(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7684916号
(P7684916)

(45)発行日　令和7年5月28日(2025.5.28)

(24)登録日　令和7年5月20日(2025.5.20)

(51)国際特許分類
Ｇ０６Ｆ　21/35　(2013.01)
Ｇ０６Ｑ　20/40　(2012.01)

ＦＩ
Ｇ０６Ｆ　21/35
Ｇ０６Ｑ　20/40

請求項の数　20　（全34頁）

(21)出願番号　特願2021-577912(P2021-577912)
(86)(22)出願日　令和2年6月30日(2020.6.30)
(65)公表番号　特表2022-538649(P2022-538649A)
(43)公表日　令和4年9月5日(2022.9.5)
(86)国際出願番号　PCT/US2020/040261
(87)国際公開番号　WO2021/003137
(87)国際公開日　令和3年1月7日(2021.1.7)
審査請求日　令和5年6月27日(2023.6.27)
(31)優先権主張番号　16/503,142
(32)優先日　令和1年7月3日(2019.7.3)
(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
(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
最終頁に続く

(54)【発明の名称】　非接触型カードの取引機能の制限

(57)【特許請求の範囲】
【請求項１】
非接触型カードであって、
プロセッサ回路と、
通信インタフェースと、
メモリとを備え、前記メモリが格納する命令は、前記プロセッサ回路により実行されると、前記プロセッサ回路に、以下を行わせる：
前記通信インタフェースを介して、モバイルデバイス上で実行されるアカウントアプリケーションから、サーバがモバイルデバイスの位置を示す位置データと暗号化データの復号とに基づいて決済取引を事前に承認したことのインジケーションを受信する、ここで、前記暗号化データは、前記非接触型カードのメモリに格納された暗号アルゴリズムおよび鍵を使用して前記非接触型カードによって生成され、前記インジケーションはさらに、前記非接触型カードに関連付けられたアカウントのための１つまたは複数の資格情報が前記アカウントアプリケーションによって受信されたことを特定する；
前記通信インタフェースを介して、販売時点情報管理（ＰＯＳ）デバイスから、前記非接触型カードを使用して取引の支払いをするインジケーションを受信する；
前記メモリに格納された１つまたは複数の規則に基づいて、前記モバイルデバイスの位置が、前記非接触型カードの使用が許可されている１つまたは複数の位置の閾値距離内にあることを判断する；
（ｉ）前記非接触型カードに関連付けられたアカウント番号、カード照合値（ＣＶＶ

）および有効期限のインジケーションと、ここで、前記アカウント番号、前記ＣＶＶおよび前記有効期限の各インジケーションは、前記決済取引に関連付けられた決済取引データの１つまたは複数の第１の部分に書き込まれる、（ｉｉ）前記決済取引に関連付けられた前記決済取引データの第２の部分に書き込まれる、前記サーバによる前記決済取引の事前承認のインジケーションとを含む取引データを生成する；

前記取引の支払いとして、前記決済取引データに含まれる前記取引データを前記ＰＯＳデバイスに送信する；

前記ＰＯＳデバイスから、前記サーバが前記取引データの少なくとも一部を使用して、および前記取引データにおける前記サーバによる取引の事前承認のインジケーションを識別することに少なくとも部分的に基づいて、取引の支払いを承認するインジケーションを受信する

非接触型カード。

【請求項２】

前記メモリは、前記プロセッサ回路によって実行されると前記プロセッサ回路に以下を行わせる命令を格納している：

前記アカウントアプリケーションから受信された前記位置データのインジケーションを前記決済取引データの前記１つまたは複数の第１の部分に書き込む、ここで、前記決済取引は、ＥＭＶ取引に対応し、前記決済取引データは、ＥＭＶ取引データに対応する

請求項１に記載の非接触型カード。

【請求項３】

前記メモリは、認可アプレットおよび決済アプレットを格納しており、

前記認可アプレットは、前記モバイルデバイスの位置が、前記非接触型カードの使用が許可されている１つまたは複数の位置の閾値距離内にあることを判断し、

前記認可アプレットは、前記モバイルデバイスから、前記サーバによる取引の事前承認のインジケーションを受信し、

前記認可アプレットは、前記非接触型カードに関連付けられた顧客ＩＤに基づいて、前記暗号化データを生成し、

前記決済アプレットは、前記ＥＭＶ取引データを生成し、前記認可アプレットからの承認の受信に応答して、前記ＥＭＶ取引データを前記ＰＯＳデバイスに送信し、

前記認可アプレットは、前記モバイルデバイスから受信した前記サーバによる取引の事前承認のインジケーションと、前記モバイルデバイスの位置が前記非接触型カードの使用が許可されている１つまたは複数の位置の閾値距離内にあることの判断とに基づいて、前記決済アプレットに承認を提供する

請求項２に記載の非接触型カード。

【請求項４】

前記メモリは、前記プロセッサ回路によって実行されると前記プロセッサ回路に以下を行わせる命令を格納している：

前記通信インタフェースを介して、前記モバイルデバイス上で実行されるアカウントアプリケーションから、前記モバイルデバイスを使用してアカウントの多要素認証が完了したことのインジケーションを受信する、ここで、前記多要素認証は、（ｉ）前記アカウントのログインとパスワード、（ｉｉ）前記アカウントに関連付けられた電話番号に送信されたワンタイムパスワード、（ｉｉｉ）前記アカウントに関連付けられた生体認証情報、（ｉｖ）認証アプリケーションによって生成された一時的なコード、および（ｖ）非接触型カードによって生成されたデータ、の少なくとも２つに基づく

請求項３に記載の非接触型カード。

【請求項５】

前記メモリは、前記プロセッサ回路によって実行されると前記プロセッサ回路に以下を行わせる命令を格納している：

前記取引のための承認のインジケーションを前記ＰＯＳデバイスに送信する前に、

前記モバイルデバイスの位置が、前記ＰＯＳデバイスの位置を示す位置データの閾値

距離内にあると前記サーバが判断したことを特定するインジケーションを受信する
　前記ＥＭＶ取引データの前記第１の部分における前記サーバによる取引の事前承認のインジケーションに基づいて前記取引が事前承認されたと前記サーバが認証したことを特定するインジケーションを受信する
請求項３に記載の非接触型カード。
【請求項６】
　前記メモリは、前記プロセッサ回路によって実行されると前記プロセッサ回路に以下を行わせる命令を格納している：
　前記認可アプレットにより、前記通信インタフェースを介して、前記モバイルデバイスから、前記モバイルデバイスの更新された位置を示す更新された位置データを受信する、ここで、前記更新された位置は、前記位置とは異なる；
　前記認可アプレットにより、前記メモリに格納された１つまたは複数の規則に基づいて、前記モバイルデバイスの位置が、前記非接触型カードの使用が許可されている１つまたは複数の位置の閾値距離内にないことを判断する；
　前記決済アプレットにより、第２のＰＯＳデバイスから、前記非接触型カードを使用して第２の取引の支払いを行うインジケーションを受信する；
　前記決済アプレットは、前記認可アプレットに、前記第２の取引の支払いの承認を要求する；
　前記認可アプレットにより、前記モバイルデバイスの位置が、前記非接触型カードの使用が許可されている１つまたは複数の位置の閾値距離内にないという判断に基づいて、前記第２の取引に対する支払いの承認を拒否する；
　前記決済アプレットにより、前記認可アプレットによる拒否に基づいて、前記非接触型カードを使用した前記第２の取引の支払いを拒否するインジケーションを、前記第２のＰＯＳデバイスに送信する
請求項３に記載の非接触型カード。
【請求項７】
　前記取引データにおける前記サーバによる前記取引の事前承認のインジケーションは、前記サーバによる前記取引の事前承認の異なるインジケーションを含み、前記非接触型カードの通信インタフェースは、近距離無線通信（ＮＦＣ）、Ｂｌｕｅｔｏｏｔｈ、およびＷｉ－Ｆｉのうちの少なくとも１つをサポートするように構成されており、前記メモリは、前記プロセッサ回路によって実行されると前記プロセッサ回路に以下を行わせる命令を格納している：
　前記取引に関連付けられた現在の時刻を受信する；
　前記メモリに格納された１つまたは複数の規則に基づいて、前記現在の時刻が、前記非接触型カードの使用が許可された時間内であることを判断する；
　前記ＰＯＳデバイスから、前記取引の金額のインジケーションを受信する；
　前記メモリに格納された１つまたは複数の規則に基づいて、前記取引の金額が、前記非接触型カードに関連付けられた最大支出額よりも小さいことを判断する
請求項１に記載の非接触型カード。
【請求項８】
　サーバのプロセッサによって実行されると前記プロセッサに以下を行わせる命令を格納した非一時的なコンピュータ可読記憶媒体であって、
　モバイルデバイス上で実行されるアカウントアプリケーションから暗号化データを受信する；
　暗号アルゴリズムと鍵を用いて前記暗号化データを復号する、ここで、前記鍵は、非接触型カードに関連付けられる；
　アカウントに関連付けられた１つまたは複数の規則に基づいて、前記モバイルデバイスから受信された位置データが、前記非接触型カードの使用が許可されている１つまたは複数の位置の閾値距離内にあることを判断する；
　前記暗号化データの復号と、前記モバイルデバイスが、前記非接触型カードの使用が許

可されている１つまたは複数の位置の閾値距離内にあることの判断とに基づいて、前記非接触型カードを使用する決済取引を事前承認する；
前記アカウントアプリケーションに、前記決済取引に対する事前承認のインジケーションを送信する；
販売時点情報管理（ＰＯＳ）デバイスから、（ｉ）前記非接触型カードのアカウント番号、カード照合値（ＣＶＶ）および有効期限のインジケーションと、（ｉｉ）前記ＰＯＳデバイスにより前記非接触型カードから受信された前記決済取引の事前承認のインジケーションのインスタンスとを含む取引データを受信する；
前記決済取引に関連付けられた決済取引データの第１の部分における前記決済取引の事前承認のインジケーションのインスタンスを特定する；
前記決済取引に関連付けられた前記決済取引データの１つまたは複数の第２の部分における前記アカウント番号、前記ＣＶＶ、および前記有効期限の各インジケーションを特定する；
前記取引データにおいて、前記サーバによる取引の事前承認のインジケーションを特定することに少なくとも部分的に基づいて、前記取引を承認する
非一時的なコンピュータ可読記憶媒体。
【請求項９】
前記決済取引は、ＥＭＶ取引に対応し、前記取引データは、ＥＭＶ取引データを含む
請求項８に記載の非一時的なコンピュータ可読記憶媒体。
【請求項１０】
前記プロセッサによって実行されると前記プロセッサに以下を行わせる命令を格納している：
前記事前承認のインジケーションを格納する；
前記格納された取引の事前承認のインジケーションを、前記ＥＭＶ取引データの前記第１の部分における前記取引の事前承認のインジケーションのインスタンスと比較する；
一致する前記比較の結果を決定する；
前記ＰＯＳデバイスに前記取引に対する承認のインジケーションを送信する
請求項９に記載の非一時的なコンピュータ可読記憶媒体。
【請求項１１】
前記事前承認は、事前承認の１つまたは複数のレベルを含み、事前承認の前記レベルは、（ｉ）前記サーバが前記鍵のコピーおよび前記暗号アルゴリズムを使用して、前記暗号化データを復号すること、および（ｉｉ）前記モバイルデバイスから受信された位置データが、前記非接触型カードの使用が許可されている１つまたは複数の位置の閾値距離内にあることを判断すること、に基づく
請求項１０に記載の非一時的なコンピュータ可読記憶媒体。
【請求項１２】
前記プロセッサによって実行されると前記ＰＯＳデバイスに前記取引に対する承認のインジケーションを送信する前に、前記プロセッサに以下を行わせる命令を格納している：
前記ＰＯＳデバイスから、前記ＥＭＶ取引データ、および前記ＰＯＳデバイスの位置を示す位置データを受信する；
前記モバイルデバイスの位置が前記ＰＯＳデバイスの位置から前記閾値距離内にあると判断する
請求項１１に記載の非一時的なコンピュータ可読記憶媒体。
【請求項１３】
前記プロセッサによって実行されると前記プロセッサに以下を行わせる命令を格納している：
前記取引に関連付けられた現在の時刻を受信する；
前記アカウントに関連付けられた１つまたは複数の規則に基づいて、前記現在の時刻が、前記非接触型カードの使用を許可された時間内であることを判断する
請求項１１に記載の非一時的なコンピュータ可読記憶媒体。

