(19)日本国特許庁(JP)

# (12)特許公報(B2)

(11)特許番号
特許第7706455号
(P7706455)

(45)発行日　令和7年7月11日(2025.7.11)

(24)登録日　令和7年7月3日(2025.7.3)

| (51)国際特許分類 | | | FI | | |
|---|---|---|---|---|---|
| *H04L* | *9/32* | *(2006.01)* | H04L | 9/32 | 100E |
| *G06F* | *21/31* | *(2013.01)* | G06F | 21/31 | |
| *G06F* | *21/33* | *(2013.01)* | G06F | 21/33 | |

請求項の数　15　（全25頁）

(21)出願番号　特願2022-538157(P2022-538157)
(86)(22)出願日　令和2年11月23日(2020.11.23)
(65)公表番号　特表2023-508317(P2023-508317A)
(43)公表日　令和5年3月2日(2023.3.2)
(86)国際出願番号　PCT/US2020/061864
(87)国際公開番号　WO2021/133494
(87)国際公開日　令和3年7月1日(2021.7.1)
審査請求日　令和5年11月21日(2023.11.21)
(31)優先権主張番号　16/725,133
(32)優先日　令和1年12月23日(2019.12.23)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　519111877
キャピタル・ワン・サービシーズ・リミテッド・ライアビリティ・カンパニー
Ｃａｐｉｔａｌ Ｏｎｅ Ｓｅｒｖｉｃｅｓ，ＬＬＣ
アメリカ合衆国２２１０２バージニア州マクリーン、キャピタル・ワン・ドライブ１６８０番
(74)代理人　100145403
弁理士　山尾 憲人
(74)代理人　100135703
弁理士　岡部 英隆
(74)代理人　100221556
弁理士　金田 隆章
(72)発明者　オズボーン，ケビン

最終頁に続く

(54)【発明の名称】　非接触カード個人識別システム

(57)【特許請求の範囲】

【請求項１】

入力装置と、

非接触インタフェースと、

プロセッサと、

前記非接触インタフェース及び前記入力装置に結合されたメモリと、

を備えるコンピューティングデバイスであって、

前記メモリは、命令を格納するように構成され、

前記命令は、前記プロセッサによって実行されたときに、

前記非接触インタフェースを介して、非接触カードから、取引を実行するための暗号を受信し、

前記入力装置を介して、入力された個人識別番号（ＰＩＮ）を受信する、

ように動作可能であり、

前記暗号は、前記非接触カードの動的鍵を用いて形成され、

前記動的鍵は、前記非接触カードによって保持されたカウンタ値を用いて形成され、

前記暗号は、前記カウンタ値と、前記動的鍵を用いて符号化された非接触カードデータとを含み、

前記命令は、前記プロセッサによって実行されたときに、更に、

前記プロセッサによって、前記暗号と前記ＰＩＮとを暗号化し、

少なくとも前記暗号を使用して、前記カウンタ値と前記非接触カードデータと前記Ｐ

ＩＮとを認証することを含む認証動作を実行し、前記取引が認証されているか認証されていないかに関する指示を含む認証応答を生成するように構成されたサーバに、前記暗号化された暗号と前記ＰＩＮとを送信し、
前記認証応答を、前記サーバから受信し、
前記指示が、前記取引が認証されていることを示す場合、前記取引を可能にし、
前記指示が、前記取引が認証されていないことを示す場合、前記取引を阻止するように動作可能である、
コンピューティングデバイス。
【請求項２】
前記命令は、さらに、前記プロセッサに、前記暗号を要求するために前記非接触カードとの近距離無線通信（ＮＦＣ）交換を開始させるように構成された、請求項１に記載のコンピューティングデバイス。
【請求項３】
前記暗号は、前記非接触カードに関連付けられたユーザを識別するための識別情報を含む、請求項１に記載のコンピューティングデバイス。
【請求項４】
前記命令は、さらに、前記プロセッサに、前記ＰＩＮ、前記暗号、又はこれらの両方を暗号化して前記サーバに送信するように構成された、請求項１に記載のコンピューティングデバイス。
【請求項５】
前記ＰＩＮ、前記暗号、又はこれらの両方を暗号化するために、対称暗号化アルゴリズムが使用される、請求項４に記載のコンピューティングデバイス。
【請求項６】
前記非接触インタフェースは、近距離無線通信（ＮＦＣ）インタフェースを含む、請求項１に記載のコンピューティングデバイス。
【請求項７】
前記命令は、さらに、前記入力装置を介して前記ＰＩＮを提供することをユーザに促すプロンプトを出力するように構成される、請求項１に記載のコンピューティングデバイス。
【請求項８】
前記コンピューティングデバイスは、モバイル装置又は加盟店取引装置である、請求項１に記載のコンピューティングデバイス。
【請求項９】
コンピュータで実現する方法であって、
非接触インタフェースを介して、非接触カードから、取引を実行するための暗号を受信するステップと、
入力装置を介して、入力された個人識別番号（ＰＩＮ）を受信するステップと、を含み、
前記暗号は、前記非接触カードの動的鍵を用いて形成され、
前記動的鍵は、前記非接触カードによって保持されたカウンタ値を用いて形成され、
前記暗号は、前記カウンタ値と、前記動的鍵を用いて符号化された非接触カードデータとを含み、
前記方法は、更に、
プロセッサによって、前記暗号と前記ＰＩＮとを暗号化するステップと、
少なくとも前記暗号を使用して、前記カウンタ値と前記非接触カードデータと前記ＰＩＮとを認証することを含む認証動作を実行し、前記取引が認証されているか認証されていないかに関する指示を含む認証応答を生成するように構成されたサーバに、ネットワークインタフェースを介して、前記暗号化された暗号と前記ＰＩＮとを送信するステップと、
前記ネットワークインタフェースによって、前記認証応答を、前記サーバから受信するステップと、
前記指示が、前記取引が認証されていることを示す場合、前記取引を可能にするステップと、

前記指示が、前記取引が認証されていないことを示す場合、前記取引を阻止するステップと、
を含む方法。
【請求項１０】
前記非接触カードとの近距離無線通信（ＮＦＣ）交換を開始して前記暗号を要求する、請求項９に記載の方法。
【請求項１１】
前記暗号は、前記非接触カードに関連付けられたユーザを識別するための識別情報を含む、請求項９に記載の方法。
【請求項１２】
前記ＰＩＮ、前記暗号、又はこれらの両方を暗号化して前記サーバに送信するステップを含む、請求項９に記載の方法。
【請求項１３】
前記ＰＩＮ、前記暗号、又はこれらの両方を暗号化するために、対称暗号化アルゴリズムが使用される、請求項１２に記載の方法。
【請求項１４】
前記非接触インタフェースは、近距離無線通信（ＮＦＣ）インタフェースを含む、請求項９に記載の方法。
【請求項１５】
前記入力装置を介して前記ＰＩＮを提供することをユーザに促すステップを更に含む、請求項９に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本出願は、２０１９年１２月２３日に出願された、「非接触カード個人識別システム」と題する米国特許出願第１６／７２５，１３３号に対する優先権を主張する。上記出願の内容は、その全体が参照により本明細書に援用される。
【背景技術】
【０００２】
クレジットカードのクローニング、又は「スキミング」は、悪意のある行為者が、ある口座に関連するクレジットカードから偽造カードにクレジットカード情報を複写する技術である。クローニングは、典型的には、クレジットカードをスキマに通してカードの磁気ストライプからクレジットカード情報を抽出（「スキム」）し、その情報を偽造カードに保存することによって行われる。偽造カードは、口座に対する請求に使用され得る。
【０００３】
ＥＭＶ（由来はEuropay, Mastercard, Visa）は、スマート支払カード、並びにそれらを受け入れる端末及び自動預払機を使用するための規格を規定する。
【０００４】
ＥＭＶカードは、（後方互換性のため）磁気ストライプ情報に加えてカード情報を保存するように構成された集積回路を含むスマートカード（すなわち、チップカード又はＩＣ（集積回路）カード）である。ＥＭＶカードは、読取機に物理的に挿入される（又は「ディップされる」）カード、及び近距離無線通信（ＮＦＣ）技術を使用して短距離を越えて読み取られ得る非接触カードの両方を含む。
【０００５】
いくつかのＥＭＶカードは、クローニングに関連する問題を克服するために、チップ及びＰＩＮ（個人識別番号）技術を使用する。例えば、取引を許可するために、ユーザは、カードスワイプに続いて、取引端末で個人識別番号（ＰＩＮ）を入力してもよい。取引端末によってカードから取得され、保存されたＰＩＮは、ＰＩＮ入力と比較され、両者が一致した場合にのみ取引が承認される。このようなソリューションは、不正行為を低減し得るが、傍受、中間者、又は他のタイプの攻撃によって引き起こされるＰＩＮの盗聴に対し

て脆弱であることに変わりはない。
【発明の概要】
【０００６】
本発明の一態様によれば、多要素認証システム、装置及び方法は、個人識別番号（ＰＩＮ）検証手順を非接触カード認証プロセスと組み合わせて、カードクローニングによる損失の可能性を低減させる。
【０００７】
一態様によれば、クライアントに関連するアカウントへのアクセスについての要求に対する二要素認証のための方法は、ユーザインタフェースから入力ＰＩＮを受信するステップと、クライアントに関連するＰＩＮを記憶する非接触カードを嵌め込むステップと、入力ＰＩＮを非接触カードに送信するステップと、入力ＰＩＮと記憶されたＰＩＮとが一致すると、非接触カードから暗号を受信するステップと、暗号を認証装置に送信するステップと、認証装置によって暗号が認証されると要求を許可するステップと、を含み、暗号は、非接触カードの動的鍵を用いて形成され、動的鍵は、非接触カードによって保持されるカウンタ値を用いて形成され、暗号は、動的鍵を用いて符号化された非接触カードのデータを含む。
【０００８】
他の態様によれば、クライアントに関連するアカウントへのアクセスについての要求に対する二要素認証のための方法は、ユーザインタフェースから入力ＰＩＮを受信するステップを含む。本方法は、クライアントに関連するＰＩＮを記憶する非接触カードを嵌め込むステップを更に含む。本方法は、非接触カードから暗号を受信するステップを更に含み、暗号は、非接触カードの動的鍵を用いて形成され、動的鍵は、非接触カードによって保持されるカウンタを用いて形成され、暗号は、ＰＩＮを含む非接触カードのデータを含み、動的鍵を用いて符号化される。本方法は、入力ＰＩＮ及び暗号を認証装置に送信するステップを更に含む。本方法は、認証装置によって入力ＰＩＮ及び暗号が認証されると要求を許可するステップを更に含む。
【０００９】
更なる態様によれば、装置は、クライアントに関連する非接触カードと通信するように構成された非接触カードインタフェースと、ユーザインタフェースと、プロセッサと、クライアントによる要求を認証するための記憶されたプログラムコードを有する不揮発性メモリとを含む。プログラムコードは、プロセッサによって実行されたときに、ユーザインタフェースによって受信された入力ＰＩＮを非接触カードに送信し、入力ＰＩＮと記憶されたＰＩＮとが一致すると、非接触カードから暗号を受信するように動作可能である。暗号は、非接触カードの動的鍵を用いて形成され、動的鍵は、非接触カードによって保持されるカウンタ値を用いて形成され、暗号は、動的鍵を用いて符号化された非接触カードのデータを含む。プログラムコードは、更に、暗号を認証装置に送信し、認証装置によって暗号が認証されると要求を許可するように動作可能であってもよい。
【図面の簡単な説明】
【００１０】
【図１Ａ】例示的な実施形態に係る、個人識別番号（ＰＩＮ）を用いて顧客の要求の多要素認証を提供するように構成されたデータ送信システムのブロック図である。
【図１Ｂ】非接触カードに記憶されたデータを使用して認証されたアクセスを提供するためのシーケンスの一実施形態を示すデータフロー図である。
【図２Ａ】本明細書に開示される二要素ＰＩＮに基づく認証のためのシステム及び方法の一実施形態を示す。
【図２Ｂ】本明細書に開示される二要素ＰＩＮに基づく認証のためのシステム及び方法の一実施形態を示す。
【図３Ａ】本明細書に開示される二要素ＰＩＮに基づく認証のためのシステム及び方法の代替的な実施形態を示す。
【図３Ｂ】本明細書に開示される二要素ＰＩＮに基づく認証のためのシステム及び方法の

