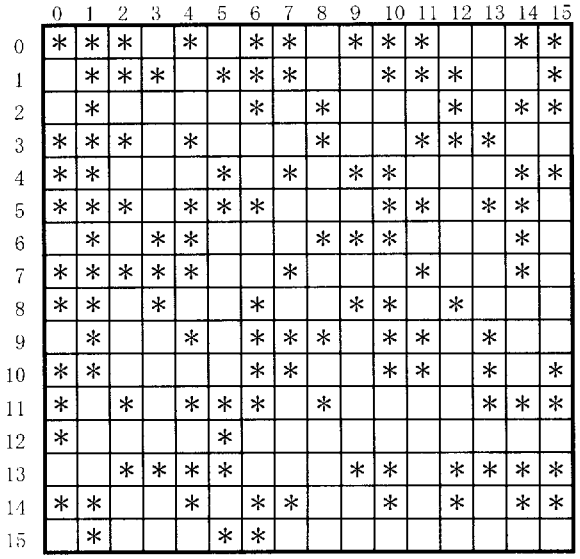
4進乱数列a

B, G, G, B, R, B, 0, B, R, R, B, B, G, 0, G, B,
R, B, R, B, 0, B, G, R, 0, 0, G, B, G, G, 0, B,
R, 0, 0, G, G, 0, G, B, B, B, B, B, 0, 0, 0, R,
B, G, G, 0, G, R, B, 0, G, 0, R, 0, B, G, 0, B,
B, 0, R, R, R, G, 0, B, B, 0, R, R, R, R, G, B,
B, G, B, G, 0, B, R, G, 0, 0, B, G, R, 0, 0, R,
R, R, G, 0, B, G, 0, G, R, B, B, B, G, R, R, R,
B, B, G, R, 0, R, 0, G, G, G, R, G, 0, B, 0, R,
B, R, 0, G, R, G, G, 0, B, G, R, G, 0, B, 0, G,
R, 0, G, B, G, B, R, 0, 0, R, B, 0, R, B, B, B,
B, 0, 0, B, 0, B, R, R, R, 0, R, G, B, G, G, G,
G, G, B, G, G, 0, R, B, G, R, G, G, G, B, R, B,
G, 0, R, 0, 0, 0, 0, 0, 0, G, R, B, 0, 0, G, R,
0, B, B, 0, R, G, B, B, R, R, B, G, G, G, G, B,
B, 0, G, B, 0, G, G, B, G, R, B, G, R, B, R, G,
R, 0, R, G, 0, 0, 0, 0, 0, R, G, B, R, G, G,
B, R, B, R, G, 0, B, G, G, 0, R, G, 0, B, B, 0,
0, R, G, R, G, G, B, 0, 0, G, R, G, B, 0, B, R,
G, R, R, B, R, R, 0, 0, G, B, R, 0, G, 0, B, R,
R, R, B, 0, B, G, B, B, B, G, B, B, G, G, B, G,
G, 0, G, B, R, 0, R, B, G, R, G, 0, G, G, G, G,
B, G, R, R, B, G, B, R, 0, R, 0, 0, 0, R, B, B,
0, B, 0, B, G, R, 0, R, B, B, R, G, G, B, R, B,
0, B, 0, 0, 0, R, G, G, B, B, R, R, R, 0, G, B,
G, G, R, B, B, R, G, B, 0, 0, R, G, R, B, 0, R,
0, G, G, R, R, G, B, G, R, G, B, G, B, G, R, 0,
G, 0, R, G, G, B, 0, 0, R, B, 0, R, G, B, G, R,
R, 0, 0, B, G, B, G, G, 0, 0, G, 0, 0, B, R, R,
B, G, B, B, R, B, B, 0, R, 0, B, B, G, G, 0, G,
0, B, G, 0, G, G, 0, G, R, R, R, G, B, R, R, 0,
B, G, G, 0, G, R, 0, B, B, G, G, R, B, B, B, G,
B, 0, G, 0, R, B, G, 0, 0, R, R, 0, B, G, 0, B,

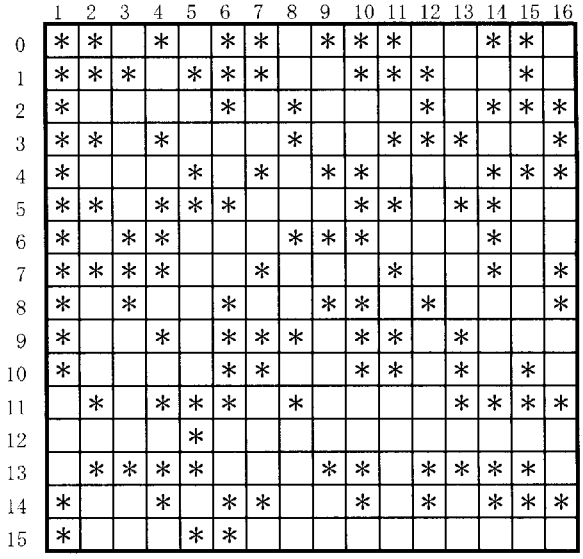
[図19]