【請求項１４】
前記事前承認のインジケーションは、事前承認の複数のインジケーションの１つであり、事前承認の各インジケーションは、前記取引を含む複数の取引の各取引のためであり、事前承認の各インジケーションは、事前承認の前記各々のインジケーションに固有の識別子をさらに含み、
前記非一時的なコンピュータ可読記憶媒体は、前記プロセッサによって実行されると前記プロセッサに以下を行わせる命令を格納している：
前記ＰＯＳデバイスから前記取引の金額のインジケーションを受信する；
前記アカウントに関連付けられた１つまたは複数の規則に基づいて、前記取引の金額が前記非接触型カードに関連付けられた最大支出額よりも小さいことを判断する
請求項８に記載の非一時的なコンピュータ可読記憶媒体。
【請求項１５】
方法であって、
サーバが、モバイルデバイス上で実行されるアカウントアプリケーションから、暗号化データを受信すること；
前記サーバが、暗号アルゴリズムと鍵を用いて前記暗号化データを復号すること、ここで、前記鍵は、非接触型カードに関連付けられる；
前記サーバが、アカウントに関連付けられた１つまたは複数の規則に基づいて、前記モバイルデバイスから受信された位置データが、前記非接触型カードの使用が許可されている１つまたは複数の位置の閾値距離内にあることを判断すること；
前記暗号化データの復号と、前記モバイルデバイスが、前記非接触型カードの使用が許可されている１つまたは複数の位置の閾値距離内にあることの判断とに基づいて、前記サーバが、前記非接触型カードを使用する決済取引を事前承認すること；
前記サーバが、前記アカウントアプリケーションに、前記決済取引に対する事前承認のインジケーションを送信すること；
前記サーバが、販売時点情報管理（ＰＯＳ）デバイスから、（ｉ）前記非接触型カードのアカウント番号、カード照合値（ＣＶＶ）および有効期限のインジケーションと、（ｉｉ）前記ＰＯＳデバイスにより前記非接触型カードから受信された前記決済取引の事前承認のインジケーションのインスタンスとを含む取引データを受信すること；
前記サーバが、前記決済取引に関連付けられた決済取引データの第１の部分における前記決済取引の事前承認のインジケーションのインスタンスを特定すること；
前記サーバが、前記決済取引に関連付けられた前記決済取引データの１つまたは複数の第２の部分における前記アカウント番号、前記ＣＶＶ、および前記有効期限の各インジケーションを特定すること；
前記取引データにおいて、前記サーバによる取引の事前承認のインジケーションを特定することに少なくとも部分的に基づいて、前記サーバが取引を承認すること
を含む、方法。
【請求項１６】
前記決済取引は、ＥＭＶ取引に対応し、前記取引データは、ＥＭＶ取引データを含む
請求項１５に記載の方法。
【請求項１７】
さらに、
前記サーバが、前記事前承認のインジケーションを格納すること；
前記サーバが、前記格納された取引の事前承認のインジケーションを、前記ＥＭＶ取引データの前記第１の部分における前記取引の事前承認のインジケーションと比較すること；
一致する前記比較の結果を決定すること；
前記ＰＯＳデバイスに前記取引に対する承認のインジケーションを送信すること
を含む、請求項１６に記載の方法。
【請求項１８】
前記事前承認は、事前承認の複数のレベルの第１のレベルであり、事前承認の前記複数

のレベルは、前記非接触型カードのアカウント番号とは異なる
請求項１７に記載の方法。
【請求項１９】
さらに、
前記サーバが、（ｉ）前記鍵のコピーおよび前記暗号アルゴリズムを使用して、前記暗号化データを復号すること、（ｉｉ）前記モバイルデバイスから受信された位置データが、前記非接触型カードの使用が許可されている１つまたは複数の位置の閾値距離内にあることを判断すること、（ｉｉｉ）前記アカウントの多要素認証の完了、および（ｉｖ）前記１つまたは複数の規則に基づいて、事前承認の前記第１のレベルを選択すること
を含む、請求項１８に記載の方法。
【請求項２０】
前記事前承認のインジケーションは、事前承認の複数のインジケーションの１つであり、事前承認の各インジケーションは、前記取引を含む複数の取引の各取引のためであり、事前承認の各インジケーションは、事前承認の前記各々のインジケーションに固有の識別子をさらに含み、
前記非接触型カードの通信インタフェースは、近距離無線通信（ＮＦＣ）、Ｂｌｕｅｔｏｏｔｈ、およびＷｉ‐Ｆｉの少なくとも１つをサポートするように構成され、
さらに、前記取引を承認する前に、
前記サーバが、前記取引に関連付けられた現在の時刻を受信すること；
前記サーバが、前記アカウントに関連付けられた１つまたは複数の規則に基づいて、前記現在の時刻が、前記非接触型カードの使用が許可された時間内であることを判断すること；
前記サーバが、前記ＰＯＳデバイスから前記取引の金額のインジケーションを受信すること；
前記サーバが、前記アカウントに関連付けられた１つまたは複数の規則に基づいて、前記取引の金額が前記非接触型カードに関連付けられた最大支出額よりも小さいことを判断すること
を含む、請求項１５に記載の方法。
【発明の詳細な説明】
【関連出願の相互参照】
【０００１】
本出願は、２０１９年７月３日に出願された「非接触型カードの取引機能の制限」と題された米国特許出願第１６／５０３，１４２号の優先権を主張する。前述の特許出願の内容は、参照によりその全体が本明細書に組み込まれる。
【技術分野】
【０００２】
本明細書の実施形態は、概して非接触型カードに関し、より具体的には、非接触型カードの取引機能の制限に関する。
【背景技術】
【０００３】
カード所有者（例えばクレジットカード所有者、銀行カード所有者など）は、家族および従業員などの信頼できる個人のために、追加の物理的なカードおよび／または仮想カード番号を取得することがよくある。しかし、このような場合、セキュリティ上のリスクが生じ得る。従来のソリューションは、物理的なカードおよび／または仮想カード番号が、何らかの定義された制限に従って使用されることを保証するために必要なセキュリティメカニズムを提供していない。
【発明の概要】
【０００４】
本明細書に開示される実施形態は、非接触型カードの取引機能を制限するシステム、方法、製造品、およびコンピュータ可読媒体を提供する。一例では、通信インタフェースは

、アカウントアプリケーションを実行するモバイルデバイスから、モバイルデバイスの位置を記述する位置データおよび暗号化データの認証に基づいてサーバが取引を事前に承認したというインジケーションを受信し得る。暗号化データは、暗号アルゴリズムと非接触型カードのメモリに格納された秘密鍵を使用して非接触型カードによって生成され、非接触型カードに関連付けられたアカウントに関する１つまたは複数の資格情報が、アカウントアプリケーションによって受信される。通信インタフェースは、販売時点情報管理（ＰＯＳ）デバイスから、非接触型カードを使用して取引の決済を行うためのインジケーションを受信し得る。非接触型カードは、メモリに格納された１つまたは複数の規則に基づいて、モバイルデバイスの位置が、非接触型カードの使用が許可された１つまたは複数の位置の閾値距離内にあることを決定し得る。非接触型カードは、（ｉ）アカウント番号と非接触型カードの有効期限のインジケーション、および（ｉｉ）サーバによる取引の事前承認のインジケーションを含む取引データを生成してもよい。非接触型カードは、取引の決済として取引データをＰＯＳデバイスに送信してもよく、サーバは、取引データにおいてサーバによる取引の事前承認のインジケーションを識別することに少なくとも部分的に基づいて、取引データの少なくとも一部を使用して取引の決済を承認する。

【図面の簡単な説明】

【０００５】

【図１Ａ】図１Ａは非接触型カードの取引機能を制限するシステムの実施形態を示す。

【図１Ｂ】図１Ｂは非接触型カードの取引機能を制限するシステムの実施形態を示す。

【図１Ｃ】図１Ｃは非接触型カードの取引機能を制限するシステムの実施形態を示す。

【図１Ｄ】図１Ｄは非接触型カードの取引機能を制限するシステムの実施形態を示す。

【図２Ａ】図２Ａは非接触型カードの取引機能を制限するシステムの実施形態を示す。

【図２Ｂ】図２Ｂは非接触型カードの取引機能を制限するシステムの実施形態を示す。

【図３Ａ】図３Ａは非接触型カードの取引機能を制限するシステムの実施形態を示す。

【図３Ｂ】図３Ｂは非接触型カードの取引機能を制限するシステムの実施形態を示す。

【図３Ｃ】図３Ｃは非接触型カードの取引機能を制限するシステムの実施形態を示す。

【図３Ｄ】図３Ｄは非接触型カードの取引機能を制限するシステムの実施形態を示す。

【図４】図４は第１論理フローの実施形態を示す。

【図５】図５は第２論理フローの実施形態を示す。

【図６】図６は第３論理フローの実施形態を示す。

【図７】図７は第４論理フローの実施形態を示す。

【図８】図８は第５論理フローの実施形態を示す。

【図９】図９はコンピューティングアーキテクチャの実施形態を示す。

【図１０Ａ】図１０Ａは非接触型カードの例を示す。

【図１０Ｂ】図１０Ｂは非接触型カードの例を示す。

【発明を実施するための形態】

【０００６】

本明細書に開示される実施形態は、非接触型カードの取引機能を制限するための安全な技術を提供する。一般に、非接触型カードは、非接触型カードの使用に関する制限を含むようにプログラム可能である。制限には、地理的（または位置）制限、金額制限、および／または時間制限が含まれ得る。カード所有者が非接触型カードを使用しようとすると、非接触型カードのロジックによって、制限に照らして使用が許可されているかどうかが判断され得る。たとえば、非接触型カードは、アカウント管理アプリケーションを実行するモバイルデバイスと定期的に通信する場合がある。非接触型カードは、アカウント管理アプリケーションから定期的に位置データを受信し得る。位置データは、モバイルデバイス（および／または非接触型カード）の位置を示す。カード所有者が非接触型カードを使用しようとすると、非接触型カードのロジックによって、受信した位置データが、非接触型カードの使用が許可されている１つ以上の地理的位置にあるかどうかが判断され得る。たとえば、非接触型カードは、カード所有者の自宅から半径５マイルでの使用に制限される場合がある。受信した位置データがモバイルデバイスおよび／または非接触型カードが自

宅から１０マイル離れていることを示している場合、非接触型カードは試行された取引の処理を拒否する可能性がある。同様に、位置データが、モバイルデバイスおよび／または非接触型カードが自宅から１マイル離れていることを示している場合、非接触型カードは試行された取引を許可し得る。