代替的な実施形態を示す。
【図４Ａ】本明細書に開示される二要素ＰＩＮに基づく認証のためのシステム及び方法の代替的な実施形態を示す。
【図４Ｂ】本明細書に開示される二要素ＰＩＮに基づく認証のためのシステム及び方法の代替的な実施形態を示す。
【図５Ａ】本明細書に開示される二要素ＰＩＮに基づく認証のためのシステム及び方法の代替的な実施形態を示す。
【図５Ｂ】本明細書に開示される二要素ＰＩＮに基づく認証のためのシステム及び方法の代替的な実施形態を示す。
【図６】図１Ａのシステムにおいて使用され得る認証情報を記憶するための非接触カードの一例である。
【図７】図３の非接触カードに含まれ得る例示的な構成要素を示すブロック図である。
【図８】本明細書の様々な実施形態において開示されるようなＰＩＮ交換の一部として使用され得る暗号の例示的な領域を示す図である。
【図９】本発明の態様をサポートするために利用され得る図１Ａのシステムの構成要素の詳細なブロック図である。
【図１０】本明細書において開示される一実施形態に係るクライアント装置のユーザインタフェースによって提供され得るプロンプトを示す。
【発明を実施するための形態】
【００１１】
データのセキュリティとトランザクションの完全性は、企業及び消費者にとって極めて重要である。電子取引が商業活動のますます大きな割合を構成し、悪意のある行為者が取引セキュリティを侵害しようとますます積極的になるにつれて、この必要性は増大し続ける。
【００１２】
本開示の実施形態は、非接触カードと組み合わせて個人識別番号（ＰＩＮ）を使用してクライアント装置で受信したトランザクションの多要素認証のためのシステム、方法及び装置を提供する。
【００１３】
非接触カードは、１以上のアプレット、カウンタ値、及び１以上の鍵を記憶するメモリを含む基板を含んでもよい。いくつかの実施形態では、本明細書に記載されるように、メモリは、非接触カードの使用を制御するＰＩＮを更に記憶してもよい。一実施形態では、カウンタ値は、非接触カード取引の認証に使用され得る固有の暗号を生成するために使用されてもよい。暗号は、非接触カード取引の二要素認証を提供するために、ＰＩＮと共に使用される場合がある。
【００１４】
暗号は、Osbornらによって２０１８年１１月２９日に出願され、援用によって本明細書に組み込まれる「Systems and Methods for Cryptographic Authentication of Contactless Cards」と題する米国特許出願シリアルナンバー１６／２０５，１１９（以下「’１１９出願」という。）に記載されているように形成されてよい。いくつかの実施形態において、暗号は、共有秘密、複数の鍵、及びカウンタ値の暗号ハッシュから形成されてもよい。
【００１５】
一態様によれば、暗号はＰＩＮと共に使用され、非接触カード取引の多要素認証を提供してもよい。多要素認証は、暗号を使用する取引の認証の前に、又はその一部として、カードのＰＩＮに関するユーザの知識を検証することを含む場合がある。いくつかの実施形態では、暗号は、ＰＩＮを使用して形成されてもよい。いくつかの実施形態では、暗号は、符号化されたＰＩＮを含んでもよい。いずれの場合も、ＰＩＮが識別可能な形式で送信されることがないため、取引のセキュリティが維持され、したがって、盗難の可能性が低減される。二要素認証のためにＰＩＮを暗号と共に使用するこのような措置は、無許可の

第三者による非接触カードのクローニングに対する保護機能を有する。

【００１６】

いくつかの実施形態では、ＰＩＮ検証は、暗号生成の前提条件として、カードによって実行されてもよい。他の実施形態では、ＰＩＮ検証は、暗号認証の一部として、取引装置又はバックエンド認証サーバによって実行されてもよい。以下、これらの方法の各々をより詳細に説明する。

【００１７】

当然、様々な実施形態のクライアント、クライアント装置、及び認証サーバを含む様々なシステムにおいて、ＰＩＮストレージ、暗号化、及び認証の機能は、様々な構成要素によって実行されてもよい。いくつかの実施形態では、ＰＩＮのコピーは、非接触カードのメモリに保持されてもよい。そのような実施形態では、ＰＩＮのコピーは、暗号認証プロセスの一部として非接触カードのユーザを検証するために使用されてもよい。いくつかの実施形態では、ＰＩＮは、デジタル署名又は暗号を生成するために使用されてもよい。いくつかの実施形態では、暗号認証は、取引装置、認証サーバ、又はそれらのいくつかの組合せによって実行されてもよい。

【００１８】

このように、本システムは、知識（すなわち、ＰＩＮ番号）及び所有（すなわち、非接触カード及び動的鍵）の両方を確立する二要素認証を提供し、悪意ある行為者の、非接触カードを首尾よく複製する能力を低減することができる。

【００１９】

次に、本発明のこれらの特徴及び他の特徴を図面を参照して説明する。ここで、同様の参照数字は、全体を通して同様の要素を参照するために使用される。本明細書において使用される表記及び命名法を一般的に参照すると、以下に続く詳細な説明は、コンピュータ又はコンピュータのネットワーク上で実行されるプログラムプロセスの観点から提示され得る。これらのプロセスの説明及び表現は、その仕事の内容を当業者に最も効果的に伝達するために、当業者によって使用される。

【００２０】

プロセスは、ここでは、そして一般的には、所望の結果をもたらす自己矛盾のない操作のシーケンスであると考えられる。これらの操作は、物理的な量の物理的な操作を要求する。通常、もっとも必ずしもそうではないが、これらの量は、記憶、送信、結合、比較、及び他の操作を行うことができる電気、磁気、又は光学信号の形態をとる。主に一般的な使用上の理由から、これらの信号をビット、値、要素、記号、文字、用語、数などと呼ぶことが時に便利であることがわかる。しかし、これらの用語及び類似の用語の全ては、適切な物理量と関連付けられるべきであり、それらの量に適用される便宜的なラベルに過ぎないことに留意すべきである。

【００２１】

さらに、実行される操作は、しばしば、人間の操作者によって実行される精神的操作に一般的に関連付けられる、加算又は比較などの用語で呼ばれる。１以上の実施形態の一部を形成する本明細書に記載された操作のいずれにおいても、ほとんどの場合、人間の操作者のそのような能力は必要でなく望ましくもない。むしろ、この操作は機械操作である。様々な実施形態の操作を実行するための有用な機械は、汎用デジタルコンピュータ又は同様の装置を含む。

【００２２】

様々な実施形態はまた、これらの操作を実行するための装置又はシステムに関する。この装置は、必要な目的のために特別に構成されてもよく、又は、コンピュータの中に記憶されたコンピュータプログラムによって選択的に起動され又は再構成されるように汎用コンピュータを含んでもよい。本明細書に示されるプロセスは、特定のコンピュータ又は他の装置と本質的に関連しない。様々な汎用機械が、本明細書の教示に従って書かれたプログラムと共に使用されてもよく、又は、必要な方法ステップを実行するためにより特殊な装置を構築することが好都合であることがわかってもよい。これらの様々な機械に必要な

構造は、与えられた説明から明らかになる。

【００２３】

ここで図面を参照する。全体を通して、同様の参照数字は、全体を通して同様の要素を参照するために使用される。以下の説明では、説明の目的で、その完全な理解を提供するために、多数の特定の詳細を示す。しかしながら、新たな実施形態は、これらの具体的な詳細がなくとも実施され得ることが明らかであり得る。他の例では、その説明を容易にするために、周知の構造及び装置をブロック図の形で示す。その意図は、請求される主題と一致する全ての修正物、均等物、及び代替物を網羅することである。

【００２４】

図１Ａは、例示的な実施形態に係るデータ送信システムを示す。以下で更に議論されるように、システム１００は、非接触カード１０５と、クライアント装置１１０と、ネットワーク１１５と、サーバ１２０とを含んでもよい。図１Ａは構成要素の単一の例を示しているが、システム１００は、任意の数の構成要素を含んでもよい。

【００２５】

システム１００は、１以上の非接触カード１０５を含んでもよい。一実施形態では、非接触カード１０５は、組み込み集積回路、ストレージ装置、及びカードが近距離無線通信（ＮＦＣ）プロトコルを使用して送信装置と通信することを可能にするインタフェースを含むクレジットカード寸法のカードを含む。本明細書で使用され得る非接触カードは、例えば、’１１９出願に記載されている非接触カードを含む。

【００２６】

システム１００は、クライアント装置１１０を含んでもよい。クライアント装置１１０は、ネットワーク対応コンピュータであってもよい。本明細書で言及するように、ネットワーク対応コンピュータは、例えば、サーバ、ネットワーク機器、パーソナルコンピュータ、ワークステーション、電話、ハンドヘルドＰＣ、パーソナルデジタルアシスタント、シンクライアント、ファットクライアント、インターネットブラウザ、又は他の装置を含むコンピュータ装置、又は通信装置を含み得るが、それらに限定されない。クライアント装置１１０はまた、モバイル装置であってもよい。例えば、モバイル装置は、Ａｐｐｌｅ（登録商標）のｉＰｈｏｎｅ（登録商標）、ｉＰｏｄ（登録商標）、ｉＰａｄ（登録商標）、又はＡｐｐｌｅ（登録商標）のｉＯＳオペレーティングシステムを実行する任意の他のモバイル装置、ＭｉｃｒｏｓｏｆｔのＷｉｎｄｏｗｓ（登録商標）モバイルオペレーティングシステムを実行する任意の装置、ＧｏｏｇｌｅのＡｎｄｒｏｉｄ（登録商標）オペレーティングシステムを実行する任意の装置、及び／又は他のスマートフォン、タブレット、又は同様のウェアラブルなモバイル装置を含んでもよい。

【００２７】

クライアント装置１１０は、プロセッサ及びメモリを含んでもよく、処理回路は、本明細書に記載される機能を実行するために必要なプロセッサ、メモリ、エラー及びパリティ／ＣＲＣチェッカ、データエンコーダ、衝突防止アルゴリズム、コントローラ、コマンドデコーダ、セキュリティプリミティブ及び改竄防止ハードウェアを含む付加的な構成要素を含んでもよいことが理解される。クライアント装置１１０は、ディスプレイ及び入力装置を更に含んでもよい。ディスプレイは、液晶ディスプレイ、発光ダイオードディスプレイ、プラズマパネル、及び陰極線管ディスプレイを含む、コンピュータモニタ、フラットパネルディスプレイ、及びモバイル装置スクリーンなどの視覚情報を提示するための任意のタイプの装置であってもよい。入力装置は、タッチスクリーン、キーボード、マウス、カーソル制御装置、タッチスクリーン、マイクロフォン、デジタルカメラ、ビデオレコーダ又はカムコーダなどの、ユーザ装置によって利用可能でサポートされ得る、ユーザ装置に情報を入力するための任意の装置を含んでもよい。これらの装置は、情報を入力し、本明細書に記載されるソフトウェア及び他の装置と相互作用するために使用されてもよい。