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | R | B | B | G | B | R | B | R | R | B | B | G | R | B | B | G | R | B | B | 0 | B | R | R | B | B | R | B | B | B | R | G | R |
| 1 | 0 | R | G | G | G | G | R | R | G | R | B | 0 | B | R | 0 | B | 0 | B | B | G | B | R | 0 | R | 0 | R | R | B | 0 | R | G | 0 |
| 2 | G | G | G | R | G | 0 | 0 | G | B | R | 0 | R | R | R | R | B | 0 | R | R | 0 | 0 | R | G | R | 0 | R | G | R | G | R | B | R |
| 3 | B | G | 0 | B | R | B | G | G | G | R | G | B | B | 0 | 0 | G | B | 0 | R | 0 | B | R | G | 0 | G | 0 | B | R | 0 | 0 | 0 | G |
| 4 | B | 0 | G | B | 0 | G | 0 | 0 | R | G | 0 | B | R | R | R | G | B | R | G | R | G | G | R | G | 0 | G | R | 0 | B | B | G | 0 |
| 5 | R | R | R | 0 | 0 | 0 | 0 | B | B | 0 | G | 0 | R | R | 0 | G | R | R | G | G | G | 0 | 0 | G | 0 | G | B | 0 | G | B | 0 | 0 |
| 6 | 0 | G | R | R | G | R | 0 | 0 | B | 0 | 0 | 0 | 0 | G | 0 | 0 | B | 0 | G | B | B | B | R | B | G | B | G | B | B | R | B | B |
| 7 | 0 | 0 | 0 | G | 0 | R | 0 | R | 0 | G | G | B | G | R | G | R | R | G | R | G | G | B | R | B | B | 0 | G | B | B | B | G | 0 |
| 8 | B | R | B | 0 | G | G | B | R | G | B | 0 | B | R | 0 | G | B | 0 | R | B | R | G | R | 0 | R | 0 | G | B | R | 0 | B | 0 | 0 |
| 9 | R | 0 | B | B | B | G | B | G | G | R | B | B | 0 | B | B | R | R | B | B | B | B | B | G | 0 | B | R | R | B | B | G | B | 0 |
| 10 | R | R | G | B | R | R | G | G | R | R | 0 | 0 | R | R | 0 | G | G | R | 0 | B | B | G | B | 0 | 0 | R | R | B | 0 | B | 0 | G |
| 11 | B | G | 0 | 0 | G | B | 0 | R | G | 0 | R | 0 | R | R | G | G | B | G | R | R | R | R | G | B | R | R | R | B | 0 | G | 0 | 0 |
| 12 | R | R | R | R | G | B | B | 0 | B | G | G | G | G | 0 | 0 | R | 0 | G | G | R | B | 0 | 0 | R | B | G | R | R | B | R | 0 | 0 |
| 13 | R | 0 | 0 | B | G | G | B | G | 0 | B | G | G | 0 | B | 0 | R | 0 | 0 | R | B | R | G | B | 0 | G | 0 | B | G | 0 | R | G | G |
| 14 | G | R | B | G | G | B | 0 | 0 | 0 | 0 | R | G | 0 | B | 0 | R | 0 | G | G | 0 | R | R | 0 | B | R | R | 0 | B | B | R | R | B |
| 15 | 0 | 0 | G | 0 | B | B | G | R | B | 0 | 0 | G | B | 0 | 0 | 0 | B | B | B | B | B | G | B | R | B | 0 | B | B | R | B | B | G |
| 16 | B | G | G | B | R | B | 0 | B | R | R | B | B | G | 0 | G | B | R | B | R | B | 0 | B | G | R | 0 | 0 | G | B | G | G | 0 | B |
| 17 | R | 0 | 0 | G | G | 0 | G | B | B | B | B | B | 0 | 0 | 0 | R | B | G | G | 0 | G | R | B | 0 | G | 0 | R | 0 | B | G | 0 | B |
| 18 | B | 0 | R | R | R | G | 0 | B | B | 0 | R | R | R | R | G | B | B | G | B | G | 0 | B | R | G | 0 | 0 | B | G | R | 0 | 0 | R |
| 19 | R | R | G | 0 | B | G | 0 | G | R | B | B | B | G | R | R | R | B | B | G | R | 0 | R | 0 | G | G | G | R | G | 0 | B | 0 | R |
| 20 | B | R | 0 | G | R | G | G | 0 | B | G | R | G | 0 | B | 0 | G | R | 0 | G | B | G | B | R | 0 | 0 | R | B | 0 | R | B | B | B |
| 21 | B | 0 | 0 | B | 0 | B | R | R | R | 0 | R | G | B | G | G | G | G | G | B | G | G | 0 | R | B | G | R | G | G | G | B | R | B |
| 22 | G | 0 | R | 0 | 0 | 0 | 0 | 0 | 0 | G | R | B | 0 | 0 | G | R | 0 | B | B | 0 | R | G | B | B | R | R | B | G | G | G | G | B |
| 23 | B | 0 | G | B | 0 | G | G | B | G | R | B | G | R | B | R | G | R | 0 | R | G | 0 | 0 | 0 | 0 | 0 | 0 | R | G | B | R | G | G |
| 24 | B | R | B | R | G | 0 | B | G | G | 0 | R | G | 0 | B | B | 0 | 0 | R | G | R | G | G | B | 0 | 0 | G | R | G | B | 0 | B | R |
| 25 | G | R | R | B | R | R | 0 | 0 | G | B | R | 0 | G | 0 | B | R | R | R | B | 0 | B | G | B | B | B | G | B | B | G | G | B | G |
| 26 | G | 0 | G | B | R | 0 | R | B | G | R | G | 0 | G | G | G | G | B | G | R | R | B | G | B | R | 0 | R | 0 | 0 | 0 | R | B | B |
| 27 | 0 | B | 0 | B | G | R | 0 | R | B | B | R | G | G | B | R | B | 0 | B | 0 | 0 | 0 | R | G | G | B | B | R | R | R | 0 | G | B |
| 28 | G | G | R | B | B | R | G | B | 0 | 0 | R | G | R | B | 0 | R | 0 | G | G | R | R | G | B | G | R | G | B | G | B | G | R | 0 |
| 29 | G | 0 | R | G | G | B | 0 | 0 | R | B | 0 | R | G | B | G | R | R | 0 | 0 | B | G | B | G | G | 0 | 0 | G | 0 | 0 | B | R | R |
| 30 | B | G | B | B | R | B | B | 0 | R | 0 | B | B | G | G | 0 | G | 0 | B | G | 0 | G | G | 0 | G | R | R | R | G | B | R | R | 0 |
| 31 | B | G | G | 0 | G | R | 0 | B | B | G | G | R | B | B | B | G | B | 0 | G | 0 | R | B | G | 0 | 0 | R | R | 0 | B | G | 0 | B |

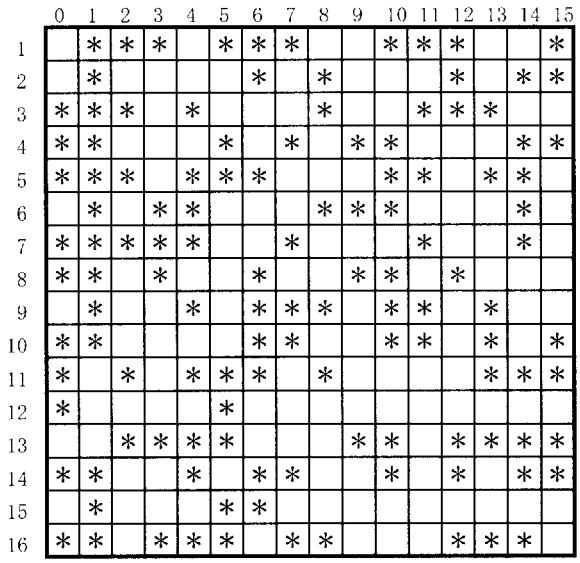
[図20]



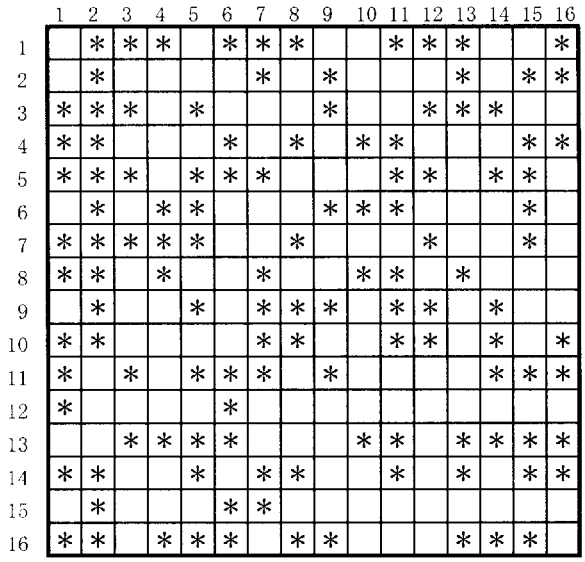
(a)



(b)