【０００７】

いくつかの実施形態では、位置データは、取引の事前承認プロセスの一部として使用され得る。たとえば、ユーザは、時計などの高価な商品を購入する際に、アカウントアプリケーションを実行するモバイルデバイスに非接触型カードをタップして、高額な取引を事前承認（preauthorize）できる。アカウントアプリケーションは、非接触型カードによって生成された暗号化データを受信し得る。アカウントアプリケーションは、モバイルデバイスの現在の位置を記述する暗号化データおよび位置データをサーバに送信し得る。サーバは暗号化データを復号し、それによって暗号化データを認証（validate）し得る。サーバはさらに、位置データが、モバイルデバイスおよび／または非接触型カードが非接触型カードの使用が許可されている１つまたは複数の位置内にあることを示していると判断し得る。同様に、サーバは、事前承認のために要求された購入金額および／または期間を認証し得る。サーバは、非接触型カードを使用して取引を事前承認し、事前承認のインジケーションをモバイルデバイスで実行されているアカウントアプリケーションに送信することを決定し得る。事前承認のインジケーションは、モバイルデバイスから非接触型カードに送信され得る。非接触型カードは、カードが取引の決済に使用されていると判断した場合、販売時点情報管理（ＰＯＳ）デバイスに送信される決済ペイロードの１つまたは複数のフィールドに事前承認のインジケーションを書き込み得る。ＰＯＳデバイスは、事前承認のインジケーションを含む決済ペイロードをサーバに送信し得る。サーバは、決済ペイロードにおける事前承認のインジケーションを識別することに少なくとも部分的に基づいて、取引の決済を承認できる。サーバは、購入が試みられた際の非接触型カードのタップに応答して、モバイルデバイスから受信したデータ（例えば、要求された購入金額、時間、位置など）をさらに認証し得る。その後、サーバは承認のインジケーションをＰＯＳデバイスに送信し得る。

【０００８】

有利なことに、本明細書に開示される実施形態は、すべてのデバイスおよび関連するデータのセキュリティを改善する。たとえば、事前承認技術は、非接触型カードの不正および／またはセキュリティリスクを軽減し得る。別の例として、サーバによって実行される認証は、許可されたユーザが物理カードにアクセスできることを保証するためのセーフガードを提供する。さらに、物理カードおよび／または仮想アカウント番号の使用に関連する規則を適用することにより、関連するアカウントのセキュリティが維持される。

【０００９】

本明細書で使用される表記法および用語体系を一般的に参照して、以下の詳細な説明の１つまたは複数の部分は、コンピュータまた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に関して提示され得る。これらの手順の説明および表現は、当業者が自己の業績の要旨を他の当業者に最も効果的に伝えるために使用される。手順は本明細書にあって、一般に、望ましい結果につながる自己矛盾のない一連の操作であると考えられる。これらの操作は、物理量の物理的な操作を必要とする操作である。通常、必須ではないが、これらの量は、保存、転送、結合、比較、およびその他の方法で操作できる電気信号、磁気信号、または光信号の形をとる。主に一般的な使用法の理由から、これらの信号をビット、値、要素、記号、文字、用語、数値などとして言及すると便利な場合がある。ただし、これらおよび類似の用語はすべて、適当な物理量に関連付けられており、これらの量に適用される便利なラベルにすぎない。

【００１０】

さらに、これらの操作は、加算または比較など、一般に人間の知的活動に関連付けられた用語で呼ばれることが多い。しかしながら、１つまたは複数の実施形態の一部を形成する、本明細書に記載の操作のいずれにおいても、人間の操作者のそうした能力は必須では

なく、ほとんどの場合、望ましくもない。むしろ、これら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、その内部に格納されて本明細書における教示に従って書かれたコンピュータプログラムによって、選択的に起動または構成されるデジタルコンピュータを含み、および／または必要な目的のために特別に構築された装置またはデジタルコンピュータを含む。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またはシステムに関する。これらの装置は、必要な目的のために特別に構築されてもよい。これらの様々な機械に必要な構造は、与えられる説明から明らかになる。

【００１１】

図面を参照して、ここで、同様の参照符合は、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、それらを完全に理解するために、多くの具体的な詳細が示されている。しかしながら、これらの特定の詳細なしで新規の実施形態を実施できることは明らかであろう。他の例では、よく知られている構造およびデバイスは、それらの説明を容易にするためにブロック図の形で示されている。特許請求の範囲内のすべての変更、均等物、および代替案を対象とすることが意図される。

【００１２】

図１Ａは、開示された実施形態と一致する、例示的なシステム１００の概略図を示している。図示されるように、システム１００は、１つまたは複数の非接触型カード１０１、１つまたは複数のモバイルデバイス１１０、サーバ１２０、および１つまたは複数のＰＯＳデバイス１４０を含む。非接触型カード１０１は、クレジットカード、デビットカード、ＡＴＭカード、ギフトカードなど、任意のタイプの決済カードを代表する。非接触型カード１０１は、ＮＦＣ、ＥＭＶ規格、または無線通信における他の短距離プロトコルを介して、モバイルデバイス１１０の通信インタフェース１０５－１と通信するように構成された、無線自動識別（ＲＦＩＤ）チップなどの１つまたは複数の通信インタフェース１０５－２を備え得る。通信プロトコルの例としてＮＦＣが使用されているが、本開示は、ＥＭＶ規格、Ｂｌｕｅｔｏｏｔｈ（登録商標）、および／またはＷｉ‐Ｆｉ（登録商標）などの他のタイプの無線通信にも同様に適用可能である。モバイルデバイス１１０は、スマートフォン、タブレットコンピュータ、ウェアラブルデバイス、ラップトップ、ポータブルゲームデバイス、モバイルデバイスなどのあらゆるタイプのネットワーク対応コンピューティングデバイスの代表である。サーバ１２０は、サーバ、ワークステーション、コンピュータクラスタ、クラウドコンピューティングプラットフォーム、仮想化コンピューティングシステムなどの任意のタイプのコンピューティングデバイスを代表する。ＰＯＳデバイス１４０は、カードリーダーデバイス、スマートフォン、タブレットコンピュータ、デスクトップコンピュータ、ＰＯＳ端末、サーバ、ワークステーション、ラップトップコンピュータなどの、決済を処理するための任意のタイプのデバイスの代表である。

【００１３】

図示されるように、モバイルデバイス１１０のメモリ１１１は、アカウントアプリケーション１１３のインスタンスを含む。アカウントアプリケーション１１３により、ユーザは、アカウント残高の表示、商品の購入、決済の処理、非接触型カード１０１の制限の定義、非接触型カード１０１への位置データの通信、および事前承認のためのサーバ１２０との通信など、様々なアカウント関連の操作を行うことができる。最初に、ユーザは、アカウントアプリケーション１１３の特定の機能にアクセスするために、認証資格情報（authentication credentials）を使用して認証し得る。例えば、認証資格情報は、ユーザ名およびパスワード、生体認証資格情報（例えば、指紋、フェイスＩＤなど）などを含み得る。いくつかの実施形態では、ユーザは、認証資格情報に加えて、追加の認証（例えば、多要素認証）を行うことができる。例えば、ユーザは、テキストメッセージで受信したワンタイムパスコード、アカウントに関連付けられた生体認証資格情報、および／または認証アプリケーション（図示せず）によって生成された一時的なコードをアカウントアプリケーション１１３に提供してもよい。いくつかの実施形態では、非接触型カード１０１は、追加の認証要素として使用される暗号化データ１０８を生成して送信してもよい。いくつかの実施形態では、アカウントアプリケーション１１３は、非接触型カード１０１に、

ユーザが認証資格情報を使用して認証されたことを特定するインジケーションを送信してもよい。

【００１４】

ユーザがアカウントアプリケーション１１３において自分のアカウントに認証されると、アカウントアプリケーション１１３は、位置モジュール１１４から位置データを受信し得る。位置データは、一般に、モバイルデバイス１１０の位置を記述し得る。位置モジュール１１４は、全地球測位システム（ＧＰＳ）モジュール、全地球的航法衛星システム（ＧＮＳＳ）モジュール、ガリレオモジュールなど、位置を決定する任意のデバイスであり得る。いくつかの実施形態では、ネットワークインタフェース１１２は、（例えば、セルラーネットワーク信号、タワーの位置などに基づき）モバイルデバイスの位置を記述する位置データを提供し得る。アカウントアプリケーション１１３は、通信インタフェース１０５－１、１０５－２を介して、生成された位置データを非接触型カード１０１に周期的に提供し得る。以下でより詳細に説明するように、非接触型カード１０１は、位置データを使用して、非接触型カード１０１の取引機能を制限し得る。例えば、非接触型カード１０１の規則１０７－１は、非接触型カード１０１が取引の決済に使用され得る１つまたは複数の位置を指定してもよい。受信した位置データが、規則１０７－１で指定された１つまたは複数の位置範囲内（および／または１つまたは複数の位置の閾値距離内）にない場合、非接触型カード１０１は、取引の決済のためのデータの生成および／またはＰＯＳデバイス１４０へのデータの送信を控えることができる。

【００１５】

一実施形態では、ユーザは、非接触型カード１０１を使用した購入のための事前承認を得ることを望む場合がある。例えば、ユーザは、宝石店で非接触型カード１０１を使用して高価な宝石を購入することを望む場合がある。事前承認を受けるために、ユーザは、一般に、モバイルデバイス１１０のロックを解除し、アカウントアプリケーション１１３で認証を行い得る。いくつかの実施形態では、事前承認ページは、アカウントアプリケーション１１３のページではなく、別のアプリケーションの一部であってもよい。応答して、アカウントアプリケーション１１３は、非接触型カード１０１をモバイルデバイス１１０にタップすることを指定する通知をモバイルデバイス１１０に出力してもよく、それによって、非接触型カード１０１の通信インタフェース１０５－２とモバイルデバイス１１０の通信インタフェース１０５－１との間のデータ転送（例えば、ＮＦＣデータ転送、Ｂｌｕｅｔｏｏｔｈデータ転送など）を可能にするように、非接触型カード１０１をモバイルデバイス１１０の通信インタフェース１０５－１に十分に近づけさせる。そして、非接触型カード１０１のプロセッサ（図示せず）上で実行される認可（authorization）アプレット１０４は、暗号化データ１０８を生成して、通信インタフェース１０７を介してモバイルデバイス１１０に送信し得る。非接触型カード１０１の認可アプレット１０４は、暗号アルゴリズムを使用して、非接触型カード１０１のメモリ１０２に格納された秘密鍵に少なくとも部分的に基づいて、暗号化データ１０８の暗号ペイロードを生成してもよい。そのような実施形態では、秘密鍵と他のデータ（例えば、顧客識別子、アカウント識別子など）が、暗号化データ１０８を出力する暗号アルゴリズムに入力として提供されてもよい。一般に、認可アプレット１０４は、任意のタイプの暗号アルゴリズムおよび／またはシステムを使用して暗号化データ１０８を生成でき、本明細書の例として特定の暗号アルゴリズムを使用することは、本開示を限定するとみなされるべきではない。いくつかの実施形態において、認可アプレット１０４は、暗号化データ１０８を生成するために、鍵多様化（key diversification）技術を使用して暗号化を実行してもよい。鍵多様化技術の例は、２０１８年１１月２９日に出願された米国特許出願１６／２０５，１１９に記載されている。前述の特許出願は、その全体が参照により本明細書に組み込まれる。一実施形態では、認可アプレット１０４は、ユーザがアカウント資格情報を使用して自分のアカウントに認証されたことを指定する、アカウントアプリケーション１１３から受信したインジケーションに少なくとも部分的に基づいて、暗号化データ１０８を生成する。

【００１６】

いくつかのそのような実施形態では、認可アプレット１０４は、直近に受信された位置データが、非接触型カード１０１の使用が許可された位置として規則１０７－１で指定された１つまたは複数の位置内にあるかどうかを判断する。位置データが規則１０７－１で指定された１つまたは複数の位置内にある場合、認可アプレット１０４は、暗号化データ１０８を生成し得る。位置データが規則１０７－１で指定された１つまたは複数の位置内にない場合、セキュリティを維持するために、認可アプレット１０４は、暗号化データ１０８の生成を控えることができる。さらに、認可アプレット１０４は、暗号化データ１０８を生成するかどうかを決定する際に、規則１０７－１の他の規則を適用してもよい。例えば、規則１０７－１は、非接触型カード１０１を使用できる時間を指定してもよい（例えば、平日の午前８時～午後５時の間、発行から１年以内など）。他の例として、規則１０７－１は、非接触型カード１０１を使用する任意の取引（または複数の取引）の金額制限を指定してもよい。現在の時刻が規則１０７－１で指定された時間内でない場合、認可アプレット１０４は、暗号化データ１０８の生成を控えてもよい。同様に、規則１０７－１で指定された金額の制限を超えて、ユーザがアカウントアプリケーション１１３に事前承認のための金額を提供した場合（非接触型カード１０１に送信され得る）、認可アプレット１０４は、暗号化データ１０８の生成を控えてもよい。