【００２８】

いくつかの例では、システム１００のクライアント装置１１０は、例えば、データを送信及び／又は受信するためにシステム１００の１以上の構成要素とのネットワーク通信を

可能にするソフトウェアアプリケーションなどの１以上のアプリケーションを実行してもよい。

【００２９】

クライアント装置１１０は、１以上のネットワーク１１５を介して１以上のサーバ１２０と通信してもよく、サーバ１２０と共に、それぞれのフロントエンドとバックエンドの組として動作してもよい。クライアント装置１１０は、例えば、クライアント装置１１０上で実行されるモバイル装置アプリケーションから、１以上の要求をサーバ１２０に送信してもよい。１以上の要求は、サーバ１２０からデータを取得することに関連してもよい。サーバ１２０は、クライアント装置１１０から１以上の要求を受信してもよい。クライアント装置１１０からの１以上の要求に基づいて、サーバ１２０は、要求されたデータを１以上のデータベース（図示せず）から取得するように構成されてもよい。１以上のデータベースからの要求されたデータの受信に基づいて、サーバ１２０は、１以上の要求に応答する受信されたデータをクライアント装置１１０に送信するように構成されてもよい。

【００３０】

システム１００は、１以上のネットワーク１１５を含んでもよい。いくつかの例では、ネットワーク１１５は、無線ネットワーク、有線ネットワーク、又は無線ネットワークと有線ネットワークとの任意の組合せのうちの１以上であってもよく、クライアント装置１１０をサーバ１２０に接続するように構成されてもよい。例えば、ネットワーク１１５は、光ファイバネットワーク、受動光ネットワーク、ケーブルネットワーク、インターネットネットワーク、衛星ネットワーク、無線ローカルエリアネットワーク（ＬＡＮ）、移動通信用グローバルシステム、パーソナルコミュニケーションサービス、パーソナルエリアネットワーク、無線アプリケーションプロトコル、マルチメディアメッセージサービス、拡張メッセージサービス、ショートメッセージサービス、時間分割多重化に基づくシステム、符号分割多重アクセスに基づくシステム、Ｄ－ＡＭＰＳ、Ｗｉ－Ｆｉ（登録商標）、固定無線データ、ＩＥＥＥ８０２．１１ｂ、８０２．１５．１、８０２．１１ｎ及び８０２．１１ｇ、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＮＦＣ、無線自動識別（ＲＦＩＤ）、Ｗｉ－Ｆｉ（登録商標）などのうちの１以上を含んでもよい。

【００３１】

さらに、ネットワーク１１５は、限定されないが、電話回線、光ファイバ、ＩＥＥＥイーサネット９０２．３、広域ネットワーク、無線パーソナルエリアネットワーク、ＬＡＮ、又はインターネットなどのグローバルネットワークを含んでもよい。さらに、ネットワーク１１５は、インターネットネットワーク、無線通信ネットワーク、セルラーネットワークなど、又はそれらの任意の組合せをサポートしてもよい。ネットワーク１１５は、スタンドアロンネットワークとして動作し、又は互いに協働して動作する、１つのネットワーク、又は前述の例示的なタイプのネットワークうちの任意の数を更に含んでもよい。ネットワーク１１５は、それらが通信可能に結合されている１以上のネットワーク要素の１以上のプロトコルを利用してもよい。ネットワーク１１５は、他のプロトコルに、又は他のプロトコルからネットワークデバイスの１以上のプロトコルに翻訳してもよい。ネットワーク１１５は単一のネットワークとして描かれているが、１以上の例によれば、ネットワーク１１５は、例えば、インターネット、サービス提供者のネットワーク、ケーブルテレビネットワーク、クレジットカード協会ネットワークなどの企業ネットワーク、及びホームネットワークなどの複数の相互接続されたネットワークを含んでもよいことが理解されるべきである。

【００３２】

システム１００は、１以上のサーバ１２０を含んでもよい。いくつかの例では、サーバ１２０は、メモリに結合された１以上のプロセッサを含んでもよい。サーバ１２０は、様々なタイミングで様々なデータを制御して呼び出して複数のワークフロー動作を実行するための中央システム、サーバ、又はプラットフォームとして構成されてもよい。サーバ１２０は、１以上のデータベースに接続するように構成されてもよい。サーバ１２０は、少なくとも１つのクライアント装置１１０に接続されてもよい。いくつかの実施形態では、

サーバ１２０は、本明細書に開示されるような暗号認証を実行するように構成された認証サーバであってよい。

【００３３】

図１Ｂは、本開示の１以上の実施形態に係る非接触カード取引を認証するための例示的なシーケンスを示すタイミング図である。特に、図１Ｂは、非接触カード１０５とクライアント装置１１０との間で、暗号を含む認証データを交換するための例示的なプロセスを記述する。システム１００は、アプリケーション１２２及びプロセッサ１２４を含み得る非接触カード１０５及びクライアント装置１１０を含んでもよい。図１Ｂは、図１Ａに示されているのと同様の構成要素を参照してもよい。

【００３４】

ステップ１０２で、アプリケーション１２２は、（例えば、非接触カード１０５の近くに持ち運ばれた後）非接触カード１０５と通信する。アプリケーション１２２と非接触カード１０５との間の通信は、アプリケーション１２２と非接触カード１０５との間のＮＦＣデータ送信を可能にするために、非接触カード１０５がクライアント装置１１０のカードリーダー（図示せず）に十分に近付くことを含んでもよい。

【００３５】

ステップ１０４において、クライアント装置１１０と非接触カード１０５との間で通信が確立された後、非接触カード１０５は、メッセージ認証コード（ＭＡＣ）暗号を生成する。いくつかの例では、これは、アプリケーション１２２によって非接触カード１０５が読み取られる時に行われてもよい。特に、これは、ＮＦＣデータ交換フォーマットに従って生成され得る近距離データ交換（ＮＤＥＦ）タグの、ＮＦＣ読み取りなどの読み取り時に行われてもよい。例えば、アプリケーション１２２などのリーダは、ＮＤＥＦ生成アプレットのアプレットＩＤを有するアプレット選択メッセージなどのメッセージを送信してもよい。選択が確認されると、選択ファイルメッセージのシーケンスに続いて読み取りファイルメッセージが送信されてもよい。例えば、シーケンスは、「機能ファイルを選択する」、「機能ファイルを読み込む」、及び「ＮＤＥＦファイルを選択する」を含んでもよい。この時点で、非接触カード１０５によって保持されるカウンタ値が更新又はインクリメントされてもよく、その後に「ＮＤＥＦファイルを読み込む」を送信してもよい。この時点で、ヘッダと共有秘密とを含むメッセージが生成されてもよい。

【００３６】

その後、セッション鍵が生成されてもよい。一実施形態では、変形鍵は、暗号ハッシュを使用してマスタ対称鍵と非接触カードによって維持される動的カウンタ値とを組み合わせることによって生成されてもよい。使用され得る暗号ハッシュアルゴリズムの例は、対称暗号化アルゴリズム、ＨＭＡＣアルゴリズム、及びＣＭＡＣアルゴリズムを含む。ユーザ名及び／又は暗号を暗号化するために使用され得る対称アルゴリズムの非限定的な例は、３ＤＥＳ（トリプルデータ暗号化アルゴリズム）又はＡＥＳ（高度暗号化標準）１２８などの対称暗号化アルゴリズム、ＨＭＡＣ－ＳＨＡ－２５６などの対称ハッシュベースメッセージ認証（ＨＭＡＣ）アルゴリズム、及びＡＥＳ－ＣＭＡＣなどの対称暗号ベースメッセージ認証コード（ＣＭＡＣ）アルゴリズムを含んでもよい。暗号化の多数の形式が当業者に知られていることが理解され、本開示は、本明細書で具体的に特定される形式に限定されない。

【００３７】

ＭＡＣ暗号はメッセージから生成されてもよく、メッセージは、ヘッダ及び共有秘密を含んでもよい。いくつかの実施形態では、共有秘密及び／又はＰＩＮを含むがこれに限定されない共有情報は、その後、ランダムデータの１以上のブロックと連結され、暗号アルゴリズム及び変形鍵を使用して符号化されて、ＭＡＣ暗号を生成してもよい。その後、ＭＡＣ暗号とヘッダとが連結され、ＡＳＣＩＩの１６進数として符号化され、（「ＮＤＥＦファイルを読み込む」メッセージに応答する）ＮＤＥＦメッセージ形式で返信されてもよい。

【００３８】

いくつかの例では、ＭＡＣ暗号はＮＤＥＦタグとして送信されてもよく、他の例では、ＭＡＣ暗号は、（例えば、フォーマットされた文字列として）統一資源標識と共に含まれてもよい。

【００３９】

いくつかの例では、アプリケーション１２２は、要求を非接触カード１０５に送信するように構成されてもよく、要求は、ＭＡＣ暗号を生成する命令を含む。

【００４０】

ステップ１０６において、非接触カード１０５は、ＭＡＣ暗号をアプリケーション１２２に送信する。いくつかの例では、ＭＡＣ暗号の送信は、ＮＦＣによって行われるが、本開示はこれに限定されない。他の例では、この通信は、Ｂｌｕｅｔｏｏｔｈ（登録商標）、Ｗｉ－Ｆｉ（登録商標）、又は無線データ通信の他の手段によって行われてもよい。

【００４１】

ステップ１０８において、アプリケーション１２２は、ＭＡＣ暗号をプロセッサ１２４に伝達する。

【００４２】

ステップ１１２において、プロセッサ１２４は、アプリケーション１２２からの命令にしたがって、ＭＡＣ暗号を検証する。例えば、ＭＡＣ暗号は、図１Ａのサーバ１２０などの認証サーバによって検証されてもよい。認証サーバは、各クライアント装置１１０のために、クライアント装置のカウンタ、共有秘密、及び鍵のコピーを保存してもよい。いくつかの実施形態では、以下でより詳細に説明するように、認証サーバは、クライアント装置に関連付けられたＰＩＮを記憶してもよい。認証サーバは、カウンタが同期した状態を維持するように、クライアント装置１１０と認証サーバとの間で確立されたプロトコルにしたがって、各非接触カード取引のカウンタを更新してもよい。認証サーバは、カウンタ、鍵、共有秘密及び／又はＰＩＮのコピーを使用して、予想ＭＡＣ暗号を構築してもよい。

【００４３】

いくつかの例では、ＭＡＣ暗号は、検証の目的のためにデジタル署名として機能し得る。公開鍵非対称アルゴリズムなどの他のデジタル署名アルゴリズム、例えば、デジタル署名アルゴリズム、ＲＳＡアルゴリズム、又はゼロ知識プロトコルが、この検証を実行するために使用されてもよい。

【００４４】

認証サーバは、非接触カードから受信したＭＡＣ暗号を、認証サーバによって生成される予想ＭＡＣ暗号と比較してもよい。このような措置は、様々な方法で取引のセキュリティを向上させる。第一に、クライアントとサーバの間で確立されたプロトコルに従って定期的に更新される可変カウンタ値を使用して構築された暗号の動的な性質は、悪意のある第三者の、認証情報を再利用する能力を低下させる。第二に、暗号化アルゴリズムの使用はさらに、盗聴による機密情報の発見を防ぐ。第三に、ＰＩＮコード検証を暗号認証と共に組み込むことで、二要素認証のための知識修飾子が追加される。