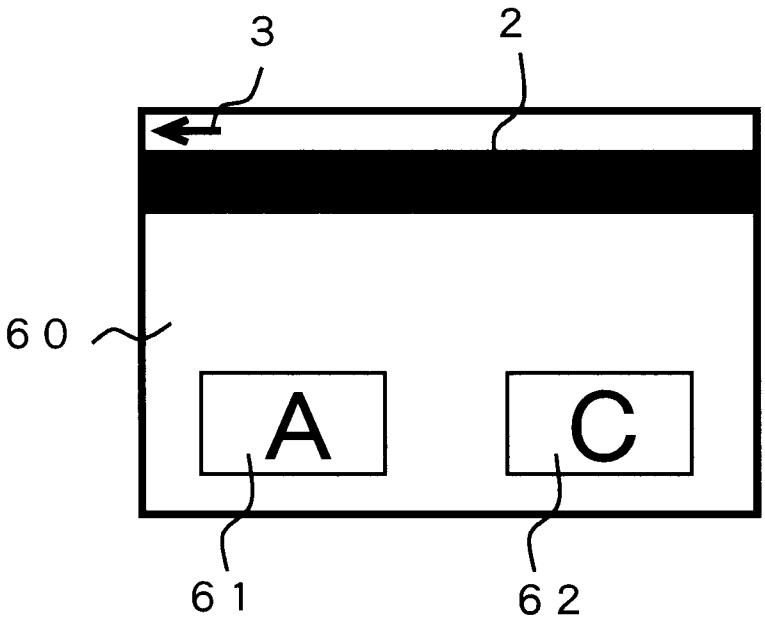


(c)

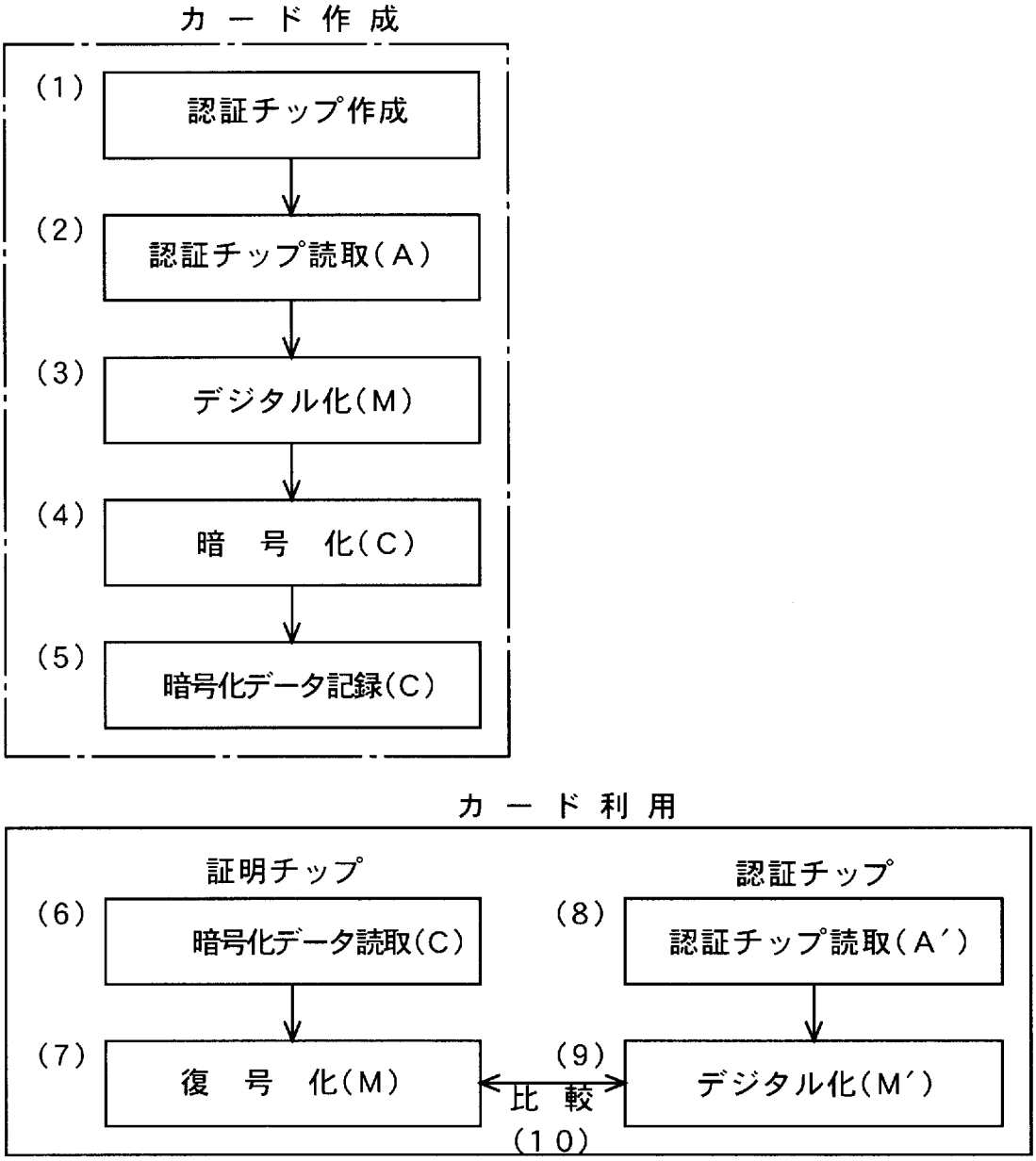


(d)

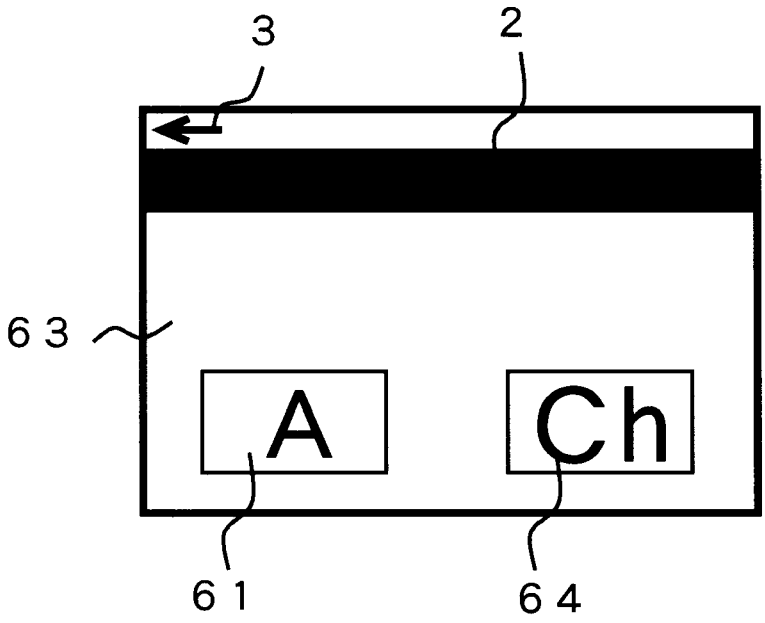
[図21]