【００１７】

生成されると、認可アプレット１０４は、暗号化データ１０８を、例えばＮＦＣを介して、モバイルデバイス１１０のアカウントアプリケーション１１３に送信し得る。例えば、認可アプレット１０４は、暗号化データ１０８を受信するためにアカウントアプリケーション１１３を起動するように、モバイルデバイス１１０のオペレーティングシステム（ＯＳ、図示せず）に指定するＮＤＥＦタグにおいて、暗号化データ１０８を送信し得る。より一般には、モバイルデバイス１１０と通信するとき、非接触型カード１０１によって生成されたデータは、（例えばインテント属性を介して）アカウントアプリケーション１１３を起動するように指定できる。ＯＳは、非接触型カード１０１からのＮＦＣ信号を検出し、非接触型カード１０１によって送信されたデータを読み取り、アカウントアプリケーション１１３を起動し得る。

【００１８】

アカウントアプリケーション１１３は、暗号化データ１０８および位置モジュール１１４によって生成された位置データ１１５を、サーバ１２０の認可アプリケーション１２３に送信し得る。アカウントアプリケーション１１３は、さらに、事前認証のために要求された金額などの他のデータをサーバ１２０に送信してもよい。認可アプリケーション１２３は、受信した暗号化データ１０８の認証を試み得る。たとえば、認可アプリケーション１２３は、サーバ１２０のメモリ１２２に格納された秘密鍵のコピーを使用して、暗号化データ１０８の復号を試み得る。この秘密鍵は、非接触型カード１０１のメモリ１０２に格納された秘密鍵と同一であってよく、各非接触型カード１０１は、固有の秘密鍵を含むように作られている（そして、サーバ１２０は、各固有の秘密鍵の対応するコピーを格納している）。したがって、認可アプリケーション１２３は、暗号化データ１０８の復号に成功し、それによって、暗号化データ１０８を認証し得る。秘密鍵は、メモリ１２２に格納されると記載されているが、セキュアエレメントおよび／またはハードウェアセキュリティモジュール（ＨＳＭ）など、他の場所に格納されていてもよい。そのような実施形態では、セキュアエレメントおよび／またはＨＳＭは、秘密鍵および暗号関数を使用して、暗号化データ１０８を復号してもよい。

【００１９】

例えば、前述のように、非接触型カード１０１に関連付けられた顧客識別子を使用して、暗号化データ１０８を生成し得る。このような例では、認可アプリケーション１２３は、サーバ１２０の秘密鍵を使用して、暗号化データ１０８を復号し得る。復号の結果、アカウントデータ１２４のアカウントに関連付けられた顧客識別子が生成される場合、認可アプリケーション１２３は、暗号化データ１０８を認証する。認可アプリケーション１２３が暗号化データを復号して期待される結果（たとえば、非接触型カード１０１に関連付

けられたアカウントの顧客識別子）を生成できない場合、認可アプリケーション１２３は暗号化データ１０８を認証しない。認証の失敗により、認可アプリケーション１２３は、要求された取引の事前承認を行わないことがある。

【００２０】

より一般的には、事前承認プロセスの一部として、認可アプリケーション１２３は、位置データ１１５が、非接触型カード１０１の使用が許可された位置としてアカウントのアカウントデータ１２４の規則１０７－２で指定された、１つまたは複数の位置内にあるかどうかを判断してもよい。位置情報が規則１０７－２で指定された１つまたは複数の位置にある場合、認可アプリケーション１２３は取引を事前承認する。位置情報が規則１０７－１で指定された１つまたは複数の位置にない場合、セキュリティを維持するために、認可アプリケーション１２３は取引の事前承認を控え得る。同様に、規則１０７－２における非接触型カード１０１を使用するための時間制限が、事前承認要求に関連付けられた時間によって満たされない場合、認可アプリケーション１２３は、取引の事前認証を控え得る。さらに、取引の金額の制限が、事前認証要求に関連付けられた金額によって満たされない場合、認可アプリケーション１２３は、取引の事前認証を控え得る。

【００２１】

いくつかの実施形態では、認可アプリケーション１２３は、事前承認の結果として、事前承認のバイナリインジケーション（例えば、事前承認された、および／または。事前承認されていない）を返し得る。他の実施形態では、認可アプリケーション１２３は、事前承認結果として、１つまたは複数の事前承認レベルから、事前承認レベルを選択できる。例えば、最高レベルの事前承認は、認可アプリケーション１２３が暗号化データ１０８の復号に成功し、事前承認要求が規則１０７－２の制限に準拠していると判断したときに選択され得る。別の例として、最高レベルの事前承認よりも低い第２のレベルの事前承認は、認可アプリケーション１２３が暗号化データ１０８を正常に復号し、事前承認要求が規則１０７－２の制限の少なくとも１つに準拠していないと判断した場合に選択され得る。別の例として、最高レベルの事前承認よりも低い第３のレベルの事前承認は、認可アプリケーション１２３が暗号化データ１０８の復号に成功せず、事前承認要求が規則１０７－２の制限に準拠していると判断した場合に選択され得る。別の例として、事前承認の最高レベル、第２レベル、および第３レベルよりも低い最低レベルの事前承認は、認可アプリケーション１２３が暗号化データ１０８を正常に復号せず、事前承認要求が規則１０７－２の制限の少なくとも１つに準拠していないと判断した場合に選択され得る。事前承認結果のタイプに関係なく、いくつかの実施形態では、認可アプリケーション１２３は、追加の不正ベクトル（fraud vector）分析を実行し、追加の分析に基づいて取引を事前承認および／または事前承認を拒否してもよい。

【００２２】

図１Ｂに示すように、認可アプリケーション１２３が暗号化データ１０８を認証して事前承認結果を決定すると、認可アプリケーション１２３は、事前承認１３２のインジケーションをモバイルデバイス１１０に送信する。事前承認結果１３２は、関連するタイムスタンプ、受信した位置データ１１５、事前承認額、およびその他の属性をメタデータとして含み得る。認可アプリケーション１２３は、非接触型カードに関連付けられたアカウントのアカウントデータ１２４に、事前承認結果１３２をさらに格納してもよい。受信されると、アカウントアプリケーション１１３は、非接触型カード１０１をタップすることを指定するインジケーションをモバイルデバイス１１０に出力し得る。タップされると、アカウントアプリケーション１１３は、非接触型カード１０１の認可アプレット１０４に事前承認１３２のインジケーションを送信し得る。いくつかの実施形態では、アカウントアプリケーション１１３は、サーバ１２０から受信した事前承認のインジケーション１３２を、非接触型カード１０１の認可アプレット１０４に送信する。他の実施形態では、アカウントアプリケーション１１３は、非接触型カード１０１の認可アプレット１０４に、異なる事前承認１３２のインジケーションを送信する。そして、認可アプレット１０４は、受信した事前承認１３２のインジケーションを非接触型カードのメモリ１０２に格納して

もよい。

【００２３】

ユーザが購入を試みるとき、ユーザは非接触型カード１０１をＰＯＳデバイス１４０の通信インタフェース１０５－３の通信範囲内に持ってくることができる。例えば、ユーザは非接触型カード１０１をＰＯＳデバイス１４０にタップして無線通信させたり、および／または非接触型カードをＰＯＳデバイス１４０のカードリーダーの通信インタフェース１０５－３に挿入したりできる。そして、ＰＯＳデバイス１４０のメモリ１４２内の取引ロジック１４４は、取引データ１４５を非接触型カード１０１に送信し得る。取引データ１４５は、取引の金額、加盟店識別子、ＰＯＳデバイス１４０の位置データ、タイムスタンプなどを含み得る。例えば、取引データ１４５は、ユーザが１，０００ドルの指輪を購入しようとしていることを特定し、宝石商の加盟店識別子、ＰＯＳデバイス１４０および／または宝石商の位置データを含んでもよい。決済アプレット１０６は、取引データ１４５を受信し、認可アプレット１０４に、取引の決済としてカードデータ１０３を提供する承認を要求し得る。

【００２４】

取引を承認するかどうかを決定するために、認可アプレット１０４は、周期的な間隔で取引データ１４５および／またはモバイルデバイス１１０から受信した位置情報データによって規則１０７－１が満たされているかどうかを決定してもよい。たとえば、取引の１０００ドルの金額が規則１０７－１の最大支出額を超えている場合、認可アプレット１０４は、決済アプレット１０６によって要求された承認を拒否し得る。別の例として、モバイルデバイス１１０から受信した位置情報（または取引データ１４５内の位置情報）が、規則１０７－１で指定された位置の外にある場合、認可アプレット１０４は、決済アプレット１０６によって要求された承認を拒否してもよい。さらに、認可アプレット１０４は、取引に対して事前承認１３２が受信されたか否かを判断してもよい。事前承認１３２が受信された場合、認可アプレット１０４は、決済アプレット１０６によって要求された承認を拒否してもよい。いくつかの実施形態では、認可アプレット１０４は、取引データ１４５のタイムスタンプと、事前承認１３２のタイムスタンプとの差が、規則１０７－１で指定された時間閾値を超えているかどうかを判断する。差が時間閾値を超えている場合、認可アプレット１０４は、決済アプレット１０６によって要求された承認を拒否してもよい。

【００２５】

しかし、認可アプレット１０４が、すべての規則１０７－１が満たされていると判断し、および／または、事前承認１３２がサーバ１２０から受信されたと判断した場合、認可アプレット１０４は、決済アプレット１０６によって要求された承認を提供し得る。図１Ｃは、認可アプレット１０４が、決済アプレット１０６によって要求された承認を決済アプレット１０６に提供する実施形態を示す。これに応答して、決済アプレット１０６は、カードデータ１０３および事前承認１３２のインジケーションを含む取引データ１０９を生成し得る。カードデータ１０３は、カード番号（またはアカウント番号）、有効期限、および／またはカード照合値（ＣＶＶ）を含み得る。いくつかの実施形態では、取引のデータ１０９はＥＭＶペイロードである。そのような実施形態では、カードデータ１０３は、ＥＭＶペイロードの１つまたは複数の対応するフィールドに挿入され、事前承認１３２のインジケーションは、ＥＭＶペイロードの１つまたは複数の他のフィールドに格納される。例えば、カード番号は、ＥＭＶペイロードのタグ（またはフィールド）５Ａに格納されてもよく、有効期限は、ＥＭＶペイロードのタグ５９に格納されてもよい。一部の実施形態では、ＣＶＶはＥＭＶペイロードに含まれない。他の実施形態では、ＣＶＶはＥＭＶペイロードの１つまたは複数の他のタグに含まれる。事前承認のインジケーションは、ＥＭＶペイロードの任意のデータフィールドおよび／またはパディングデータフィールドなど、ＥＭＶペイロードの他のタグに格納されてもよい。

【００２６】

図１Ｄは、ＰＯＳデバイス１４０の取引ロジック１４４が、取引データ１５０を、ネッ

トワーク１３０を介してサーバ１２０に送信して、要求された取引の承認を要求する実施形態を示す。図示されるように、取引データ１５０は、カードデータ１０３、事前承認１３２、ＰＯＳデバイスの位置を記述する位置データ１３２、および取引データ１４５を含み得る。少なくとも１つの実施形態では、取引データ１５０は、決済アプレット１０６によって生成されたＥＭＶペイロードを含む。ＥＭＶペイロードは、カードデータ１０３および事前承認１３２のインジケーションを、ＥＭＶペイロードのそれぞれの１つまたは複数のフィールドに含む。いくつかの実施形態では、モバイルデバイス１１０は、取引データ１５０の少なくとも一部を（例えば、要求された購入金額、モバイルデバイス１１０の位置など）、取引の承認の要求の一部として、サーバ１２０に送信してもよい。