【００４５】

図２Ａ及び図２Ｂは、暗号と共に、及び／又は暗号の一部としてＰＩＮを使用する認証方法をサポートするように構成された二要素認証システムの一実施形態のそれぞれのシステム及びプロセスを示す。

【００４６】

図２Ａのシステム２００において、取引装置２２２（これは、クライアントモバイル装置、加盟店取引装置、又はＮＦＣ通信能力を備える任意の装置であってもよい）は、ユーザ２０２から入力ＰＩＮなどの情報を受け取るためのユーザインタフェース２２５を含むことがわかる。取引装置２２２はまた、非接触カード２０５とのＮＦＣ通信をサポートするように構成されたＮＦＣインタフェース２２０と、認証サーバ２２３とのインターネットプロトコル（ＩＰ）通信を含むがこれに限定されないネットワーク通信をサポートするように構成されたネットワークインタフェース２２７とを含むことがわかる。

【００４７】

一態様によれば、非接触カード２０５はＰＩＮ照合ロジック２１０を含み、これは、非接触カードのメモリ内に記憶されたＰＩＮを、例えばＮＤＥＦレコードの一部として取引装置２２２から受信されたＰＩＮと比較するように構成されたハードウェア、ソフトウェア又はそれらの組合せを含んでもよい。カード２０５はまた、例えば’１１９出願に開示されたような暗号を生成するように構成された暗号生成ロジック２１１を含む。

【００４８】

暗号ロジック２１１は、ハードウェア構成要素とソフトウェア構成要素との組合せを備えてもよく、この組合せは、カード２０５についての１以上の鍵及びカウンタ値を記憶するように構成されたストレージ装置を含むが、これに限定されない。非接触カードは、非接触カードからのメッセージを符号化する際に使用するための変形動的鍵を生成する際に使用するためのカウンタ、暗号化及び／又はハッシュ化ハードウェア及びソフトウェアなどを更に含んでもよい。いくつかの実施形態では、暗号ロジック２１１は、少なくとも部分的に、非接触カード２０５のメモリに記憶されたアプレットとして実装されてもよい。ＰＩＮロジック２１０及び暗号ロジック２１１は、別々に区切られて示されているが、様々な実施形態において機能が異なるように配分されてもよいことが理解される。例えば、いくつかの実施形態では、ＰＩＮロジック２１０及び暗号ロジック２１１は、単一のアプレットによって実装されてもよい。

【００４９】

サーバ２２３は、暗号検証ロジック２２８を含むことがわかる。暗号検証ロジック２２８は、ハードウェア構成要素とソフトウェア構成要素との組合せを備えてもよく、この組合せは、クライアント鍵及びカウンタ値を記憶するストレージ装置、カウンタ、暗号化及び／又はハッシュ化ハードウェア及びソフトウェアなどを含むが、これに限定されない。一実施形態では、暗号検証ロジック２２８は、予想暗号の生成に使用するための変形動的鍵を生成するように構成されてもよく、検証ロジックは、予想暗号と、クライアント装置から受信した暗号とを比較してもよい。暗一致する暗号は、クライアント装置のカウンタと認証サーバとの間の同等性を示す。さらに、一致する暗号は、共有秘密、ＰＩＮなどの情報の知識を示し得る。

【００５０】

図２Ｂは、図２Ａのシステムを使用する二要素認証のための方法を示す。ステップ２５１では、ユーザ２０２によって取引が開始される。例えば、ユーザは、アカウントにアクセスし、購入を行い、又は本明細書に開示される二要素認証方法から利益を得る動作を実行しようとしてもよい。ステップ２５２において、ユーザ２０２は、ＰＩＮを入力するように促され、入力ＰＩＮを受け取ると、取引装置２２２は、例えば、取引装置２２２上でカード２０５をタップするか、又は取引装置２２２との通信範囲内に非接触カード２０５を持って行くようにユーザを促すことによって、非接触カード２０５との二重認証暗号交換を開始してもよい。

【００５１】

非接触カードが取引装置の範囲内にあるとき、ステップ２５３では、取引装置２２２は、入力ＰＩＮを、例えばＰＩＮ記録として非接触カード２０５に送信し、暗号生成アプレットに関連付けられたＮＦＣタグの読み取りを発令する。ステップ２５４では、ＰＩＮ照合ロジック２１０は、入力ＰＩＮと記憶されたＰＩＮ２１５とを比較してもよい。ステップ２５５で「一致」と判定された場合、暗号生成アプレットは、ステップ２５６において暗号を生成し、暗号を取引装置２２２に送信するよう指示される。

【００５２】

ステップ２５７において、例えばＰＩＮの不一致のために暗号が受信されない場合、ステップ２５９で取引がキャンセルされてもよい。ステップ２５７で暗号が受信された場合、ステップ２５８において、取引装置２２２は、取引の認証を要求し、暗号を認証サーバ２２３に送信する。

【００５３】

ステップ２６０では、認証サーバ２２３が暗号を受信すると、認証サーバは、非接触カ

ード２０５に関連するカウンタ、鍵、共有秘密などを含むクライアントデータを取得する。この情報を使用して、ステップ２６１において、認証サーバは、予想暗号を生成し、ステップ２６２において、生成された暗号が、受信された暗号によって提供される固有のデジタル署名に一致するか否かを判断する。ステップ２６３において、認証サーバは、取引装置２２２に許可／拒否の応答を返す。取引装置２２２が、ステップ２６４において取引が許可されたと判断した場合、ステップ２６５において取引が実行されてもよい。取引が拒否された場合、取引装置は、ステップ２５０において取引をキャンセルする。

【００５４】

開示される二要素ＰＩＮに基づく認証システムは、保存されたＰＩＮ２１５を発見から保護することによって、取引セキュリティを改善する。議論されたように、保存されたＰＩＮは公に送信されず、したがってＰＩＮ交換中に悪意ある監視によって取得されることはない。ＰＩＮ、共有秘密及び／又はカウンタ値がスキミングによって取得され得る場合、カードと認証サーバとの間に実装された動的カウンタプロトコルの知識を有しないクローンカードは、動作不能になる。

【００５５】

図３Ａ及び図３Ｂは、二要素ＰＩＮに基づく認証システム及び方法の他の実施形態を開示する。ここで、ＰＩＮ照合機能性は、認証サーバ３２３によって、暗号検証ロジック３２８の一部として提供されてもよい。図３Ａのシステム３００において、カード３０５は、非接触カードのための固有のＰＩＮ３１５を記憶すると共に、前述のように暗号生成アプレットを含み得る暗号論理３１１を構成する。一実施形態によれば、以下により詳細に説明するが、非接触カード３０５によって提供される暗号は、ＰＩＮ３１５を含み、及び／又はＰＩＮ３１５を用いて形成されてもよい。

【００５６】

取引装置３２２は、ユーザインタフェース３２５と、ＮＦＣインタフェース３２０と、ネットワークインタフェース３２７とを含む。さらに、取引装置は、カプセル化ロジック３２４を含んでもよい。カプセル化ロジック３２４は、一実施形態では、入力ＰＩＮ／暗号の組を認証サーバ３２３に送信する前に入力ＰＩＮ及び／又は暗号を暗号化するためのコードを含んでもよい。

【００５７】

認証サーバ３２３は、暗号検証ロジック３２８を含む。暗号検証ロジック３２８は、暗号化された入力ＰＩＮ／暗号の組から入力ＰＩＮを抽出するように動作してもよい。暗号検証ロジック３２８は更に、入力ＰＩＮと、カウンタ及び鍵データなどの保存されたクライアントデータとを使用して、予想される暗号を生成するように構成されてもよい。暗号検証ロジック３２８は、次に、予想暗号を抽出された暗号と比較して、入力ＰＩＮ及び記憶されたＰＩＮ、並びにカウンタ及び鍵情報との相関関係を示す一致を判定してもよい。

【００５８】

図３Ｂは、システム３００によって実行され得る二要素認証プロセスのフロー図である。ステップ３５１で取引が開始された後、ステップ３５２においてユーザ３０２は入力ＰＩＮを要求される。ステップ３５３において、前述のように暗号認証プロセスが開始され、例えば、取引装置３２２は、カード３０５のＮＤＥＦタグ生成アプレット、特に、暗号ペイロードに含めるために非接触カード３０５からＰＩＮ３１５を取得するように構成されたＮＤＥＦタグ生成アプレットに、ＮＦＣ読み取り操作を発令してもよい。ステップ３５６において、非接触カードのアプレットは、＜ユーザＩＤ＞＜カウンタ＞＜ユーザＩＤ＋カウンタ＋ＰＩＮのＭＡＣ＞の形式で暗号データを組み立ててもよい。いくつかの実施形態では、カウンタを用いて形成された変形鍵は、暗号ハッシュアルゴリズムなどを用いて＜ユーザＩＤ＋カウンタ＋ＰＩＮのＭＡＣ＞を符号化するために使用されてもよい。この検証を行うために、公開鍵非対称アルゴリズム、例えば、デジタル署名アルゴリズム及びＲＳＡアルゴリズム、又はゼロ知識プロトコルが、代替的に使用されてもよい。

【００５９】

非接触カード３０５は、暗号を取引装置３２２に返し、ステップ３５４において取引装

置３２２は、入力ＰＩＮを、受信された暗号と組み合わせる。いくつかの実施形態では、入力ＰＩＮ及び／又は受信された暗号は、例えば対称暗号化アルゴリズムを用いて、入力ＰＩＮ情報を難読化するために暗号化されてもよい。この組合せは、認証サーバ３２３に送られる。

【００６０】

ステップ３６０において、認証サーバ３２３は、非接触カードに関する認証情報（カウンタ値、鍵、共有秘密などを含む）をストレージから取得する。この情報を使用して、ステップ３６１では、認証サーバは、例えば、＜ユーザＩＤのＭＡＣ＋記憶されたカウンタ＋入力ＰＩＮ＞の形式で、予想暗号を組み立ててもよい。ステップ３６２において、認証サーバは、予想暗号と非接触カードから取得された暗号とが一致するかどうかを判断し、ステップ３６３において、取引装置３２２に認証ステータスを返す。ステップ３６４における認証ステータスの受信に応じて、取引が、ステップ３６４で実行され、又は、ステップ３５９でキャンセルされる。

【００６１】

したがって、図３Ａ及び３Ｂの実施形態では、非接触カードによって生成される暗号はＰＩＮを使用して形成されるが、ＰＩＮ自体は、ネットワーク上で識別可能な形式又は導出可能な形式で送信されない。

【００６２】

図４Ａ及び図４Ｂは、二要素ＰＩＮに基づく認証システム及び方法の他の実施形態を開示する。ここで、ＰＩＮ照合は、公開鍵暗号を使用して取引装置によって実行されてもよい。一実施形態では、非接触カード４０５は、プライベート鍵４１７を保持する。プライベート鍵４１７は、非接触カード４０５のみに知られ、公開鍵によって暗号化された通信を復号するために使用されてもよい。非接触カードは、取引装置４２２への通信のための暗号を提供するために、固有のデジタル署名、暗号ハッシュを生成するように構成されたデジタル署名ロジック４１１を更に含んでもよい。

【００６３】

取引装置４２２は、ユーザインタフェース４２５とＮＦＣインタフェース４２０とを含む。取引装置は、乱数生成器４５４と、暗号化ロジック４２４と、非接触カードに関する公開鍵４５７を記憶するメモリ４５５とを更に含むことが示されている。ここで、公開鍵は、取引装置によって、信頼された認証機関から取得されてもよい。取引装置は、以下に説明するように、デジタル署名を生成するためのデジタル署名ロジック４５６を更に含む。いくつかの実施形態において、カード４０５の公開鍵は、カード４０５によって記憶され、取引装置によって認証プロセスの一部として読み出されてもよい。