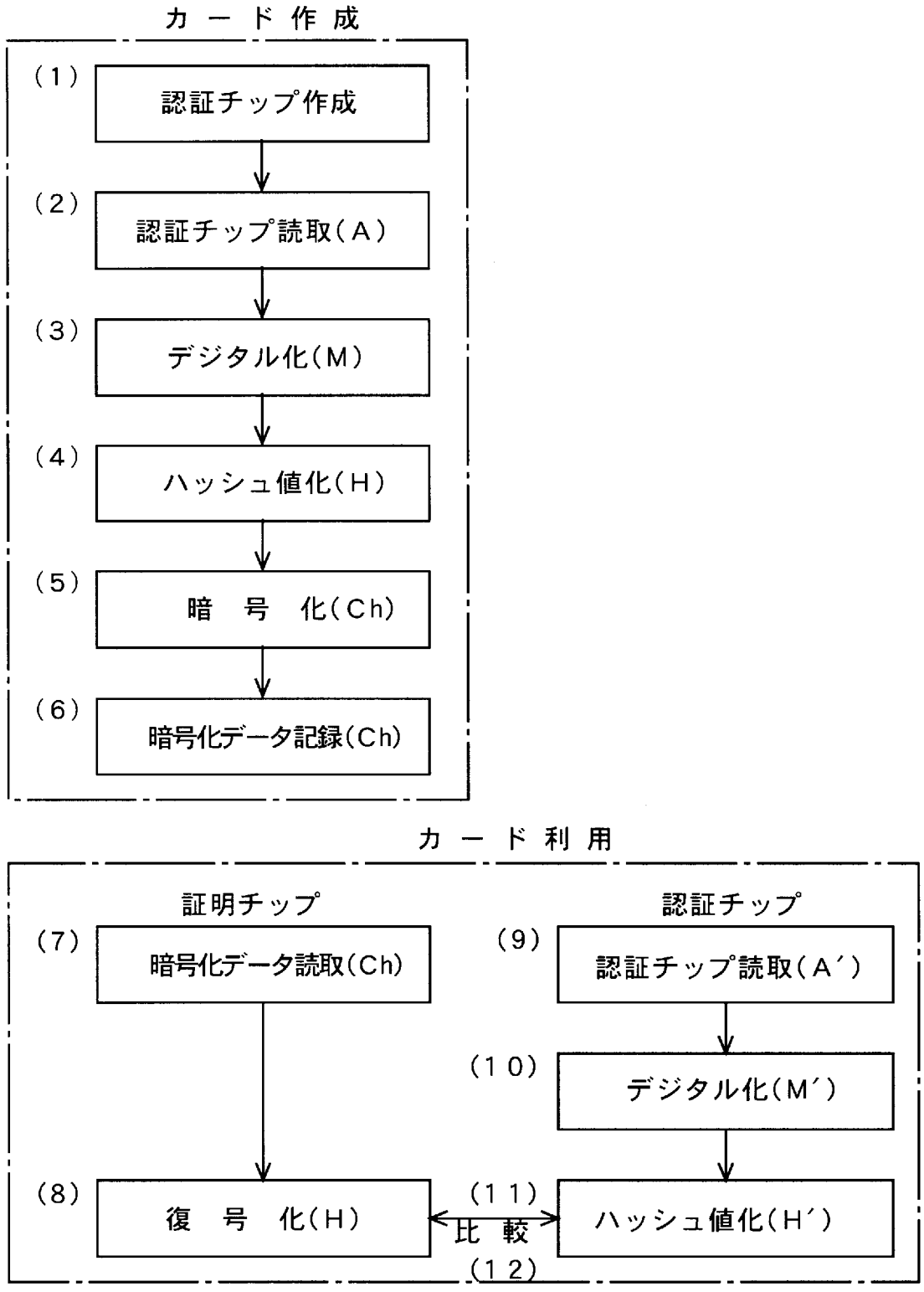
[図22]


カ ー ド 作 成
(1)
認証チップ作成
(2)
認証チップ読取(A)
(3)
デジタル化(M)
(4)
暗 号 化(C)
(5)
暗号化データ記録(C)
カ ー ド 利 用
証明チップ
認証チップ
(6)
暗号化データ読取(C)
(8)
認証チップ読取(A′)
(7)
復 号 化(M)
(9)
デジタル化(M′)
比 較
(10)

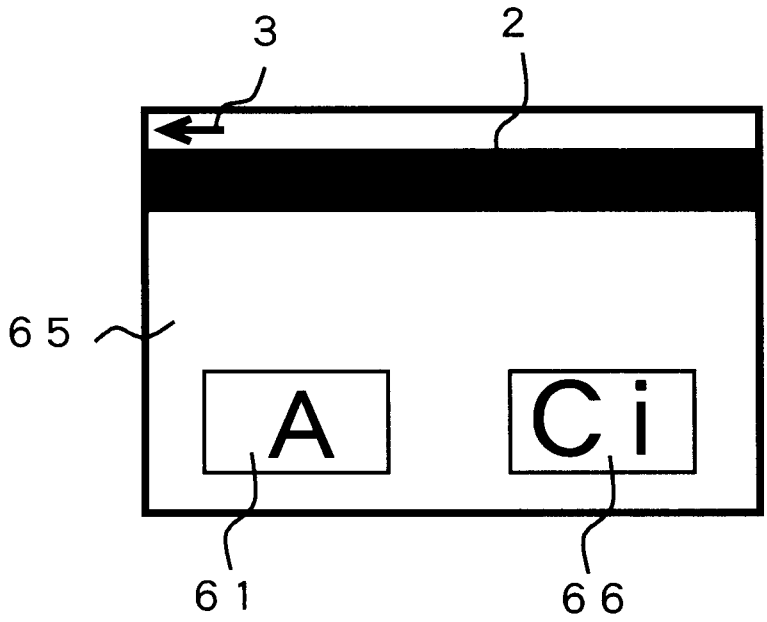
[図23]



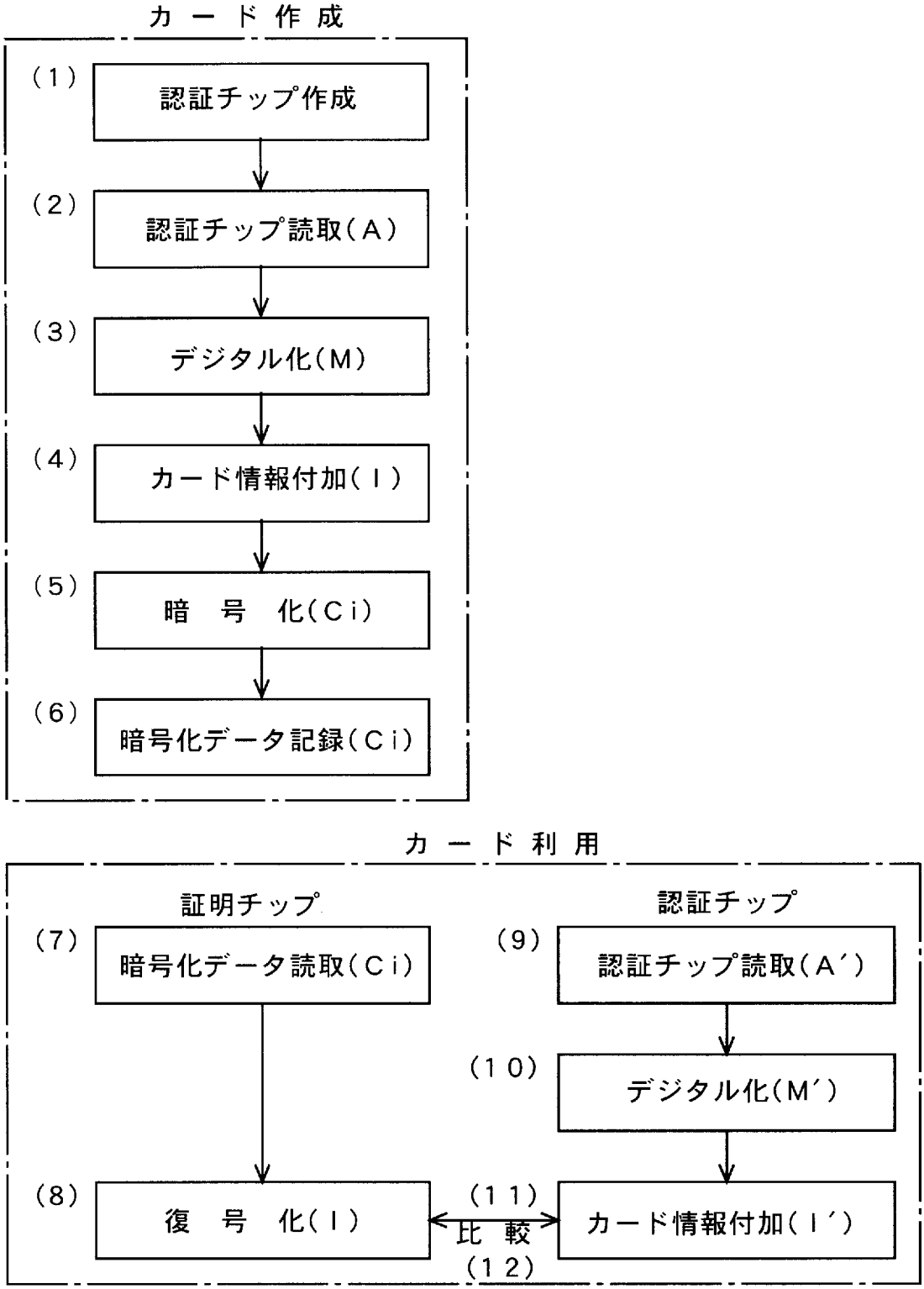
[図24]