【００２７】

受信されると、認可アプリケーション１２３は、取引データ１５０を処理して、取引を承認および／または拒否するかどうかを決定し得る。一般に、認可アプリケーション１２３は、取引データ１５０内の事前承認１３２のインジケーションを識別しようと試み得る。認可アプリケーション１２３が事前承認１３２のインジケーションを識別した場合、認可アプリケーション１２３は、受信した事前承認１３２のインジケーション（またはその任意の属性）を、非接触型カード１０１に関連付けられたアカウントのアカウントデータ１２４に格納された事前承認１３２のインジケーション（またはその任意の属性）と比較し得る。認可アプリケーション１２３は、一致する事前承認１３２のインジケーションが、非接触型カード１０１に関連付けられたアカウントのアカウントデータ１２４に存在すると判断した場合、事前承認１３２が暗号化データ１０８の事前認証を少なくとも部分的に反映するため、認可アプリケーション１２３は取引を承認し得る。認可アプリケーション１２３は、非接触型カード１０１に関連付けられたアカウントのアカウントデータ１２４に、一致する事前承認１３２のインジケーションが存在しないと判断した場合、取引を拒否し得る。いくつかの実施形態では、認可アプリケーション１２３は、ＰＯＳデバイス１４０の位置が、アカウントデータ１２４内に事前承認１３２の属性として格納された位置データ１１５の閾値距離内にあるかどうかを判断し得る。ＰＯＳデバイス１４０の位置が位置データ１１５の閾値距離内にない場合、認可アプリケーション１２３は、取引を拒否するか、および／または取引を承認する前に取引のさらなる処理を要求してもよい。

【００２８】

他の実施形態では、認可アプリケーション１２３は、取引を承認および／または拒否する前に、追加の処理を実行してもよい。例えば、認可アプリケーション１２３は、取引の金額が、アカウントの制限および／または規則１０７－２を超えているかどうかを判断してもよい。同様に、認可アプリケーション１２３は、取引の時間が、規則１０７－２における非接触型カード１０１を使用するための任意の時間制限内であるかどうかを判断してもよい。同様に、認可アプリケーション１２３は、ＰＯＳデバイス１４０の位置データが、規則１０７－２で指定された位置内にあるかどうかを判断してもよい。いくつかの実施形態では、認可アプリケーション１２３は、ＰＯＳデバイス１４０から位置データを受信しなくてもよい。そのような実施形態では、認可アプリケーション１２３は、アカウントデータ１２４の加盟店エントリで指定された加盟店識別子および加盟店識別子に関連付けられた位置に基づいて、ＰＯＳデバイス１４０の位置を判断してもよい。認可アプリケーション１２３は、次に、位置が規則１０７－２で指定された位置内にあるかどうかを判断してもよい。さらに、認可アプリケーション１２３は、取引を承認するかどうかを判断するために、追加の不正分析を実行してもよい。認可アプリケーション１２３は、次に、取引の承認および／または拒否のインジケーションをＰＯＳデバイス１４０に送信してもよい。ＰＯＳデバイス１４０は、次に、取引の承認および／または拒否のインジケーションを非接触型カード１０１に送信してもよい。さらに、認可アプリケーション１２３は、取引の承認および／または拒否に関連する追加の詳細のインジケーションをＰＯＳデバイス１４０に送信してもよい（例えば、位置分析といった取引のために認可アプリケーション１２３によって実行された処理の結果、規則１０７－２に基づく分析など）。ＰＯＳデバイス１４０は、次に、受信したインジケーションを非接触型カード１０１に送信してもよ

い。

【００２９】

図２Ａは、非接触型カード１０１を使用するための規則を定義するために、モバイルデバイス１１０上でアカウントアプリケーション１１３を使用する例示的な実施形態を示す概略図である。図示のように、アカウントアプリケーション１１３は、フィールド２０１～２０４を含むフォームを出力する。ここで、フィールド２０１は金額フィールドに対応し、フィールド２０２は位置フィールドに対応し、フィールド２０３は時間フィールドに対応し、フィールド２０４は加盟店カテゴリフィールドに対応する。図示のように、ユーザは、金額フィールド２０１に３００ドル、位置フィールド２０２にオフィスから１０マイル、時間フィールド２０３に１０日間、加盟店フィールド２０４に工具店という例示の値を提供している。したがって、フィールド２０１～２０４に値を提供することによって、ユーザは、非接触型カード１０１を用いて、最大３００ドルまで１０日間、オフィスから１０マイル以内において、工具店で使用できることを指定している。

【００３０】

図２Ｂは、ユーザがフィールド２０１～２０３の値を提出する実施形態を示す概略図２１０である。図示されているように、アカウントアプリケーション１１３は、非接触型カード１０１をモバイルデバイス１１０にタップするようにインジケーションを出力し得る。そうすることで、認可アプレット１０４が暗号化データ１０８を生成し得る。アカウントアプリケーション１１３は、暗号化データ１０８およびフィールド２０１～２０４からの値（またはそのインジケーション）をサーバ１２０に送信してもよく、サーバ１２０は、暗号化データ１０８を認証し、受信した値（またはそのインジケーション）を、アカウントデータ内の対応するアカウントのための規則１０７－２に格納し得る。次に、サーバ１２０は、暗号化データ１０８の認証のインジケーションをアカウントアプリケーション１１３に送信し、アカウントアプリケーション１１３は、モバイルデバイス１１０に非接触型カード１０１をタップするために別のインジケーションを出力し得る。タップされると、アカウントアプリケーション１１３は、フィールド２０１～２０４（またはそのインジケーション）からの値を非接触型カード１０１に送信し、非接触型カード１０１は、規則１０７－１に受信した値を格納し得る。

【００３１】

図３Ａは、非接触型カード１０１をタップして取引を事前承認する例を示す概略図３００である。図示のように、アカウントアプリケーション１１３は、ユーザのアカウントを認証するための指紋を受信した後に、非接触型カード１０１をモバイルデバイス１１０にタップして取引を事前認証するようにインジケーション出力し得る。ユーザは、アカウントアプリケーション１１３で取引を事前承認する要求を開始して、アカウントのセキュリティを維持し得る。

【００３２】

非接触型カード１０１がモバイルデバイス１１０にタップされると、非接触型カード１０１は、秘密鍵、暗号化アルゴリズム、および顧客識別子を使用して、暗号化データ１０８を生成し得る。上述したように、いくつかの実施形態では、非接触型カード１０１は、モバイルデバイス１１０から受信したデータが１つまたは複数の規則１０７－１に違反するかどうかを判断し得る。例えば、図示されるように、ユーザは１００ドルの取引を事前承認するように指定した。１００ドルの値が規則１０７－１の規則を超える場合、非接触型カード１０１は、暗号化データ１０８の生成を控え、それにより、事前承認プロセスを終了し得る。別の例として、モバイルデバイス１１０から受信した位置データが、規則１０７－１で指定された１つまたは複数の許可された位置内にない場合、非接触型カード１０１は、暗号化データ１０８の生成を控え、それによって事前承認プロセスを終了し得る。

【００３３】

生成されると、非接触型カード１０１は、暗号化データ１０８をモバイルデバイス１１０のアカウントアプリケーション１１３に送信し得る。アカウントアプリケーション１１３は、暗号化データ１０８、位置データ、およびその他のデータ（例えば、要求された金

額、要求された加盟店など）をサーバ１２０に送信し得る。次に、認可アプリケーション１２３は、暗号化データ１０８の復号を試み得る。暗号化データ１０８が正常に復号されて顧客ＩＤが得られた場合、認可アプリケーション１２３は、次に、位置データおよび受信した他のデータが規則１０７－２のいずれかの規則に違反しているかどうかを判断し得る。たとえば、１００ドルの要求が規則１０７－２で指定された金額を超えている場合、認可アプリケーション１２３は、取引への事前承認を控え得る。

【００３４】

図３Ａに示される例では、認可アプリケーション１２３は、暗号化データ１０８を復号すること、および／または要求による規則１０７－２の違反がないと判断することに基づいて、取引を事前承認する。それに応じて、認可アプリケーション１２３は、事前承認のインジケーションをアカウントデータ１２４に格納し、事前承認のインジケーションをモバイルデバイス１１０のアカウントアプリケーション１１３に送信する。格納された事前承認のインジケーションは、モバイルデバイスから受信した位置データ、タイムスタンプ、取引金額などのような１つまたは複数の属性を含み得る。次に、アカウントアプリケーション１１３は、非接触型カード１０１をタップするための別のインジケーションをモバイルデバイス１１０に出力してもよく、そうすることで、非接触型カード１０１のメモリ１０２に事前認証のインジケーションが格納されてもよい。

【００３５】

図３Ｂは、図３Ａにおける取引の事前承認を受けたユーザが、非接触型カード１０１を使用してＰＯＳデバイス１４０で購入しようとする実施形態を示す概略図３１０である。図示されるように、ユーザは、ＰＯＳデバイス１４０に非接触型カード１０１をタップし、および／または非接触型カード１０１をＰＯＳデバイス１４０に挿入し得る。そうすることで、決済アプレット１０６は、ＰＯＳデバイス１４０から取引データを受信する。取引データは、取引の金額、取引の時間、ＰＯＳデバイス１４０に関連付けられた加盟店識別子、および／または取引の位置を表し得る。次に、支払いアプレット１０６は、認可アプレット１０４から、取引を進めるために認可を要求できる。認可アプレット１０４は、図３Ａの結果に基づいて格納された事前承認のインジケーションに基づき、取引を承認するように決定し得る。認可アプレット１０４はさらに、ＰＯＳデバイス１４０から受信した取引のデータが規則１０７－２を満たすかどうか（例えば、加盟店識別子が許可された加盟店のクラスに対応するかどうか、位置データが許可された位置に対応するか、金額が許可された金額かどうかなど）を判断し得る。

【００３６】

次に、認可アプレット１０４は、決済アプレット１０６に承認のインジケーションおよび／または事前承認のインジケーションを提供し得る。次に、決済アプレット１０６は、カードデータ１０３および事前承認のインジケーションを含むＥＭＶペイロードを生成し得る。次に、決済アプレット１０６は、ＥＭＶペイロードをＰＯＳデバイス１４０に送信し得る。次に、ＰＯＳデバイス１４０は、ＥＭＶペイロードをサーバ１２０に送信し得る。ＰＯＳデバイス１４０は、さらに、取引データ、位置データ、加盟店ＩＤなどの他のデータをサーバ１２０に送信してもよい。次に、サーバ１２０は、ＥＭＶペイロードにおける事前承認のインジケーションに少なくとも部分的に基づいて、取引を承認および／または拒否し得る。例えば、サーバ１２０が事前承認のインジケーションを識別する場合、サーバ１２０は取引を承認し得る。しかし、事前承認のインジケーションが予想されるが、ＥＭＶペイロードにおいて検出されない場合、サーバ１２０は取引を拒否し得る。サーバ１２０は、取引が規則１０７－２を満たすか、および／または違反するかどうかに基づいて、取引をさらに承認および／または拒否し得る。

【００３７】

図３Ｃは、ＰＯＳデバイス１４０が、サーバ１２０が取引を拒否したインジケーションを出力する実施形態を示す概略図３２０である。例えば、サーバ１２０は、ＰＯＳデバイス１４０および／または対応する加盟店の位置が、非接触型カード１０１を使用できる規則１０７－２で指定された地理的領域の外にあることを判断し得る。別の例として、認可

アプリケーション１２３は、ＰＯＳデバイス１４０および／または対応する加盟店の位置が、アカウントデータ１２４に事前承認１３２の属性として格納された位置データの閾値距離内にないことを判断し得る。例えば、ＰＯＳデバイス１４０および／または加盟店の位置データが事前承認１３２の位置データから５マイル離れている場合、ユーザがもはや事前承認が要求された位置の閾値距離（例えば、１００フィート）内にないので、サーバ１２０は取引を拒否し得る。サーバ１２０は、拒否のインジケーションをＰＯＳデバイス１４０に送信でき、ＰＯＳデバイス１４０は、ユーザに表示するために同じものを出力してもよい。