【００６４】

図４Ｂには、図４Ａのシステム４００を使用する二要素認証の方法が示されている。ステップ４６１で取引が開始されたと判断されると、ステップ４６２において、ユーザ４０４は、入力ＰＩＮを入力するよう促される。ステップ４６３において、取引装置は、カード自体から、又は信頼された認証機関から、非接触カードに関する公開鍵を取得する。ステップ４６５で、取引装置は乱数を生成し、それを公開鍵で暗号化し、非接触カード４０５に送信する。ステップ４６６で、非接触カードは、そのプライベート鍵を使用して乱数を復号し、乱数と保存されたＰＩＮ４１５との組合せを使用してデジタル署名を生成する。得られたデジタル署名は、取引装置４２２に対して返送される。

【００６５】

ステップ４６７において、取引装置４２２はまた、乱数とユーザ４０２から受け取った入力ＰＩＮとを組み合わせて使用し、デジタル署名を生成する。ステップ４６８において、デジタル署名は、一致を識別するために比較される。一致状態に応じて、取引は、ステップ４７０（一致）において実行される、又は、ステップ４６９（不一致）においてキャンセルされる。

【００６６】

図５Ａ及び図５Ｂは、二要素ＰＩＮに基づく認証システム及び方法の他の実施形態を開

示する。ここで、非接触カードＰＩＮは、認証サーバに記憶され、取引を認証するために暗号と組み合わせて使用される。図５Ａのシステム５００において、非接触カード５０５は、前述のようにカウンタ、動的鍵、共有秘密などの組合せを用いて暗号を生成するための暗号ロジック５１１を含む。取引装置５２２は、ユーザインタフェース５２０と、ＮＦＣインタフェース５２５と、ネットワークインタフェース５２７とを含む。さらに、取引装置は、カプセル化ロジック５２４を含んでもよい。カプセル化ロジック５２４は、一実施形態では、入力ＰＩＮ／暗号の組を認証サーバ５２３に送信する前に入力ＰＩＮ及び／又は暗号を暗号化するためのコードを含んでもよい。認証サーバ５２３は、ＰＩＮテーブル５９５と、ＰＩＮ照合ロジック５９４と、暗号検証ロジック５９６とを含む。

【００６７】

図５Ｂには、図５Ａのシステム５００を使用する二要素認証の方法が示されている。ステップ５５１における取引の開始に続いて、ステップ５５２でユーザ５０２は入力ＰＩＮを促され、ステップ５５３で取引装置５２２は非接触カード５０５から暗号を要求する。ステップ５５５で、非接触カードは暗号を生成し、それを取引装置５４２２に返す。ステップ５５４で、取引装置は、ユーザから受け取った入力ＰＩＮと、非接触カードからの暗号とを組み合わせて暗号化し、認証サーバ５２３に送信する。ステップ５６０において、認証サーバは、非接触カード５０５に関するＰＩＮ、カウンタ、及び鍵を取得する。ステップ５６１で、認証サーバは、取引装置５２２からのメッセージを復号し、入力ＰＩＮを抽出し、かつステップ５６２で、抽出された入力ＰＩＮと、ＰＩＮテーブルから取得された予想入力ＰＩＮとを比較する。ステップ５６３で、認証サーバ５２３はまた、非接触カード５０５から取得された暗号を抽出してもよい。認証サーバ５２３は、暗号検証ロジックによって記憶された記憶鍵、カウンタ及び共有秘密情報を使用して、予想暗号を構築してもよい。ステップ５６４において、取引装置は、予想暗号と抽出された暗号とを比較して、一致を判定してもよい。比較に応じて、認証サーバ５２３は、ステップ５６５において、取引装置に認証ステータスを返す。ステップ５６６で認証ステータスを受信すると、取引は、ステップ５６８（一致）において実行され、又は、ステップ５６７（不一致）においてキャンセルされる。

【００６８】

以上のように、二要素ＰＩＮに基づく認証を提供するための様々なシステム及び方法を示して説明した。ここで、説明された方法をサポートするために、既に説明された構成要素と共に、及び／又はその代わりに、非接触カード、取引装置及び／又は認証サーバに含まれ得る例示的な構成要素が、図６～図１０に関して説明される。

【００６９】

図６は、非接触カード６００を示している。これは、クレジットカード、デビットカード、又はギフトカードなどの支払カードを含んでもよく、サービス提供者６０５によって発行される。サービス提供者６０５の身元は、カード６００の前面又は背面に表示されてもよい。いくつかの例では、非接触カード６００は、支払カードに関係せず、身分証明カードを含んでもよいが、これに限定されない。いくつかの例では、支払カードは、デュアルインタフェース非接触支払カードを含んでもよい。非接触カード６００は、基板６１０を含んでもよく、基板６１０は、プラスチック、金属、及び他の材料からなる単層、又は１以上の積層を含んでもよい例示的な基板材料は、ポリ塩化ビニル、ポリ塩化ビニルアセテート、アクリロニトリルブタジエンスチレン、ポリカーボネート、ポリエステル、陽極酸化チタン、パラジウム、金、カーボン、紙、及び生分解性材料を含む。いくつかの例では、非接触カード６００は、ＩＳＯ／ＩＥＣ７８１０規格のＩＤ－１形式に準拠した物理的特性を有してもよく、そうでなければ、非接触カードは、ＩＳＯ／ＩＥＣ１４４４３規格に準拠していてもよい。しかしながら、本開示に係る非接触カード６００は、異なる特性を有してもよく、本開示は、非接触カードが支払カードに実装されることを要求しないことが理解される。

【００７０】

非接触カード６００は、カードの前面及び／又は背面に表示される識別情報６１５と、

接触パッド６２０とを含んでもよい。接触パッド６２０は、ユーザ装置、スマートフォン、ラップトップ、デスクトップ、又はタブレットコンピュータなどの他の通信装置との接触を確立するように構成されてもよい。非接触カード６００は、図６に示されていない処理回路、アンテナ、及び他の構成要素も含んでもよい。これらの構成要素は、接触パッド６２０の後方又は基板６１０の他の場所に配置されてもよい。また、非接触カード６００は、磁気ストライプ又はテープを含んでもよく、これは、カードの背面に配置されてもよい（図６には示されていない）。

【００７１】

図７に示すように、接触パッド７２０は、情報を記憶して処理するための処理回路を含んでもよく、処理回路は、マイクロプロセッサ７３０とメモリ７３５とを含む。処理回路は、本明細書に記載される機能を実行するために必要なプロセッサ、メモリ、エラー及びパリティ／ＣＲＣチェッカ、データエンコーダ、衝突防止アルゴリズム、コントローラ、コマンドデコーダ、セキュリティプリミティブ及び改竄防止ハードウェアを含む付加的な構成要素を含んでもよいことが理解される。

【００７２】

メモリ７３５は、リードオンリーメモリ、ライトワンスリードマルチプルメモリ又はリード／ライトメモリ、例えば、ＲＡＭ、ＲＯＭ、及びＥＥＰＲＯＭであってよく、非接触カード７００は、これらのメモリのうちの１以上を含んでもよい。リードオンリーメモリは、読み出し専用として工場でプログラム可能であってもよいし、一度だけプログラム可能であってもよい。一度のみのプログラム可能性は、一度書き込んだ後に多数回読み出す機会を提供する。ライトワンス／リードマルチプルメモリは、メモリチップが工場から出荷された後の時点でプログラムされてもよい。メモリが一度プログラムされると、書き直すことはできないが、多数回読み出されてもよい。

【００７３】

メモリ７３５は、１以上のアプレット７４０と、１以上のカウンタ７４５と、顧客情報７５０とを記憶するように構成されてもよい。一態様によれば、メモリ７３５は、ＰＩＮ７７７を記憶してもよい。

【００７４】

１以上のアプレット７４０は、Ｊａｖａ（登録商標）カードアプレットなどの、それぞれの１以上のサービス提供者のアプリケーションに関連し、１以上の非接触カード上で実行するように構成された１以上のソフトウェアアプリケーションを含んでもよい。例えば、アプレットは、前述のようにＭＡＣ暗号を生成するように構成されたロジックを含んでもよい。ＭＡＣ暗号は、いくつかの実施形態において、ＰＩＮ情報を少なくとも部分的に使用して形成されるＭＡＣ暗号を含む。

【００７５】

１以上のカウンタ７４５は、整数を記憶するのに十分な数値カウンタを含んでもよい。顧客情報７５０は、非接触カード７００のユーザに割り当てられた固有の英数字識別子及び／又は非接触カードのユーザを他の非接触カードのユーザから区別するために共に使用され得る１以上の鍵を含んでもよい。いくつかの例では、顧客情報７５０は、顧客及びその顧客に割り当てられた口座の両方を識別する情報を含んでもよく、顧客の口座に関連付けられた非接触カードを更に識別してもよい。

【００７６】

前述の例示的な実施形態のプロセッサ及びメモリ要素は、接触パッドを参照して説明されたが、本開示はこれに限定されない。これらの要素は、パッド７２０の外部に実装されてもよいこと、又はそれとは完全に別個に実装されてもよいこと、又は接触パッド７２０内に配置されたマイクロプロセッサ７３０及びメモリ７３５要素に加えて、更なる要素として実装されてもよいことが理解される。

【００７７】

いくつかの例では、非接触カード７００は、非接触カード７００内及び接触パッド７２０の処理回路７５５の周囲に配置された１以上のアンテナ７２５を含んでもよい。例えば

、１以上のアンテナは、処理回路と一体であってもよく、１以上のアンテナは、外部のブースターコイルと共に使用されてもよい。他の例として、１以上のアンテナは、接触パッド７２０及び処理回路の外部にあってもよい。

【００７８】

上で説明したように、非接触カード７００は、Ｊａｖａ（登録商標）カードなどのプログラムコード、処理能力及びメモリを含むスマートカード又は他の装置上で動作可能なソフトウェアプラットフォーム上に構築されてもよい。アプレットは、モバイル近距離無線通信（ＮＦＣ）リーダなどのリーダからの近距離データ交換（ＮＤＥＦ）要求などの１以上の要求に応答し、ＮＤＥＦテキストタグとして符号化された暗号的に安全なＯＴＰを含むＮＤＥＦメッセージを生成するように構成されてもよい。

【００７９】

図８は、例示的な実施形態による例示的なＮＤＥＦショートレコードレイアウト（ＳＲ＝１）８００を示す。ＮＤＥＦメッセージは、取引装置が非接触カードと通信するための標準化された方法を提供する。いくつかの例では、ＮＤＥＦメッセージは、１以上のレコードを含んでもよい。ＮＤＥＦレコード８００はヘッダ８０２を含み、これは、メッセージ開始（ＭＢ）フラグ８０３ａ、メッセージ終了（ＭＥ）フラグ８０３ｂ、チャンクフラグ（ＣＦ）８０３ｃ、ショートレコード（ＳＲ）フラグ８０３ｄ、ＩＤ長（ＩＬ）フラグ８０３ｅ及びタイプ名フォーマット（ＴＮＦ）フィールド８０３ｆを含むレコードの残りの部分をどのように解釈するかを定義する複数のフラグを含む。ＭＢ８０３ａ及びＭＥフラグ８０３ｂは、メッセージのそれぞれの最初と最後のレコードを示すように設定されてもよい。ＣＦ８０３ｃ及びＩＬフラグ８０３ｅは、データが「チャンク」（メッセージ内の複数のレコード間に広がるデータ）であり得るか否か、又はＩＤタイプ長フィールド８０８が関連し得るか否かをそれぞれ含む、レコードに関する情報を提供する。ＳＲフラグ８０３ｄは、メッセージが１つのレコードのみを含む場合に設定されてもよい。