カード作成
(1)
認証チップ作成
(2)
認証チップ読取(A)
(3)
デジタル化(M)
(4)
ハッシュ値化(H)
(5)
暗号化(Ch)
(6)
暗号化データ記録(Ch)
カード利用
証明チップ
認証チップ
(7)
暗号化データ読取(Ch)
(9)
認証チップ読取(A´)
(10)
デジタル化(M´)
(8)
復号化(H)
(11)
比較
(12)
ハッシュ値化(H´)

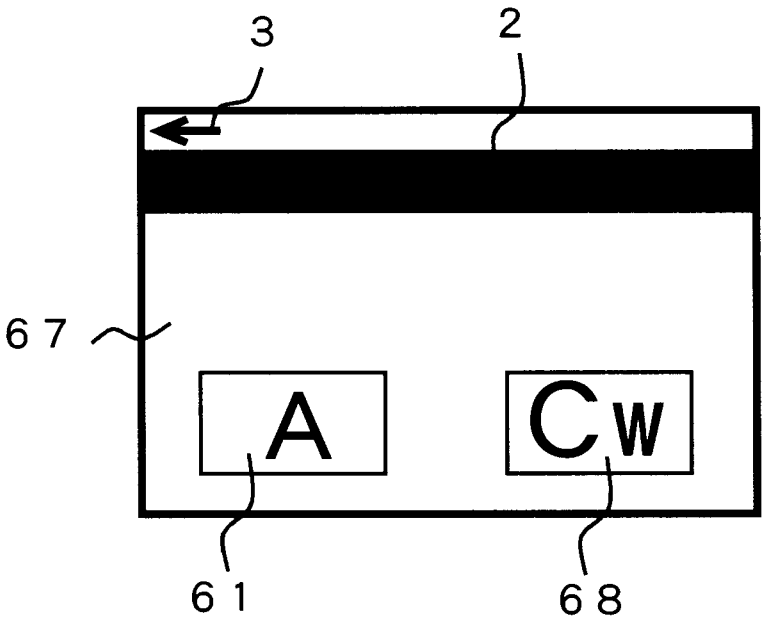
[図25]



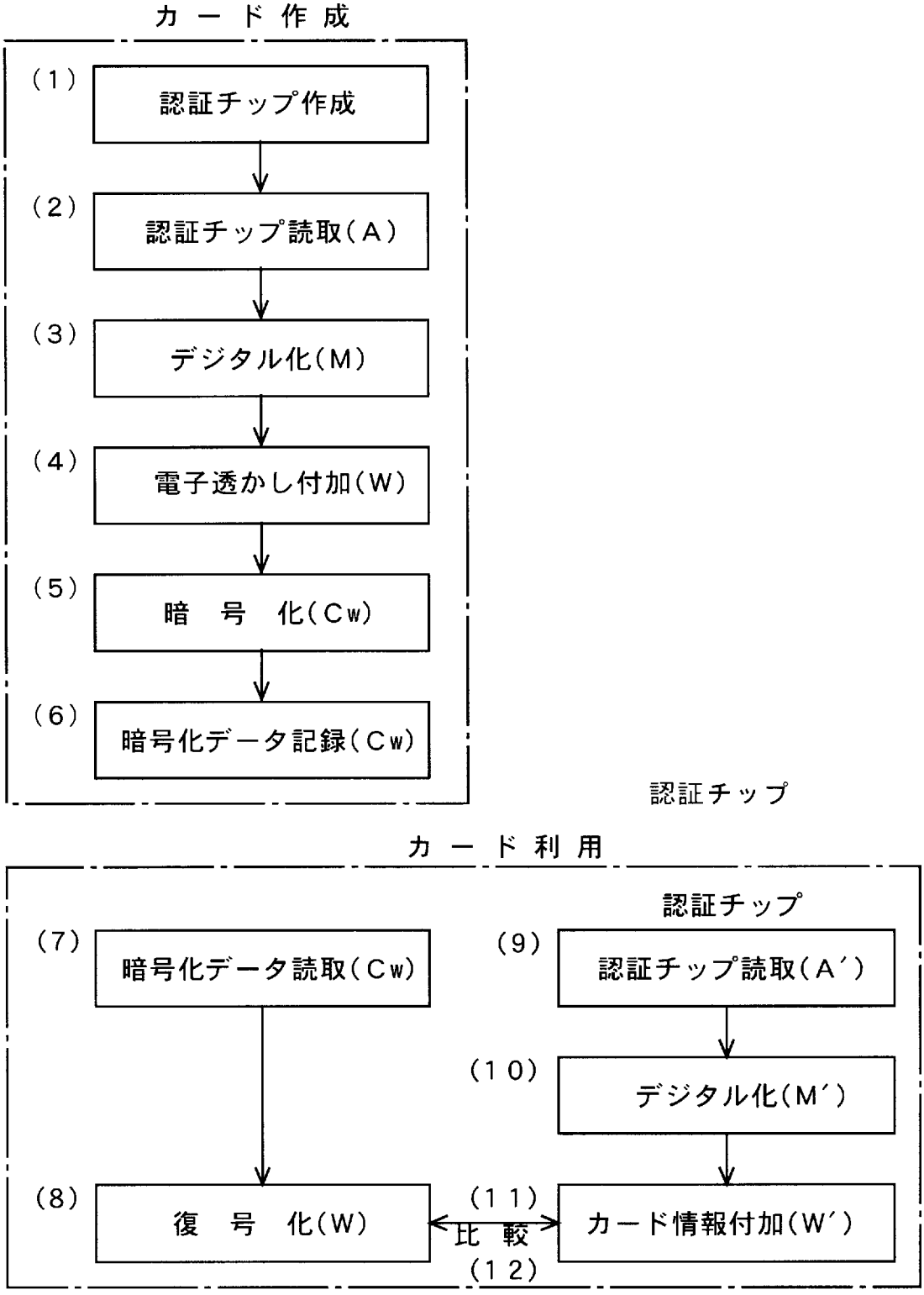
[図26]