【００３８】

図３Ｄは、ＰＯＳデバイス１４０が、ＥＭＶペイロード内の事前承認フラグに基づいてサーバ１２０が取引を承認したというインジケーションを出力する実施形態を示す概略図３３０である。前述のように、サーバ１２０は、少なくとも部分的に、予想される事前承認のインジケーションがＥＭＶペイロードに存在し、取引が事前承認されたときにアカウントデータ１２４に格納された対応するインジケーションと一致するかどうかに基づいて取引を承認し得る。しかしながら、上述のように、サーバ１２０は、規則１０７－２および／または他の不正防止分析などの追加の要因に基づいて取引を許可してもよい。承認されると、サーバ１２０は、承認のインジケーションをＰＯＳデバイス１４０に送信でき、ＰＯＳデバイス１４０は、ユーザに表示するために同じものを出力してもよい。

【００３９】

図４は、論理（logic）フロー４００の一実施形態を示す。論理フロー４００は、本明細書に記載された１つまたは複数の実施形態によって実行される操作の一部または全部を代表し得る。例えば論理フロー４００は、取引を事前承認するための操作の一部または全部を含み得る。実施形態は、この文脈において限定されない。

【００４０】

図示されるように、論理フロー４００はブロック４０５で始まり、認可アプレット１０４は、秘密鍵、入力データ（例えば、顧客識別子）、および暗号化アルゴリズムを使用して、暗号化データ１０８を生成する。認可アプレット１０４は、暗号化データ１０８を、モバイルデバイス１１０上で実行するアカウントアプリケーション１１３に送信し得る。一実施形態では、認可アプレット１０４は、ユーザがアカウントアプリケーション１１３で自分のアカウントの認証資格情報を提供した後、ユーザが事前承認を要求したことに応答して、暗号化データ１０８を生成する。ブロック４１０において、アカウントアプリケーション１１３は、暗号化データ１０８および位置モジュール１１４から受信した位置データを、ネットワーク１３０を介してサーバ１２０に送信する。上述のように、位置モジュール１１４から受信された位置データは、モバイルデバイス１１０の位置を記述する。一部の実施形態では、アカウントアプリケーション１１３は、事前承認の要求額、事前承認の加盟店、事前承認の期間、および／または事前承認の加盟店カテゴリなどの追加データをサーバ１２０に送信してもよい。

【００４１】

ブロック４２０において、認可アプリケーション１２３は、受信した位置データおよび／または暗号化データ１０８の復号に少なくとも部分的に基づいて、取引を事前承認し得る。たとえば、認可アプリケーション１２３は、受信した位置データが規則１０７－２で指定された非接触型カード１０１を使用するための１つまたは複数の許可された位置内にあるかどうかを判断し得る。認可アプリケーション１２３は、さらに、非接触型カード１０１に関連付けられた秘密鍵を使用して、暗号化データ１０８の復号を試み得る。一実施形態では、認可アプリケーション１２３は、暗号化データ１０８を復号すること、および位置データが、規則１０７－２で指定された非接触型カード１０１を使用するための１つまたは複数の位置内にあると判断することに基づいて、取引を事前承認し得る。別の実施形態では、認可アプリケーション１２３は、暗号化データ１０８を復号すること、または位置データが規則１０７－２で指定された非接触型カード１０１を使用するための１つまたは複数の位置内にあると判断することに基づいて、取引を事前承認してもよい。いくつ

かの実施形態では、認可アプリケーション１２３は、事前承認要求が規則１０７－２を満たすかどうか、例えば、要求された金額、加盟店、期間、および／または加盟店カテゴリが、規則１０７－２の１つまたは複数の対応する規則を満たすかどうか、を追加的に判断してもよい。前述のように、いくつかの実施形態では、認可アプリケーション１２３は、複数の事前承認のレベルから事前承認のレベルを選択してもよい。他の実施形態では、認可アプリケーション１３２は、二値の事前承認結果（例えば、事前承認された、および／または事前承認されていない）を返し得る。認可アプリケーション１２３は、次に、アカウントのアカウントデータ１２４に、事前認証のインジケーションを格納し得る。前述のように、事前承認の格納されたインジケーションは、事前承認のレベル、事前承認の時間、モバイルデバイスから受信された位置データなどのような属性を含み得る。

【００４２】

ブロック４３０において、モバイルデバイス１１０のアカウントアプリケーション１１３は、サーバ１２０から事前承認のインジケーションを受信し得る。次に、アカウントアプリケーション１１３は、非接触型カード１０１に事前承認のインジケーションを送信でき、非接触型カード１０１は事前承認のインジケーションをメモリ１０２に格納する。ブロック４４０で、認可アプレット１０４は、決済アプレット１０６から取引を承認する要求を受信し得る。一般に、決済アプレット１０６は、取引金額、加盟店ＩＤ、位置データ、タイムスタンプなどの属性を示す取引データを受信し得る。

【００４３】

ブロック４５０において、認可アプレット１０４は、サーバ１２０による事前承認および／またはモバイルデバイス１１０（および／またはＰＯＳデバイス１４０）の位置に少なくとも部分的に基づいて、決済アプレットからの要求を承認する。認可アプレット１０４は、メモリ１０２に格納された事前承認のインジケーションの存在に少なくとも部分的に基づいて、要求を承認および／または拒否し得る。例えば、認可アプレット１０４は、事前承認のインジケーションに関連付けられた位置が、モバイルデバイス１１０から受信された最新の位置データおよび／またはＰＯＳデバイス１４０から受信された位置データの閾値距離内にあるかどうかを判断し得る。追加および／または代替として、認可アプレット１０４は、ＰＯＳデバイス１４０から受信された取引の金額および／または時間が、規則１０７－２における金額および／または時間の規則に違反しているかどうかを判断してもよい。追加および／または代替として、認可アプレット１０４は、ＰＯＳデバイス１４０から受信された加盟店ＩＤが、規則１０７－２における加盟店および／または加盟店カテゴリの規則に違反しているかどうかを判断してもよい。

【００４４】

ブロック４６０で、決済アプレットは、取引データおよび事前承認のインジケーションを含むＥＭＶペイロードを生成する。取引データは、非接触型カード１０１のカード番号、有効期限、およびＣＶＶ値を含み得る。決済アプレット１０６は、ＥＭＶペイロードをＰＯＳデバイス１４０に送信し得る。ブロック４７０において、ＰＯＳデバイスは、ＥＭＶペイロードおよび取引データをサーバ１２０に送信して、非接触型カード１０１を使用する取引の支払いの承認を要求する。取引データは、ＰＯＳデバイス１４０の取引金額、加盟店の識別子、および／または位置データを含み得る。いくつかの実施形態では、アカウントアプリケーション１１３は、承認のためにデータ（例えば、要求された金額、位置情報、時間情報）もサーバ１２０に送信し得る。ブロック４８０では、サーバ１２０の認可アプリケーション１２３は、ＥＭＶペイロードにおける事前承認のインジケーションに少なくとも部分的に基づいて、非接触型カード１０１を使用する取引の支払いを承認する。たとえば、認可アプリケーション１２３は、アカウントデータ１２４に格納された事前承認のインジケーションにおける位置データが、ＰＯＳデバイス１４０の位置の閾値距離内にあることを判断し得る。追加および／または代替として、認可アプリケーション１２３は、取引の属性が、非接触型カード１０１を使用するための規則１０７－２に違反しないことを判断してもよい。ブロック４９０では、認可アプリケーション１２３は、取引の承認のインジケーションをＰＯＳデバイス１４０に送信し、ＰＯＳデバイス１４０は、承

認のインジケーションを出力し、取引をさらに進めてもよい。

【００４５】

図５は、論理フロー５００の一実施形態を示している。論理フロー５００は、本明細書に記載された１つまたは複数の実施形態によって実行される操作の一部またはすべてを代表し得る。例えば、論理フロー５００は、認可アプリケーション１２３が取引を事前承認するために実行する操作の一部またはすべてを含んでいてもよい。実施形態は、この文脈において限定されない。

【００４６】

図示されているように、論理フロー５００は、ブロック５１０で始まり、ここで、認可アプリケーション１２３は、モバイルデバイス１１０から受信された位置データが、規則１０７－２において非接触型カード１０１の使用が許可されるとして指定された１つまたは複数の位置内にあるかどうかを判断する。いくつかの実施形態では、認可アプリケーション１２３は、位置データが、規則１０７－２で指定された１つまたは複数の位置の閾値距離内にあるかどうかを判断する。ブロック５２０において、認可アプリケーション１２３は、例えば非接触型カード１０１に関連付けられた秘密鍵のコピーを使用して、非接触型カード１０１によって生成された暗号化データ１０８を復号しようとする。ブロック５３０において、認可アプリケーション１２３は、アカウントに対して多要素認証が完了したかどうかを判断する。例えば、認可アプリケーション１２３は、アカウントアプリケーション１１３においてアカウント内のユーザを認証するために多要素認証が使用されたかどうかに少なくとも部分的に基づいて、取引を事前認証することを判断し得る。

【００４７】

ブロック５４０において、認可アプリケーション１２３は、暗号化データ１０８を復号しようとした結果、および／またはモバイルデバイス１１０から受信された位置データが規則１０７－２で指定された１つまたは複数の位置内にあるかどうかに少なくとも部分的に基づいて、取引のための１つまたは複数の事前承認レベルを選択し得る。追加的および／または代替的に、認可アプリケーション１２３は、多要素認証が完了したかどうか、および／または要求された事前承認によって規則１０７－２が違反されているかどうかに基づいて、事前承認レベルを選択してもよい。ブロック５５０において、認可アプリケーション１２３は、選択された事前承認レベルのインジケーションを格納し得る。いくつかの実施形態において、事前承認レベルは、二値の事前承認（例えば、事前承認された、および／または事前承認されていない）である。一実施形態では、事前承認のインジケーションは、事前承認のための一意の識別子を含む。事前承認のインジケーションは、モバイルデバイスから受信した位置データ、要求された事前承認額、および／またはタイムスタンプをさらに含み得る。

【００４８】

ブロック５６０において、認可アプリケーション１２３は、事前承認のインジケーションをモバイルデバイス１１０に送信し得る。送信されたインジケーションは、アカウントデータ１２４に格納されたインジケーションと同じであってもよいし、異なるインジケーションであってもよい。たとえば、認可アプリケーション１２３は、事前承認の一意の識別子を送信し得る。ブロック５７０において、アカウントアプリケーション１１３は、認可アプリケーション１２３から受信した事前承認のインジケーションを非接触型カード１０１に送信する。次に、非接触型カード１０１は、非接触型カード１０１によって生成されたＥＭＶペイロードに含めるように、受信した事前承認のインジケーションを格納して、ＰＯＳデバイス１４０を介して取引の支払いをし得る。そうすることで、認可アプリケーション１２３は、ＥＭＶペイロード内の事前承認のインジケーションを識別し、受信したインジケーション（またはその属性）を、アカウントデータ１２４（またはその属性）に格納された事前承認のインジケーション（またはその属性）と比較し得る。

【００４９】

図６は、論理フロー６００の一実施形態を示している。論理フロー６００は、本明細書に記載された１つまたは複数の実施形態によって実行される動作の一部またはすべてを代

表し得る。例えば、論理フロー６００は、非接触型カードの取引能力を制限するために認可アプリケーション１２３によって実行される動作の一部またはすべてを含み得る。実施形態は、この文脈において限定されない。例えば、認可アプレット１０４は、暗号化データ１０８を生成するかどうか、および／または、非接触型カードを使用して取引の支払いをするという決済アプレット１０６からの要求を承認するかどうかを決定する際に、論理フロー６００の動作の一部またはすべてを実行し得る。