【００８０】

ＴＮＦフィールド８０３ｆは、ＮＦＣプロトコルによって規定されるように、当該フィールドが含むコンテンツのタイプを識別する。これらのタイプは、空、周知（ＮＦＣフォーラムのレコードタイプ定義（ＲＴＤ）によって定義されるデータ）、多目的インターネットメール拡張（ＭＩＭＥ）［ＲＦＣ２０４６によって定義される］、完全統一資源識別子（ＵＲＩ）［ＲＦＣ３９８６によって定義される］、外部（ユーザ定義）、不明、変更なし［チャンクの場合］及び予約を含む。

【００８１】

ＮＦＣレコードの他のフィールドは、タイプ長８０４、ペイロード長８０６、ＩＤ長８０８、タイプ８１０、ＩＤ８１２、及びペイロード８１４を含む。タイプ長フィールド８０４は、ペイロード内で見出されるデータの正確な種類を指定する。ペイロード長８０６は、バイト単位のペイロードの長さを含む。レコードは、最大４，２９４，９６７，２９５バイト（又は２＾３２－１バイト）のデータを含んでもよい。ＩＤ長８０８は、バイト単位のＩＤフィールドの長さを含む。タイプ８１０は、ペイロードが含むデータのタイプを特定する。例えば、認証の目的で、Ｔｙｐｅ８１０は、ペイロード８１４が、非接触カードのメモリから取り出された個人識別番号（ＰＩＮ）を少なくとも部分的に用いて形成された暗号であることを示してもよい。ＩＤフィールド８１２は、外部アプリケーションがＮＤＥＦレコード内で搬送されるペイロード全体を識別するための手段を提供する。ペイロード８１４は、メッセージを含む。

【００８２】

いくつかの例では、安全なチャネルプロトコルの下でＳＴＯＲＥ　ＤＡＴＡ（Ｅ２）を実施することにより、データが最初に非接触カードに記憶されてもよい。このデータは、カードに固有の個人ユーザＩＤ（ｐＵＩＤ）及びＰＩＮだけでなく、初期鍵、セッション鍵を含む暗号処理データ、データ暗号化鍵、乱数及び以下でより詳細に説明される他の値のうちの１以上を含んでもよい。他の実施形態では、ｐＵＩＤ及びＰＩＮは、非接触カードをクライアントに運ぶ前に、非接触カード内に予めロードされてもよい。いくつかの実

施形態では、ＰＩＮは、非接触カードに関するクライアントによって選択され、様々な厳しい認証方法を用いたクライアントの検証後に、非接触カードに書き戻されてもよい。

【００８３】

図９は、非接触カード９１０及び／又は認証サーバ９５０の一方が、第一要素の認証中に使用され得る情報を記憶することができる通信システム９００を示す。図３に関して説明したように、各非接触カードは、マイクロプロセッサ９１２と、識別子、鍵、乱数などの１以上の固有の識別属性を含む顧客情報９１９のためのメモリ９１６とを含んでもよい。一態様では、メモリは、本明細書に記載される認証プロセスを制御するために、マイクロプロセッサ９１２によって実行されたときに動作可能なアプレット９１７を更に含む。前述のように、ＰＩＮ９１８は、カード９１０のメモリ９１６内に記憶され、アプレットによって、及び／又は顧客情報９１９の一部としてアクセスされてもよい。さらに、各カード９１０は、１以上のカウンタ９１４と、インタフェース９１５とを含んでもよい。一実施形態では、インタフェースは、ＮＦＣ又は他の通信プロトコルを動作させる。

【００８４】

クライアント装置９２０は、非接触カードと通信するための非接触カードインタフェース９２５と、装置９２０が前述のような様々な通信プロトコルを使用してサービス提供者と通信することを可能にする１以上の他のネットワークインタフェース（図示せず）とを含む。クライアント装置は、サービス提供者のアプリケーションとクライアント装置９２０のユーザとの間の通信を可能にするユーザインタフェース９２９を更に含んでもよい。ユーザインタフェース９２９は、キーボード又はタッチスクリーンディスプレイのうちの１以上を含んでもよい。クライアント装置９２０は、プロセッサ９２４とメモリ９２２とを更に含む。メモリ９２２は、情報と、プロセッサによって実行されたときにクライアント装置９２０の動作を制御するプログラムコードと、を記憶し、例えば、サービス提供者のアプリケーションへのアクセスと、サービス提供者のアプリケーションの使用と、を容易にするためにサービス提供者によってクライアントに提供され得るクライアント側アプリケーション９２３を含む。一実施形態では、クライアント側アプリケーション９２３は、非接触カード９１０からのＰＩＮコードを含む認証情報を、前述のようにサービス提供者によって提供される１以上のサービスに伝送するように構成されたプログラムコードを含む。クライアント側アプリ９２３は、ユーザインタフェース９２６に表示されるアプリケーションインタフェースを介して制御されてもよい。例えば、ユーザは、アプリケーションインタフェースの一部として提供されるアイコン、リンク、又は他のメカニズムを選択して、アプリケーションサービスにアクセスするためにクライアント側アプリケーションを起動してもよい。ここで、起動の一部は、暗号交換を用いてクライアントを検証することを含む。

【００８５】

例示的な実施形態において、暗号交換は、プロセッサとメモリとを有する送信装置を含み、送信装置のメモリは、マスタ鍵と、送信データと、カウンタ値とを含む。送信装置は、プロセッサとメモリとを有する受信装置と通信し、受信装置のメモリは、マスタ鍵を含む。送信装置は、マスタ鍵と１以上の暗号アルゴリズムとを使用して変形鍵を生成し、変形鍵を送信装置のメモリに記憶し、１以上の暗号アルゴリズムと変形鍵を使用してカウンタ値を暗号化して暗号化されたカウンタ値を生成し、１以上の暗号アルゴリズムと変形鍵を使用して送信データを暗号化して暗号化送信データを生成し、暗号化されたカウンタ値と暗号化された送信データとを暗号として受信装置に送信するように構成されてもよい。受信装置は、記憶されたマスタ鍵と記憶されたカウンタ値とに基づいて変形鍵を生成し、変形鍵を受信装置のメモリに記憶し、１以上の復号アルゴリズムと変形鍵とを使用して（暗号化されたカウンタと暗号化された送信データとを含む）暗号化された暗号を復号するように構成されてもよい。受信装置は、復号化されたカウンタと記憶されたカウンタとが一致すると、送信装置を認証してもよい。カウンタは、後続の認証のために送信装置及び受信装置のそれぞれにおいてインクリメントされ、それによって送信装置／受信装置の取引に暗号に基づく動的認証メカニズムを提供してもよい。

【００８６】
図１Ａに関連して述べたように、クライアント装置９２０は、サービス提供者９０５の様々なサービスに接続され、アプリケーションサーバ９０６によって管理されてもよい。図示された実施形態では、認証サーバ９５０及びアプリケーションサーバ９０６は、別個の構成要素として示されているが、アプリケーションサーバが、認証サーバに含まれるとして説明された機能性の全てを含んでもよいことが理解されるべきである。
【００８７】
認証サーバ９５０は、ネットワーク９３０を介してネットワークのメンバと通信するためのネットワークインタフェース９５３と、中央処理ユニット（ＣＰＵ）９５９とを含むことがわかる。いくつかの実施形態では、認証サーバは、サービス提供者のクライアントに関するＰＩＮ情報を含むＰＩＮテーブル９５２を記憶するための非一時的記憶媒体を含んでもよい。そのような情報は、クライアントのユーザ名、クライアントの個人識別子、及びクライアントの鍵とカウンタとを含んでもよいが、これに限定されない。一実施形態では、認証サーバは、暗号の複号及びカウンタの抽出を制御するための認証ユニット９５４と、非接触カード９１０と連携して認証を行うために後述のように使用され得るクライアントカウンタ値テーブル９５６とを更に含む。様々な実施形態において、認証サーバは、各クライアント／非接触カードの組についてのエントリを有するように構成されたＰＩＮテーブル９５２を更に含んでもよい。
【００８８】
図１０は、プロンプトウィンドウ１０２０と入力部１０３０とを含むディスプレイ１０１０を備えるクライアント装置１０００の一例を示す。プロンプト部分は、認証プロセスを通じてクライアントを誘導するための様々なプロンプトを表示してもよく、例えば、装置１０００に向けたカード８０５の動きを促すためのプロンプト「カードをかざしてください」を含む。図１０に示すように、プロンプトは、「ＰＩＮを入力してください」などの指示を含み、ユーザがＰＩＮを入力することを可能にするためにキーボード又は他の入力機構を提供してもよい。いくつかの実施形態では、カードタップの成功及びＰＩＮ入力に続いて、ユーザは、取引を完了し得る。例えば、課金を完了する、機密データにアクセスする、特定の人にアクセスするなどである。
【００８９】
以上のように、多要素認証のために暗号及びＰＩＮ交換を使用する二要素ＰＩＮに基づく認証のシステム及び方法が、カードクローニングの可能性を低減及び／又は排除するために示され、説明された。
【００９０】
本願で使用されるように、用語「システム」、「構成要素」及び「ユニット」は、ハードウェア、ハードウェアとソフトウェアとの組合せ、ソフトウェア、又は実行中のソフトウェアのいずれかであるコンピュータ関連エンティティを指すことが意図され、その例は、本明細書に記載されている。例えば、構成要素は、プロセッサ上で実行されるプロセス、プロセッサ、ハードディスクドライブ、複数のストレージドライブ、（光及び／又は磁気記憶媒体の）非一時的コンピュータ可読媒体、オブジェクト、実行物、実行のスレッド、プログラム、及び／又はコンピュータであってもよいが、これらに限定されない。例示すると、サーバ上で実行されるアプリケーション及びサーバの両方が構成要素であってもよい。１以上の構成要素は、プロセス及び／又は実行のスレッド内に存在してもよく、構成要素は、１つのコンピュータ上にローカライズされてもよく、及び／又は２以上のコンピュータの間に分散されてもよい。
【００９１】
さらに、構成要素は、動作を調整するために、様々なタイプの通信媒体によって互いに通信可能に結合されてもよい。この調整は、情報の単方向又は双方向の交換を含んでもよい。例えば、構成要素は、通信媒体を介して通信される信号の形で情報を伝達してもよい。情報は、様々な信号線に割り当てられた信号として実装されてもよい。このような割り当てにおいて、各メッセージは信号であってもよい。しかしながら、更なる実施形態は、

代わりにデータメッセージを採用してもよい。そのようなデータメッセージは、様々な接続にわたって送信されてもよい。例示的な接続は、パラレルインタフェース、シリアルインタフェース、及びバスインタフェースを含む。

【００９２】

いくつかの実施形態は、それらの派生物と共に「一実施形態」又は「ある実施形態」という表現を用いて説明されることがある。これらの用語は、実施形態に関連して説明される特定の特徴、構造、又は特性が、少なくとも１つの実施形態に含まれることを意味する。本明細書の様々な場所で「一実施形態において」という表現が現れるが、必ずしも全てが同じ実施形態を指しているわけではない。さらに、特に注記しない限り、前述の特徴は、任意の組合せで共に使用可能であると認識される。したがって、別々に議論された特徴は、それらの特徴が互いに交換できないことが注記されない限り、互いに組み合わせて採用され得る。