カード作成
(1)
認証チップ作成
(2)
認証チップ読取(A)
(3)
デジタル化(M)
(4)
カード情報付加(I)
(5)
暗号化(Ci)
(6)
暗号化データ記録(Ci)
カード利用
証明チップ
認証チップ
(7)
暗号化データ読取(Ci)
(9)
認証チップ読取(A′)
(10)
デジタル化(M′)
(8)
復号化(I)
(11)
比較
(12)
カード情報付加(I′)

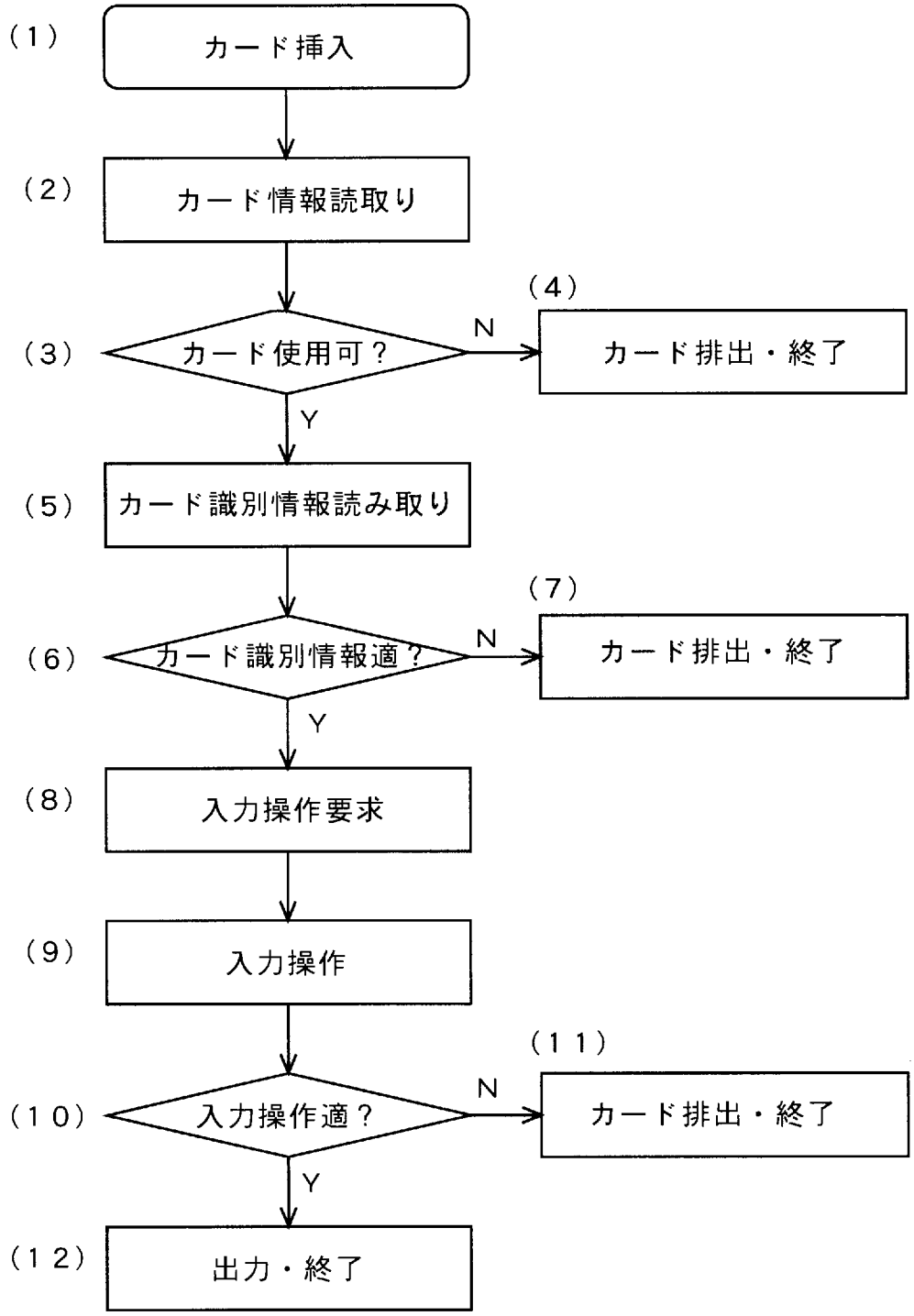
[図27]



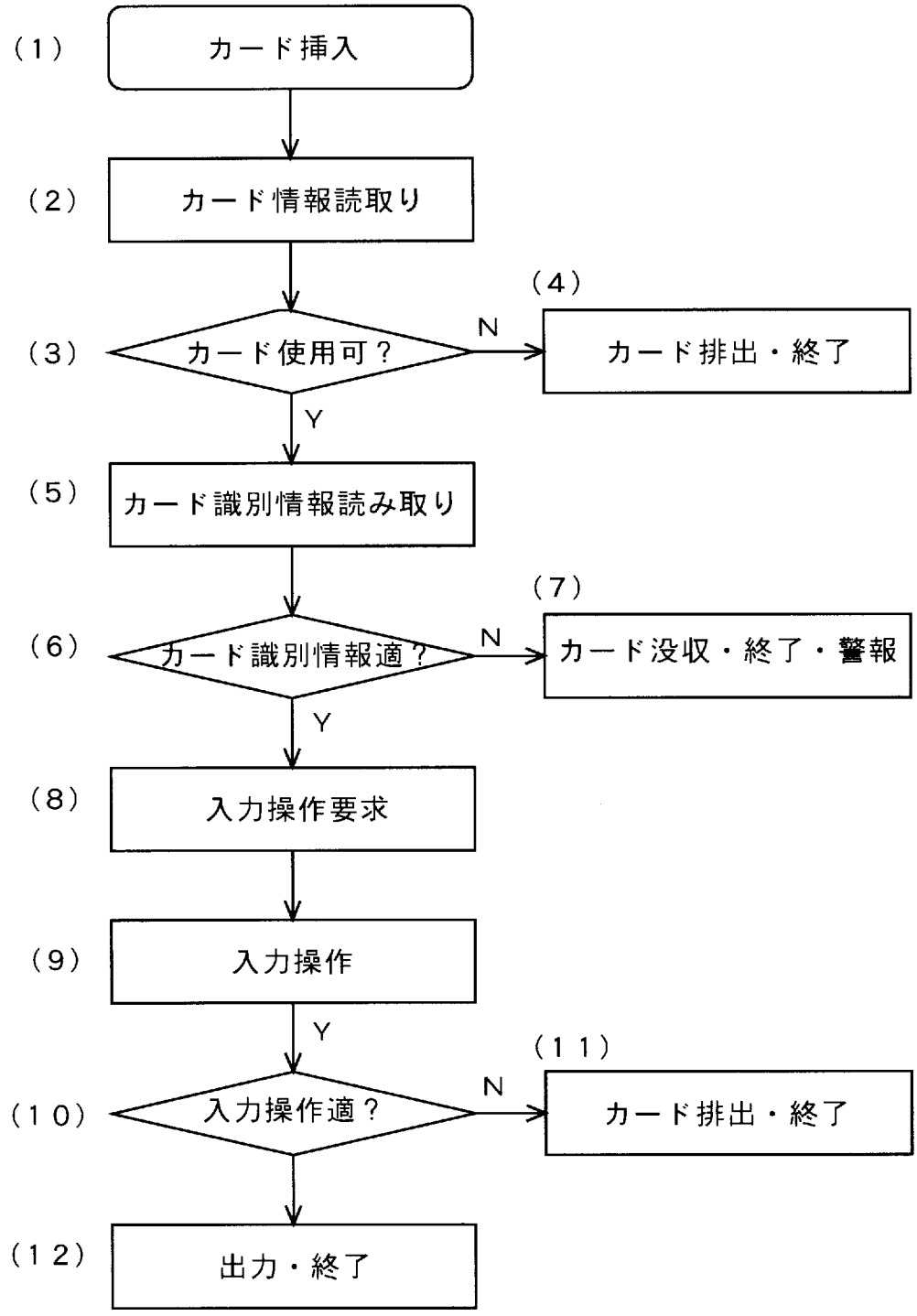
[図28]