【００５０】

図示されるように、論理フロー６００は、ブロック６１０で始まり、認可アプリケーション１２３は、モバイルデバイス１１０から受信した位置データが、非接触型カード１０１を使用するための１つまたは複数の許可された位置内（および／またはその閾値距離内）にあるかどうかを判断し得る。前述のように、非接触型カード１０１を使用するための許可された位置は、規則１０７－２に格納され得る。ブロック６２０において、認可アプリケーション１２３は、ＰＯＳデバイス１４０によって提供された位置データが、非接触型カード１０１を使用するための１つまたは複数の許可された位置内にあるかどうかを判断し得る。追加および／または代替として、認可アプリケーション１２３は、ＰＯＳデバイス１４０によって提供された位置データが、事前認証要求の一部としてモバイルデバイス１１０から受信した位置データの所定の距離内にあるかどうかを判断してもよい。

【００５１】

ブロック６３０において、認可アプリケーション１２３は、要求された取引金額が、非接触型カードを使用するための規則１０７－１および／または規則１０７－２で指定された最大金額を下回るかどうかを判断し得る。ブロック６４０において、認可アプリケーション１２３は、取引の時間が、非接触型カード１０１が使用を許可される１つまたは複数の期間内にあるかどうかを（例えば、規則１０７－１および／または規則１０７－２に基づいて）判断し得る。ブロック６５０において、認可アプリケーション１２３は、取引に関連付けられた加盟店が、非接触型カード１０１の許可された使用であるかどうかを判断し得る。前述のように、規則１０７－２は、許可された加盟店識別子および／または加盟店カテゴリを規定し得る。取引に関連付けられた加盟店識別子が許可された加盟店識別子ではなく、かつ／または許可された加盟店カテゴリ内ではない場合、サーバ１２０および／または非接触型カード１０１は、非接触型カード１０１の使用を制限し得る。ブロック６６０において、認可アプリケーション１２３は、事前承認のインジケーションがＰＯＳデバイス１４０から受信されたＥＭＶペイロードに格納されているかどうかを判断し得る。いくつかの実施形態において、認可アプリケーション１２３は、事前承認のインジケーション（またはその属性）を、アカウントデータ内のアカウントに対する１つまたは複数の格納された事前承認のインジケーションと比較し得る。さらに、認可アプリケーション１２３は、事前承認のインジケーションに関連付けられた任意の規則が違反されているかどうかを判断してもよい。例えば、事前承認は、時間、距離（例えば、事前承認が処理されたときにモバイルデバイス１１０から受信された位置データに対する）などにおいて制限されてもよい。

【００５２】

ブロック６７０において、認可アプリケーション１２３は、すべての規則１０７－２が満たされていると判断すること、および／またはＥＭＶペイロードにおける事前承認のインジケーションを識別することに少なくとも部分的に基づいて、取引を承認し得る。ブロック６８０において、認可アプリケーション１２３は、少なくとも１つの規則１０７－２が満たされていないと判断すること、および／またはＥＭＶペイロードにおける事前承認のインジケーションを識別できないことに少なくとも部分的に基づいて、取引を拒否し得る。同様に、事前承認のインジケーションに関連付けられた位置データが、ＥＭＶペイロードを提供するＰＯＳデバイス１４０の閾値距離内にない場合、認可アプリケーション１２３は、取引を拒否し得る。

【００５３】

図７は、論理フロー７００の一実施形態を示す。論理フロー７００は、本明細書に記載

される１つまたは複数の実施形態によって実行される操作の一部またはすべてを代表し得る。例えば、論理フロー７００は、非接触型カードの取引能力を制限するための操作の一部またはすべてを含み得る。実施形態は、この文脈に限定されない。

【００５４】

図示されるように、論理フロー７００はブロック７０５で始まり、ロックが解除されたモバイルデバイス１１０の位置モジュール１１４は、位置データをアカウントアプリケーション１１３に提供する。次に、アカウントアプリケーション１１３は、位置データを非接触型カード１０１に送信し得る。ブロック７１０において、非接触型カード１０１の決済アプレットは、ＰＯＳデバイス１４０から取引データ（例えば、取引金額、加盟店ＩＤ、位置データなど）を受信し得る。ブロック７２０において、決済アプレット１０６は、認可アプレット１０４に取引の承認を要求する。ブロック７３０において、認可アプレット１０４は、取引金額、ＰＯＳデバイス１４０の位置、および／または加盟店ＩＤを含む取引データによって規則１０７－１が満たされることを判断する。ブロック７４０において、認可アプレット１０４は、事前承認の有効なインジケーションがメモリ１０２に格納されていることを判断する。例えば、認可アプレット１０４は、事前承認に関連付けられた時間が、規則１０７－１で規定された時間閾値内にあることを判断し得る。別の例として、認可アプレット１０４は、事前承認のインジケーションに関連付けられた位置データが、ＰＯＳデバイス１４０の位置データの閾値距離内にあることを判断してもよい。

【００５５】

ブロック７５０において、認可アプレット１０４は、ブロック７３０および７４０で行われた判断に少なくとも部分的に基づいて、決済アプレット１０６に承認を提供する。ブロック７６０において、決済アプレット１０６は、アカウント番号、有効期限、ＣＶＶ、および事前承認のインジケーションを含むＥＭＶペイロードを生成する。次に、決済アプレット１０６は、ＥＭＶペイロードをＰＯＳデバイス１４０に送信し得る。ブロック７７０において、ＰＯＳデバイス１４０は、ＥＭＶペイロード、取引データ、およびＰＯＳデバイス１４０の位置データを、サーバ１２０の認可アプリケーション１２３に送信する。

【００５６】

ブロック７８０において、認可アプリケーション１２３は、ＥＭＶペイロード内の事前承認のインジケーションおよび／またはＰＯＳデバイス１４０から受信された位置データを検出することに少なくとも部分的に基づいて、取引を承認する。例えば、認可アプリケーション１２３は、ＰＯＳデバイス１４０によって提供された位置データが、非接触型カード１０１を使用するための１つまたは複数の許可された位置内にあるかどうかを判断し得る。追加的および／または代替的に、認可アプリケーション１２３は、ＰＯＳデバイス１４０によって提供された位置データが、アカウントデータ１２４に格納された事前承認のインジケーションの位置データの所定の距離内にあるかどうかを判断してもよい。次に、認可アプリケーション１２３は、承認のインジケーションを送信し得る。ブロック７９０において、ＰＯＳデバイス１４０は、認可アプリケーション１２３から承認のインジケーションを受信することに応答して、取引を処理し得る。

【００５７】

図８は、論理フロー８００の一実施形態を示す。論理フロー８００は、本明細書に記載された１つまたは複数の実施形態によって実行される操作の一部または全部を代表し得る。例えば、論理フロー８００は、多要素認証がアカウントに対して実行されたことを判断するために実行される操作の一部または全部を含み得る。実施形態は、この文脈に限定されない。

【００５８】

図示されるように、論理フロー８００は、ブロック８１０で始まり、アカウントアプリケーション１１３は、アカウントのための有効なログイン資格情報（例えば、ユーザ名とパスワード）を任意に受信する。ブロック８２０において、アカウントアプリケーション１１３は、アカウントの生体認証資格情報（例えば、虹彩スキャン、指紋、フェイスＩＤなど）を任意に受信する。ブロック８３０において、アカウントアプリケーション１１３

は、サーバ１２０によってモバイルデバイス１１０の電話番号にテキストメッセージで送信されたワンタイムパスコードを任意に受信する。ブロック８４０において、アカウントアプリケーション１１３は、非接触型カード１０１によって生成された暗号化データ１０８を任意に受信し、暗号化データ１０８をサーバ１２０に送信する。サーバ１２０は、暗号化データ１０８を認証するために暗号化データ１０８を復号し、認証のインジケーションをアカウントアプリケーション１１３に送信し得る。ブロック８５０において、アカウントアプリケーション１１３は、任意で、別のアプリケーションによって生成され、アカウントアプリケーション１１３への入力としてユーザによって提供されるパスコードを受信する。ブロック８６０において、アカウントアプリケーション１１３は、ブロック８１０～８５０における認証要素のうちの少なくとも２つに基づいて、アカウントに対する多要素認証が発生したと判断し得る。例えば、ブロック８１０でログイン資格情報を受信し、８２０で生体認証資格情報を受信した場合、アカウントアプリケーション１１３は、アカウントの多要素認証が完了したと判断し得る。アカウントアプリケーション１１３は、アカウントの多要素認証のインジケーションをサーバ１２０に送信し得る。

【００５９】

図９は、前述のような様々な実施形態を実施するために適し得るコンピューティングシステム９０２を含む、例示的なコンピューティングアーキテクチャ９００の一実施形態を示す。様々な実施形態において、コンピューティングアーキテクチャ９００は、電子デバイスを含むか、または電子デバイスの一部として実装され得る。いくつかの実施形態において、コンピューティングアーキテクチャ９００は、例えば、システム１００の１つまたは複数のコンポーネントを実装するシステムを代表し得る。いくつかの実施形態では、コンピューティングシステム９０２は、例えば、システム１００の非接触型カード１０１、モバイルデバイス１１０、サーバ１２０、および／またはＰＯＳデバイス１４０を代表し得る。実施形態は、この文脈に限定されない。より一般的には、コンピューティングアーキテクチャ９００は、図１～８を参照して本明細書で説明される全ての論理、アプリケーション、システム、方法、装置、および機能を実装するように構成される。

【００６０】

本出願において使用される「システム」、「コンポーネント」および「モジュール」という用語は、ハードウェア、ハードウェアとソフトウェアの組み合わせ、ソフトウェア、また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のエンティティを指すことが意図されており、その例は例示的なコンピューティングアーキテクチャ９００によって提供されている。例えば、コンポーネントは、コンピュータプロセッサ上で実行されるプロセス、コンピュータプロセッサ、ハードディスクドライブ、複数のストレージドライブ（光学および／または磁気記憶媒体の）、オブジェクト、実行可能ファイル、実行スレッド、プログラム、および／またはコンピュータであり得るが、これらに限定されない。例として、サーバ上で実行されるアプリケーションとサーバの両方がコンポーネントであり得る。１つまたは複数のコンポーネントをプロセスおよび／または実行スレッド内に配置でき、コンポーネントを１台のコンピュータにローカライズしたり、２台以上のコンピュータに分散したりできる。さらに、コンポーネントは、連携して動作するために、様々な種類の通信媒体によって互いに通信可能に結合され得る。連携には、一方向または双方向の情報交換が含まれ得る。例えば、コンポーネントは、通信媒体を介して通信される信号の形で情報を伝達できる。情報は、様々な信号線に割り当てられた信号として実装でき、そのような割り当てでは、各メッセージは信号である。しかしながら、さらなる実施形態は、代わりにデータメッセージを使用し得る。このようなデータメッセージは、さまざまな接続を通して送信され得る。例示的な接続には、パラレルインタフェース、シリアルインタフェース、およびバスインタフェースが含まれる。

【００６１】

コンピューティングシステム９０２は、１つ以上のプロセッサ、マルチコアプロセッサ、コプロセッサ、メモリユニット、チップセット、コントローラ、周辺機器、インタフェース、発信器、タイミングデバイス、ビデオカード、オーディオカード、マルチメディア

入出力（Ｉ／Ｏ）コンポーネント、電源など、様々な一般的なコンピューティング要素を含む。しかしながら、実施形態は、コンピューティングシステム９０２による実装に限定されない。