【００９３】

本明細書で使用される表記及び命名法を一般的に参照すると、本明細書の詳細な説明は、コンピュータ又はコンピュータのネットワーク上で実行されるプログラム手順として実装され得る機能ブロック又はユニットの見地から提示されてもよい。これらの手順の説明及び表現は、その仕事の内容を当業者に最も効果的に伝達するために、当業者によって使用される。

【００９４】

手順は、ここでは、そして一般的には、所望の結果をもたらす自己矛盾のない操作のシーケンスであると考えられる。これらの操作は、物理的な量の物理的な操作を要求する。通常、もっとも必ずしもそうではないが、これらの量は、記憶、送信、結合、比較、及び他の操作を行うことができる電気、磁気、又は光学信号の形態をとる。主に一般的な使用上の理由から、これらの信号をビット、値、要素、記号、文字、用語、数などと呼ぶことが時に便利であることがわかる。しかし、これらの用語及び類似の用語の全ては、適切な物理量と関連付けられるべきであり、それらの量に適用される便宜的なラベルに過ぎないことに留意すべきである。

【００９５】

さらに、実行される操作は、しばしば、人間の操作者によって実行される精神的操作に一般的に関連付けられる、加算又は比較などの用語で呼ばれる。１以上の実施形態の一部を形成する本明細書に記載された操作のいずれにおいても、ほとんどの場合、人間の操作者のそのような能力は必要でなく望ましくもない。むしろ、この操作は機械操作である。様々な実施形態の操作を実行するための有用な機械は、汎用デジタルコンピュータ又は同様の装置を含む。

【００９６】

いくつかの実施形態は、それらの派生物と共に「結合された」及び「接続された」という表現を用いて説明される場合がある。これらの用語は、必ずしも互いの同義語として意図されていない。例えば、いくつかの実施形態は、２以上の要素が互いに直接物理的又は電気的に接触していることを示すために、「接続」及び／又は「結合」という用語を用いて説明される場合がある。しかしながら、用語「結合」は、２以上の要素が互いに直接的に接触していないものの互いに協力又は相互作用することを意味してもよい。

【００９７】

強調すべきなのは、本開示の要旨が、読者が技術的な開示の性質を迅速に把握できるように提供されることである。それは、請求の範囲又は意味を解釈又は制限するために使用されるのではないことを理解した上で提出される。さらに、前述の詳細な説明では、開示を合理化するために、様々な特徴が単一の実施形態にまとめられている。この開示方法は、請求された実施形態が各請求項に明示的に記載されている以上の特徴を要求するという意図を反映したとして解釈されるべきではない。むしろ、以下の請求の範囲が反映するように、発明の主題は、単一の開示された実施形態の全ての特徴よりも少ない特徴にある。したがって、以下の請求の範囲は、各請求項が独立した実施形態としてそれ自体で成り立

っている状態で、詳細な説明に組み込まれる。添付の請求の範囲において、用語「含む（including）」及び「ここで（in which）」は、それぞれ、各用語「含む（comprising）」及び「ここで（wherein）」の平易な英語での等価物として使用される。さらに、用語「第１」、「第２」、「第３」などは、単にラベルとして使用され、それらの対象に数値要件を課すことを意図していない。

【００９８】

以上で説明したことは、開示された構成の例を含む。もちろん、構成要素及び／又は方法論の考え得る全ての組合せを説明することは不可能であるが、当業者であれば、多くの更なる組合せ及び置換が可能であることを認識し得る。したがって、新規な構成は、添付の請求の範囲の精神及び範囲内に入るそのような全ての変更、修正及び変形を包含することが意図される。