カード作成
(1)
認証チップ作成
(2)
認証チップ読取(A)
(3)
デジタル化(M)
(4)
電子透かし付加(W)
(5)
暗号化(Cw)
(6)
暗号化データ記録(Cw)
認証チップ
カード利用
認証チップ
(7)
暗号化データ読取(Cw)
(9)
認証チップ読取(A′)
(10)
デジタル化(M′)
(8)
復号化(W)
(11)
比較
(12)
カード情報付加(W′)

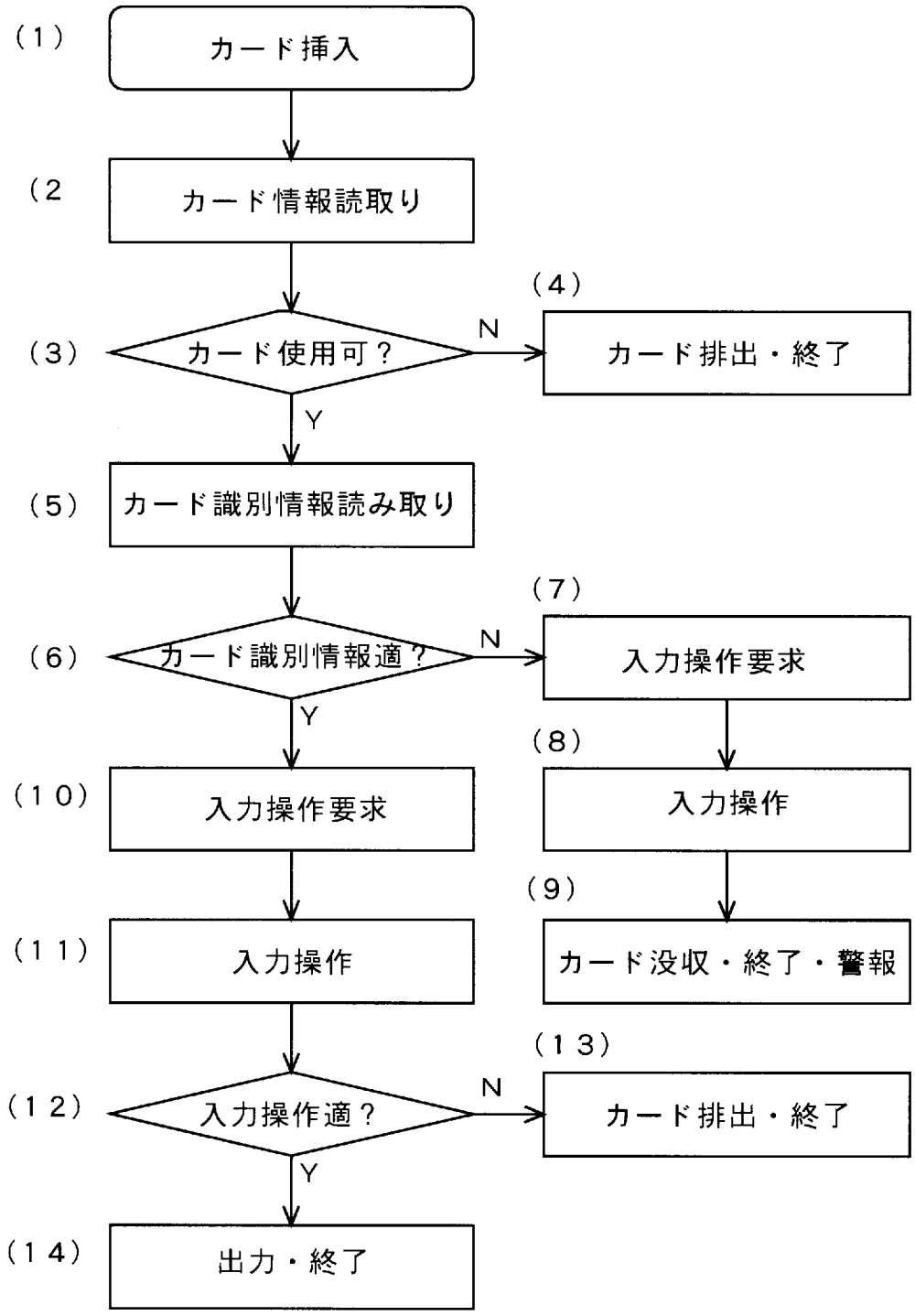
[図29]


(1)
カード挿入
(2)
カード情報読取り
(3)
カード使用可？
N
(4)
カード排出・終了
Y
(5)
カード識別情報読み取り
(6)
カード識別情報適？
N
(7)
カード排出・終了
Y
(8)
入力操作要求
(9)
入力操作
(10)
入力操作適？
N
(11)
カード排出・終了
Y
(12)
出力・終了

[図30]


(1)
カード挿入
(2)
カード情報読取り
(3)
カード使用可？
N
(4)
カード排出・終了
Y
(5)
カード識別情報読み取り
(6)
カード識別情報適？
N
(7)
カード没収・終了・警報
Y
(8)
入力操作要求
(9)
入力操作
Y
(10)
入力操作適？
N
(11)
カード排出・終了
(12)
出力・終了

[図31]


(1)
カード挿入
(2
カード情報読取り
(3)
カード使用可？
N
(4)
カード排出・終了
Y
(5)
カード識別情報読み取り
(6)
カード識別情報適？
N
(7)
入力操作要求
Y
(8)
入力操作
(10)
入力操作要求
(9)
カード没収・終了・警報
(11)
入力操作
(12)
入力操作適？
N
(13)
カード排出・終了
Y
(14)
出力・終了

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/325224

A. CLASSIFICATION OF SUBJECT MATTER
*G06K19/10(2006.01)*i, *B42D15/10*(2006.01)i, *G06F21/20*(2006.01)i, *G06F21/24*(2006.01)i, *G06K17/00*(2006.01)i, *G06K19/06*(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)
G06K19/10, B42D15/10, G06F21/20, G06F21/24, G06K17/00, G06K19/06

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 1996-2007
Kokai Jitsuyo Shinan Koho 1971-2007 Toroku Jitsuyo Shinan Koho 1994-2007

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. |
|---|---|---|
| X<br>Y | JP 10-044650 A (OTAX Co., Ltd.),<br>17 February, 1998 (17.02.98),<br>Full text; all drawings<br>(Family: none) | 1-3<br>30-32 |
| X | JP 2001-022907 A (Oki Electric Industry Co., Ltd.),<br>26 January, 2001 (26.01.01),<br>Full text; all drawings<br>(Family: none) | 1-3 |
| X<br>Y | JP 2004-171109 A (Nippon Telegraph And Telephone Corp.),<br>17 June, 2004 (17.06.04),<br>Full text; all drawings<br>(Family: none) | 1-8,11,12,19-23<br>13-18,24-32 |