【図面】

【図１Ａ】

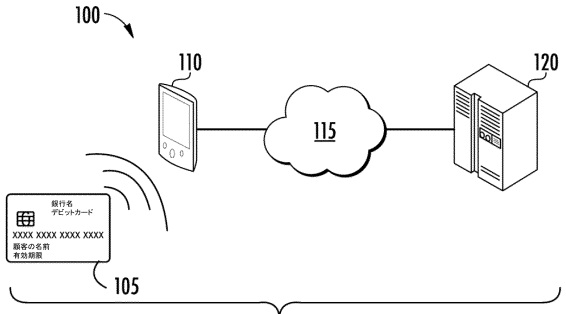


FIG. 1A

【図１Ｂ】

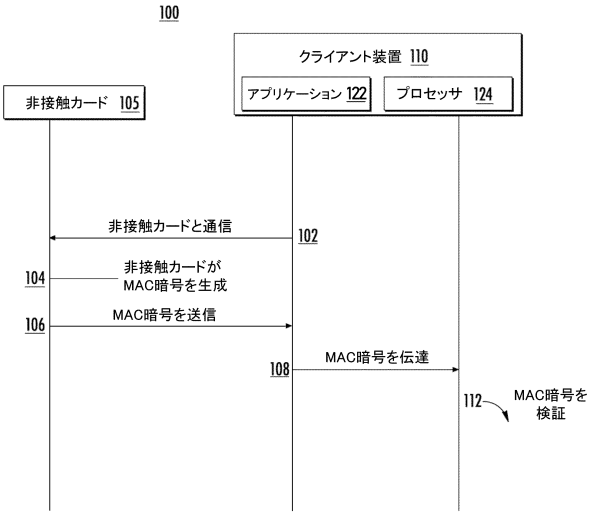


FIG. 1B

【図２Ａ】

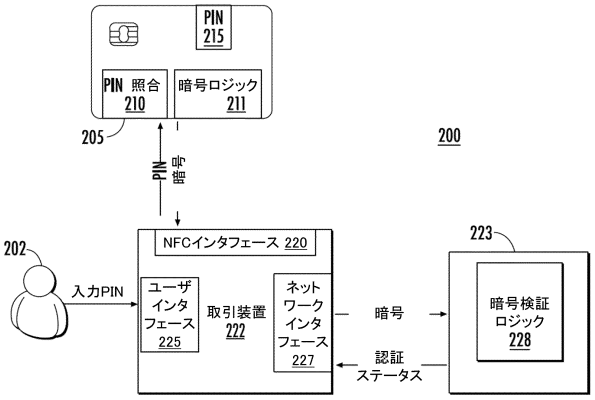


FIG. 2A

【図２Ｂ】

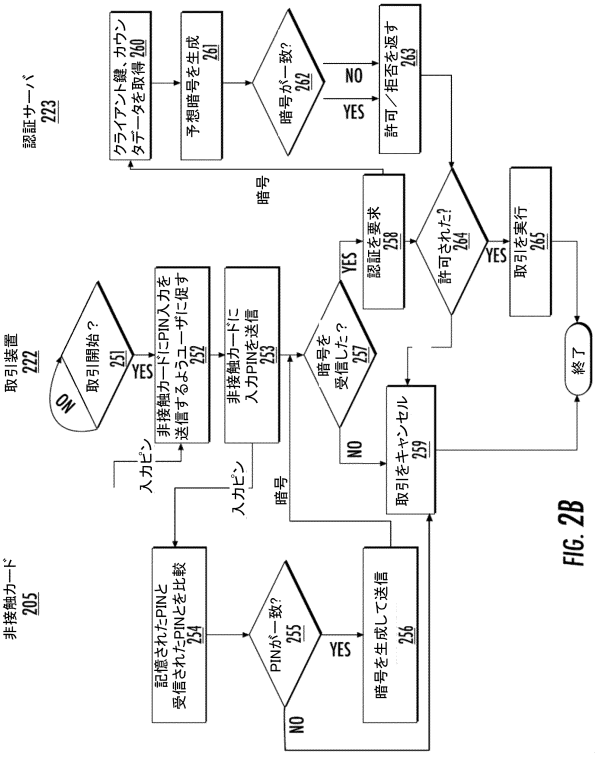


FIG. 2B

【図３Ａ】

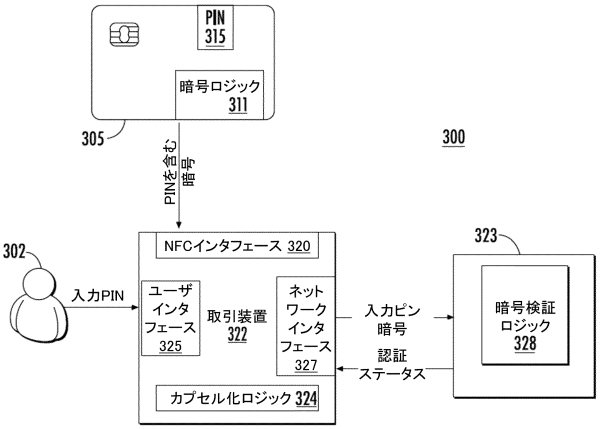


FIG. 3A

【図３Ｂ】

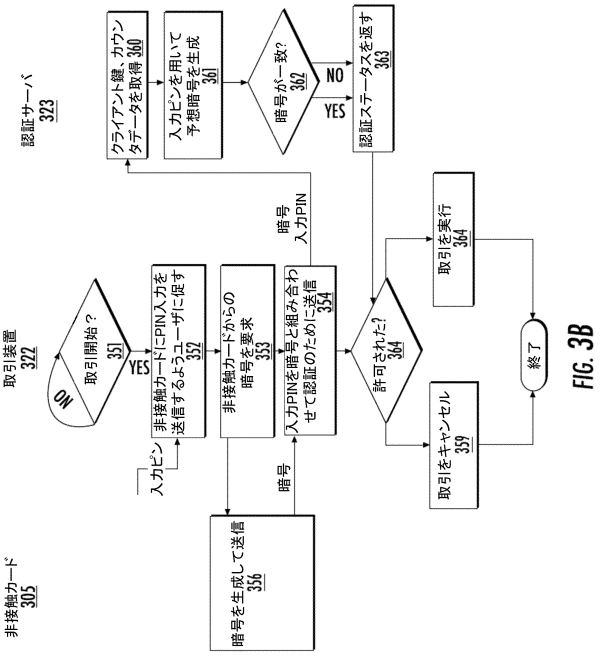


FIG. 3B

【図４Ａ】

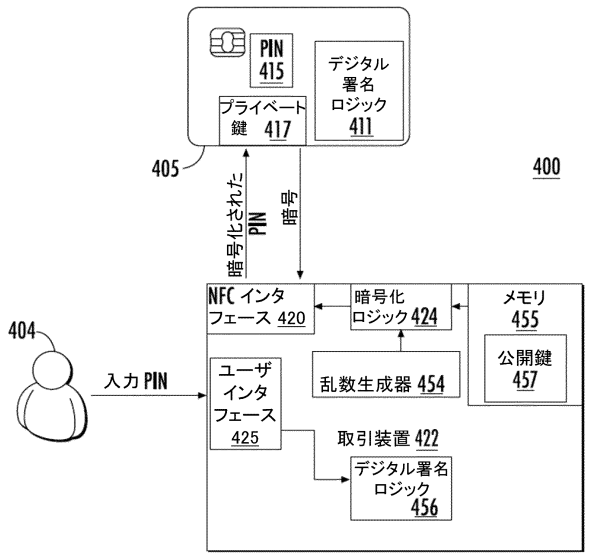


FIG. 4A

【図４Ｂ】

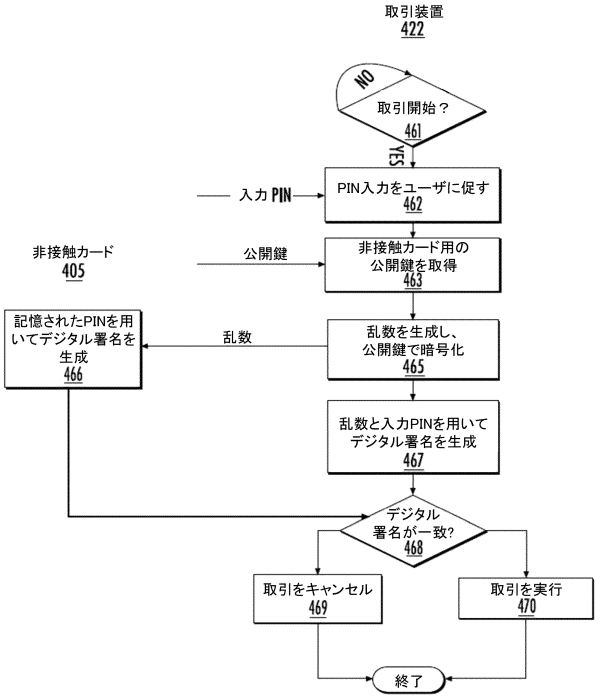


FIG. 4B

【図５Ａ】

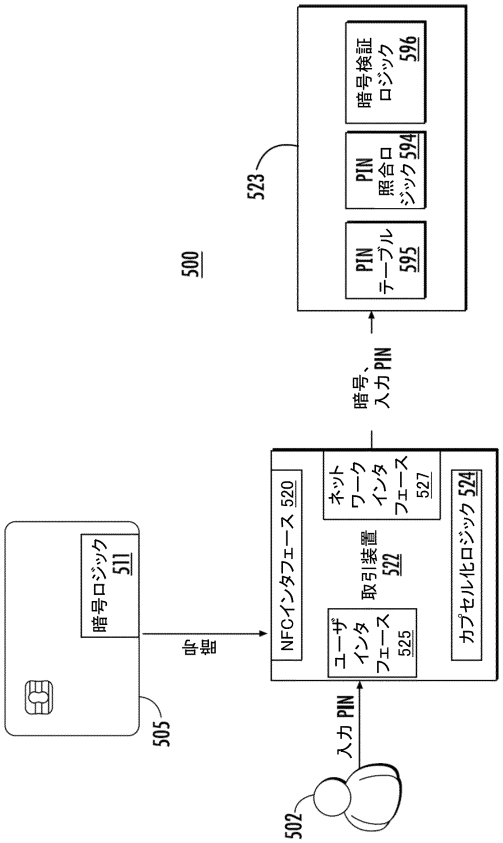


FIG. 5A

【図５Ｂ】

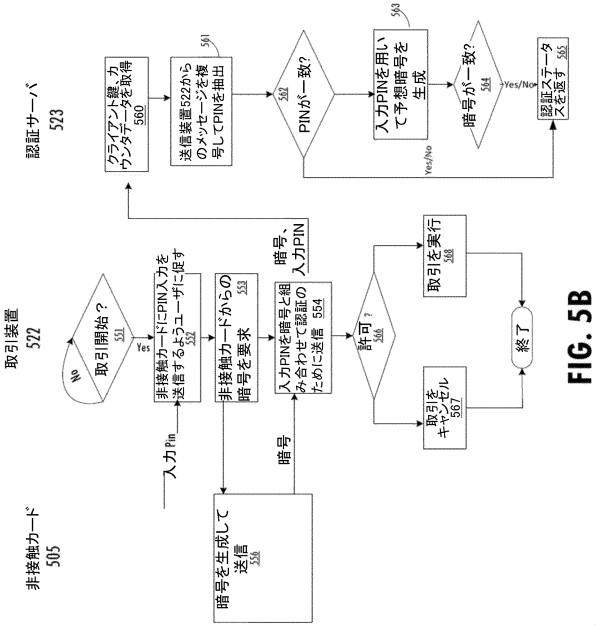


FIG. 5B

【図６】

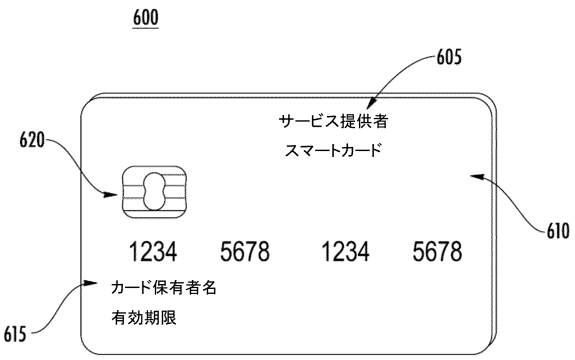


FIG. 6

【図７】

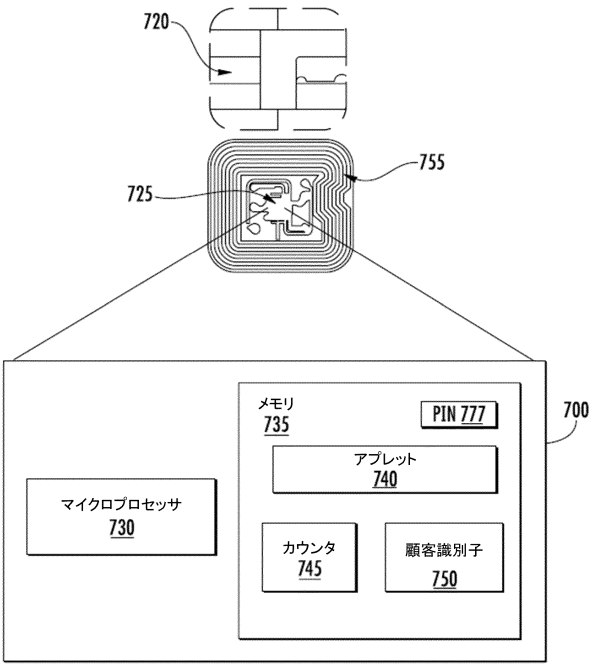


FIG. 7

【図８】

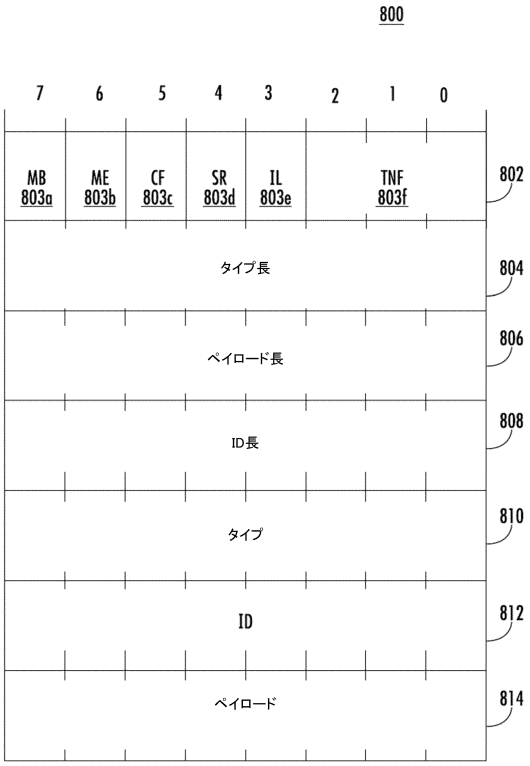


FIG. 8

【図９】

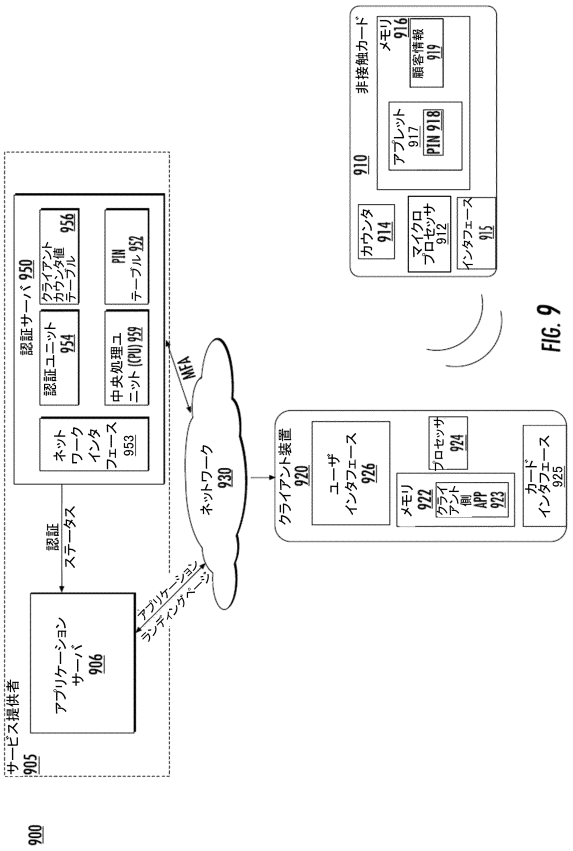


FIG. 9

【図１０】

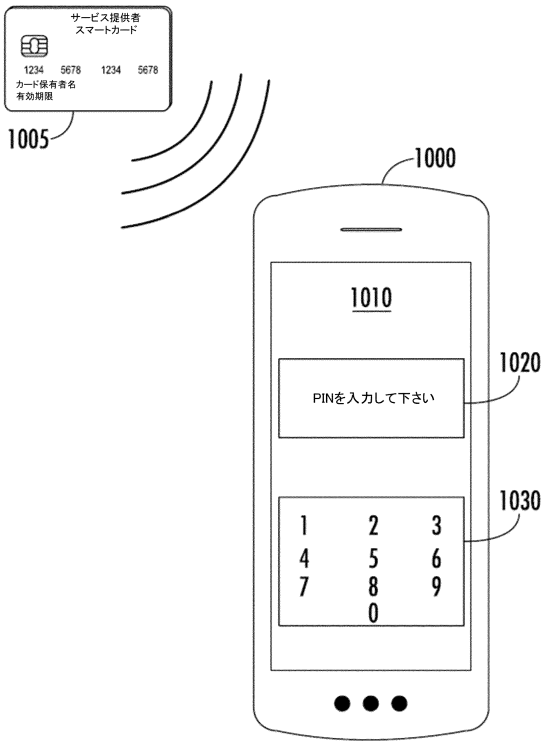


FIG. 10

フロントページの続き

アメリカ合衆国２２１０２バージニア州マクリーン、キャピタル・ワン・ドライブ１６８０、キャピタル・ワン・サービシーズ・リミテッド・ライアビリティ・カンパニー内
(72)発明者　チグルパティ，スリニバサ
アメリカ合衆国２２１０２バージニア州マクリーン、キャピタル・ワン・ドライブ１６８０、キャピタル・ワン・サービシーズ・リミテッド・ライアビリティ・カンパニー内
(72)発明者　ルール，ジェフリー
アメリカ合衆国２２１０２バージニア州マクリーン、キャピタル・ワン・ドライブ１６８０、キャピタル・ワン・サービシーズ・リミテッド・ライアビリティ・カンパニー内

審査官　金沢 史明
(56)参考文献　特表２０１７－５２４３１２（ＪＰ，Ａ）
特開２０１８－１４７１４６（ＪＰ，Ａ）
特開２００７－２４９６５４（ＪＰ，Ａ）
韓国公開特許第１０－２０１６－００１９６５３（ＫＲ，Ａ）
米国特許出願公開第２０１９／０２１３５９３（ＵＳ，Ａ１）
米国特許出願公開第２０１５／０１３４５４２（ＵＳ，Ａ１）
米国特許出願公開第２０１３／０１４４７９２（ＵＳ，Ａ１）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／３２
Ｇ０６Ｆ　２１／３０－２１／４６