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 20 March, 2007 (20.03.07) | 27 March, 2007 (27.03.07) |
| Name and mailing address of the ISA/<br>Japanese Patent Office<br><br>Facsimile No. | Authorized officer<br><br>Telephone No. |

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/325224

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X<br>Y<br>A | JP 06-032091 A (NHK Spring Co., Ltd.),<br>08 February, 1994 (08.02.94),<br>Full text; all drawings<br>& US 5583333 A & EP 0579206 A2 | 1-8,11,12,<br>19-23<br>13-18,24-32<br>9,10 |
| X<br>Y<br>A | JP 10-006673 A (Japan Exlan Co., Ltd.),<br>13 January, 1998 (13.01.98),<br>Full text; all drawings<br>(Family: none) | 1-8, 11, 12,<br>19-23<br>13-18,24-32<br>9,10 |
| X<br>Y<br>A | JP 11-259623 A (Shinsei Kagaku Kogyo Co., Ltd.),<br>24 September, 1999 (24.09.99),<br>Full text; all drawings<br>(Family: none) | 1-8,11,12,<br>19-23<br>13-18,24-32<br>9,10 |
| Y | JP 08-194790 A (Apo Sisutemu Kabushiki Kaisha),<br>30 July, 1996 (30.07.96),<br>Full text; all drawings<br>(Family: none) | 30-32 |
| Y | JP 10-016458 A (Kabushiki Kaisha Micro Denshi System),<br>20 January, 1998 (20.01.98),<br>Full text; all drawings<br>(Family: none) | 30-32 |

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/325224

**Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. [ ] Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. [ ] Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. [ ] Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

**Box No. Ill Observations where unity of invention is lacking (Continuation of item 3 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

This international application includes three groups of inventions which do not satisfy the requirement of unity of invention.
First group of inventions: inventions of claims 1-3
Second group of inventions: inventions of claims 4-29
Third group of inventions: inventions of claims 30-32
There is no technical relationship among the first, the second, and the third group of inventions involving one or more of the same or corresponding special technical features and the inventions do not satisfy the requirement of unity of invention stipulated in PCT Rule 13.1.

1. [X] As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. [ ] As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. [ ] As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. [ ] No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

**Remark on Protest**

the

[X] The additional search fees were accompanied by the applicant's protest and, where applicable, payment of a protest fee..

[ ] The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid withm the time limit specified in the invitation.

[ ] No protest accompanied the payment of additional search fees.

国際調査報告

国際出願番号 PCT／JP2006／325224

A． 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. G06K19/10(2006.01)i, B42D15/10(2006.01)i, G06F21/20(2006.01)i, G06F21/24(2006.01)i, G06K17/00(2006.01)i, G06K19/06(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. G06K19/10, B42D15/10, G06F21/20, G06F21/24, G06K17/00, G06K19/06

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--2007年 |
| 日本国実用新案登録公報 | 1996--2007年 |
| 日本国登録実用新案公報 | 1994--2007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 |
|---|---|---|
| X | JP 10－044650 A（オータックス株式会社） | 1-3 |
| Y | 1998.02.17，全文，全図（ファミリーなし） | 30-32 |
| X | JP 2001－022907 A（沖電気工業株式会社） | 1-3 |
| | 2001.01.26，全文，全図（ファミリーなし） | |
| X | JP 2004-171109 A（日本電信電話株式会社） | 1-8, 11, 12, 19-23 |
| | 2004.06.17，全文，全図（ファミリーなし） | |
| Y | | 13-18, 24-32 |

庄 C欄の続きにも文献が列挙されている。

r 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<br>20.03.2007 | 国際調査報告の発送日<br>27.03.2007 |
| 国際調査機関の名称及びあて先<br>日本国特許庁（ISA／JP）<br>郵便番号100-8915<br>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） 5N 3563<br>村田 充裕<br>電話番号 03－3581-1101 内線 3586 |

様式PCT／ISA／210（第2ページ）（2005年4月）

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 | 関連する請求の範囲の番号 |
|---|---|---|
| X<br>Y<br>A | JP 06-032091 A (日本発条株式会社)<br>1994.02.08, 全文, 全図<br>& US 5583333 A & EP 0579206 A2 | 1-8, 11, 12, 19-23<br>13-18, 24-32<br>9, 10 |
| X<br>Y<br>A | JP 10-006673 A (日本エクスラン工業株式会社)<br>1998.01.13, 全文, 全図 (ファミリーなし) | 1-8, 11, 12, 19-23<br>13-18, 24-32<br>9, 10 |
| X<br>Y<br>A | JP 11-259623 A (新生化学工業株式会社)<br>1999.09.24, 全文, 全図 (ファミリーなし) | 1-8, 11, 12, 19-23<br>13-18, 24-32<br>9, 10 |
| Y | JP 08-194790 A (アポシステム株式会社)<br>1996.07.30, 全文, 全図 (ファミリーなし) | 30-32 |
| Y | JP 10-016458 A (株式会社ミクロ電子システム)<br>1998.01.20, 全文, 全図 (ファミリーなし) | 30-32 |

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００６ノ３２５２２４

第π欄　請求の範囲の一部の調査かてきないときの青見（第１ペーy の２の続き）

怯第8条第3項（ＰＣＴ17条 (2) (a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

１．　汀　請求の範囲＿＿＿＿＿＿＿＿　は、この国際調査機関か調査をすることを要しない対象に係るものてある。
つまり、

２．　汀　請求の範囲＿＿＿＿＿＿＿＿　は、有青義な国際調査をすることかてきる程度まて所定の要件を備たしていない国際出願の部分に係るものてある。つまり、

３．　汀　請求の範囲＿＿＿＿＿＿＿＿　は、従属請求の範囲てあってＰＣＴ規則6.4(a) の第２文及ひ第3文の規定に従って記載されていない。

第m欄　発明の単一性か欠如しているときの青見（第Ｉペーノの３の続き）

次に述へるようにこの国際出願に二以上の発明かあるとこの国際調査機関は認めた。

この回際出願は、発明の単一性の要件を満たさない３つの発明を含む。
発明群１：請求の範囲１～３に係る発明
発明群２：請求の範囲４～２９に係る発明
発明群３：請求の範囲３０～３２に係る発明

発明群１、２、３の間に同一又は対応する特別な技術的特徴が存在するというこt はできず、上記３組の請求の範囲に係る発明は、特許協力条約に某づく規則１３．１に規定する発明の単一性の要件を満たすものではない。

１．河　出願人か必要な追加調査手数科をすへて期間内に納付したので、この国際調査報告は、すへての調査可能な請求の範囲について作成した。

２．r　追加調査手数科を要求するまてもなく、すへての調査可能な請求の範囲について調査することかてきたので、追加調査手数科の納付を求めなかった。

３．亡　出願人か必要な追加調査手数科を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数科の納付のあった次の請求の範囲のみについて作成した。

４．口　出願人か必要な追加調査手数科を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数科の異議の中立てに関する住青

汀　追加調査手数科及ひ、該当する場合には、異議申立手数科の納付と共に、出願人から異議申立てかあった。

汀　追加調査手数科の納付と共に出願人から異議申立てかあったか、異議申立手数科か納付命令書に示した期間内に支払われなかった。

r　追加調査手数科の納付を伴う異議申立てかなかった。