【００６２】

図９に示されるように、コンピューティングシステム９０２は、プロセッサ９０４、システムメモリ９０６、およびシステムバス９０８を備える。プロセッサ９０４は、様々な市販のコンピュータプロセッサのいずれかであり得る。当該コンピュータプロセッサには、ＡＭＤ（登録商標）Ａｔｈｌｏｎ（登録商標）、Ｄｕｒｏｎ（登録商標）およびＯｐｔｅｒｏｎ（登録商標）プロセッサ、ＡＲＭ（登録商標）アプリケーション、組み込みおよびセキュアプロセッサ、ＩＢＭ（登録商標）およびＭｏｔｏｒｏｌａ（登録商標）ＤｒａｇｏｎＢａｌｌ（登録商標）およびＰｏｗｅｒＰＣ（登録商標）プロセッサ、ＩＢＭおよびＳｏｎｙ（登録商標）Ｃｅｌｌプロセッサ、Ｉｎｔｅｌ（登録商標）Ｃｅｌｅｒｏｎ（登録商標）、Ｃｏｒｅ（登録商標）、Ｃｏｒｅ（２）Ｄｕｏ（登録商標）、Ｉｔａｎｉｕｍ（登録商標）、Ｐｅｎｔｉｕｍ（登録商標）、Ｘｅｏｎ（登録商標）、およびＸＳｃａｌｅ（登録商標）プロセッサ、および同様のプロセッサを含むが、これらに限定されない。デュアルマイクロプロセッサ、マルチコアプロセッサ、および他のマルチプロセッサアーキテクチャもまた、プロセッサ９０４として使用され得る。

【００６３】

システムバス９０８は、システムメモリ９０６を含むがこれに限定されないシステムコンポーネントのための、プロセッサ９０４とのインタフェースを提供する。システムバス９０８は、市販の様々なバスアーキテクチャのいずれかを使用して、メモリバス（メモリコントローラの有無にかかわらず）、周辺機器用バス、およびローカルバスに相互接続可能な、いくつかのタイプのバス構造のいずれかであり得る。インタフェースアダプタは、スロットアーキテクチャを介してシステムバス９０８に接続し得る。スロットアーキテクチャの例には、アクセラレイティッド・グラフィックス・ポート（ＡＧＰ）、カードバス、（拡張）業界標準アーキテクチャ（（Ｅ）ＩＳＡ）、マイクロ・チャネル・アーキテクチャ（ＭＣＡ）、ＮｕＢｕｓ、周辺コンポーネント相互接続（拡張）（ＰＣＩ（Ｘ））、ＰＣＩエクスプレス、パーソナルコンピュータメモリカード国際協会（ＰＣＭＣＩＡ）などが含まれるが、これらに限定されない。

【００６４】

システムメモリ９０６は、１つまたは複数の高速なメモリユニットの形態における様々なタイプのコンピュータ可読記憶媒体を含み得る。当該コンピュータ可読記憶媒体には、読み取り専用メモリ（ＲＯＭ）、ランダムアクセスメモリ（ＲＡＭ）、ダイナミックＲＡＭ（ＤＲＡＭ）、ダブルデータレートＤＲＡＭ（ＤＤＲＡＭ）、同期型ＤＲＡＭ（ＳＤＲＡＭ）、スタティックＲＡＭ（ＳＲＡＭ）、プログラマブルＲＯＭ（ＰＲＯＭ）、消去可能プログラマブルＲＯＭ（ＥＰＲＯＭ）、電気的消去可能プログラマブルＲＯＭ（ＥＥＰＲＯＭ）、フラッシュメモリ（例えば、１つまたは複数のフラッシュアレイ）、強誘電体ポリマーメモリ、オボニック（ovonic）メモリ、相変化または強誘電体メモリ、シリコン－酸化－シリコン－窒化－酸化－シリコン（ＳＯＮＯＳ）メモリ、磁気または光学カード、独立ディスク冗長アレイ（ＲＡＩＤ）ドライブなどのデバイスアレイ、ソリッドステートメモリデバイス（例えば、ＵＳＢメモリ、ソリッドステートドライブ（ＳＳＤ））、および情報を格納するのに適した他のタイプのストレージメディアなどがある。図９に示す実施形態では、システムメモリ９０６は、不揮発性メモリ９１０および／または揮発性メモリ９１２などを含むことができる。基本入出力システム（ＢＩＯＳ）は、不揮発性メモリ９１０に格納できる。

【００６５】

コンピューティングシステム９０２は、内蔵（または外付け）ハードディスクドライブ（ＨＤＤ）９１４、リムーバブル磁気ディスク９１８からの読み取りまたはリムーバブル磁気ディスク９１８への書き込みのための磁気フロッピーディスクドライブ（ＦＤＤ）９１６、およびリムーバブル光ディスク９２２（例えば、ＣＤ－ＲＯＭまたはＤＶＤ）の読

み取りまたは書き込みのための光ディスクドライブ９２０を含む、１つまたは複数の低速メモリユニットの形態における様々なタイプのコンピュータ可読記憶媒体を含み得る。ＨＤＤ９１４、ＦＤＤ９１６、および光ディスクドライブ９２０は、それぞれ、ＨＤＤインタフェース９２４、ＦＤＤインタフェース９２６、および光ドライブインタフェース９２８によって、システムバス９０８に接続できる。外付けドライブ実装用のＨＤＤインタフェース９２４は、ユニバーサルシリアルバス（ＵＳＢ）およびＩＥＥＥ１３９４インタフェース技術の少なくとも１つまたは両方を含むことができる。コンピューティングシステム９０２は、一般に、図１～８を参照して本明細書で説明されるすべての論理、システム、方法、装置、および機能を実装するように構成される。

【００６６】

ドライブおよび関連するコンピュータ可読媒体は、データ、データ構造、コンピュータ実行可能命令などの揮発性および／または不揮発性ストレージを提供する。例えば、オペレーティングシステム９３０、１つまたは複数のアプリケーションプログラム９３２、他のプログラムモジュール９３４、およびプログラムデータ９３６を含む、いくつかのプログラムモジュールをドライブおよびメモリユニット９１０、９１２に格納できる。一実施形態では、１つまたは複数のアプリケーションプログラム９３２、他のプログラムモジュール９３４、およびプログラムデータ９３６は、例えば、システム１００の様々なアプリケーションおよび／またはコンポーネントを含むことができ、例えば、カードデータ１０３、認可アプレット１０４、決済アプレット１０６、規則１０７、暗号化データ１０８、アカウントアプリケーション１１３、認可アプリケーション１２３、アカウントデータ１２４、および／または取引のロジック１４４などを含み得る。

【００６７】

ユーザは、１つまたは複数の有線／無線の入力デバイス、例えばキーボード９３８とマウス９４０などのポインティングデバイスなどを介して、コマンドおよび情報をコンピューティングシステム９０２に入力できる。その他の入力デバイスには、マイク、赤外線（ＩＲ）リモコン、無線周波（ＲＦ）リモコン、ゲームパッド、スタイラスペン、カードリーダー、ドングル、指紋リーダー、手袋、グラフィックタブレット、ジョイスティック、キーボード、網膜リーダー、タッチスクリーン（静電容量式、抵抗膜方式など）、トラックボール、トラックパッド、センサー、スタイラスなどがある。これらおよび他の入力デバイスは、多くの場合、システムバス９０８に結合された入力デバイスインタフェース９４２を介してプロセッサ９０４に接続されるが、パラレルポート、ＩＥＥＥ１３９４シリアルポート、ゲームポート、ＵＳＢポート、ＩＲインタフェースなどの他のインタフェースによって接続することもできる。

【００６８】

モニタ９４４または他のタイプの表示装置も、ビデオアダプタ９４６などのインタフェースを介してシステムバス９０８に接続される。モニタ９４４は、コンピューティングシステム９０２の内蔵または外付けであり得る。モニタ９４４に加えて、コンピュータは通常、スピーカ、プリンタなどの他の周辺出力デバイスを含む。

【００６９】

コンピューティングシステム９０２は、リモートコンピュータ９４８などの１つまたは複数のリモートコンピュータへの有線および／または無線通信を介した論理接続を使用して、ネットワーク環境で動作し得る。リモートコンピュータ９４８は、パーソナルコンピュータ、ポータブルコンピュータ、マイクロプロセッサベースの娯楽機器、ピアデバイス、またはその他の一般的なネットワークノードであり、通常、コンピューティングシステム９０２に関連して説明される要素の多くまたはすべてを含むが、簡潔にするために、メモリ／ストレージデバイス９５０のみが示されている。図示される論理接続には、ローカルエリアネットワーク（ＬＡＮ）９５２および／または広域ネットワーク（ＷＡＮ）９５４などのより大規模なネットワークへの有線／無線接続が含まれる。このようなＬＡＮおよびＷＡＮネットワーク環境は、オフィスおよび企業では一般的であり、イントラネットなどの企業全体のコンピュータネットワークを容易にする。これらはすべて、例えばイン

ターネットなどのグローバル通信ネットワークに接続し得る。実施形態では、図１のネットワーク１３０は、ＬＡＮ９５２およびＷＡＮ９５４のうちの１つまたは複数である。

【００７０】

ＬＡＮネットワーク環境で使用される場合、コンピューティングシステム９０２は、有線および／または無線通信ネットワークインタフェースまたはアダプタ９５６を介して、ＬＡＮ９５２に接続される。アダプタ９５６は、ＬＡＮ９５２への有線および／または無線通信を容易にでき、また、アダプタ９５６の無線機能と通信するように、アダプタ９５６上に配置される無線アクセスポイントを含んでもよい。モバイルデバイス１１０のネットワークインタフェース１１２は、アダプタ９５６の一例である。

【００７１】

ＷＡＮネットワーク環境で使用される場合、コンピューティングシステム９０２は、モデム９５８を含むか、またはＷＡＮ９５４上の通信サーバに接続されるか、またはインターネットなどを介してＷＡＮ９５４上で通信を確立するための他の手段を有し得る。内部または外部の有線および／または無線デバイスであり得るモデム９５８は、入力デバイスインタフェース９４２を介してシステムバス９０８に接続する。ネットワーク環境では、コンピューティングシステム９０２またはその一部に関連して記載されるプログラムモジュールは、リモートメモリ／ストレージデバイス９５０に格納できる。図示されるネットワーク接続は例示であり、コンピュータ間の通信リンクを確立する他の手段を使用できると理解される。

【００７２】

コンピューティングシステム９０２は、ＩＥＥＥ８０２ファミリーの規格を使用する有線および無線デバイスまたはエンティティ、例えば無線通信で動作可能に配置された無線デバイス（例えば、ＩＥＥＥ　８０２．１６無線変調技術）などと通信するように動作可能である。これには、少なくともＷｉ－Ｆｉ（すなわちＷｉｒｅｌｅｓｓ　Ｆｉｄｅｌｉｔｙ）、ＷｉＭａｘ、およびＢｌｕｅｔｏｏｔｈ無線技術などが含まれる。したがって、通信は、従来のネットワークのように所定の構造にすることも、単に少なくとも２つのデバイス間のアドホック通信にすることもできる。Ｗｉ－Ｆｉネットワークは、ＩＥＥＥ８０２．１１ｘ（ａ、ｂ、ｇ、ｎなど）と称される無線技術を使用して、安全で信頼性の高い高速無線接続を提供する。Ｗｉ－Ｆｉネットワークを使用して、コンピュータを相互に接続したり、インターネットに接続したり、（ＩＥＥＥ　８０２．３関連のメディアと機能を使用して）有線ネットワークに接続したりすることができる。

【００７３】

図１０Ａは、クレジットカード、デビットカード、および／またはギフトカードなどの決済カードを含み得る非接触型カード１０１を示す。図示されるように、非接触型カード１０１は、カード１０１の前面または背面に表示されるサービスプロバイダ１００２により発行され得る。いくつかの例では、非接触型カード１０１は、決済カードに関連せず、ＩＤカードを含み得るが、これに限定されない。いくつかの例では、決済カードは、デュアルインタフェース非接触型決済カードを含み得る。非接触型カード１０１は、プラスチック、金属、および他の材料で構成される単層または１つまたは複数の積層を含む基板１０１０を含み得る。例示的な基板材料には、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、および生分解性材料が含まれる。いくつかの例では、非接触型カード１０１は、ＩＳＯ／ＩＥＣ７８１０規格のＩＤ－１フォーマットに準拠した物理的特性を有していてもよく、そうでなければ、非接触型カードは、ＩＳＯ／ＩＥＣ１４４４３規格に準拠していてもよい。しかし、本開示による非接触型カード１０１は、異なる特性を有していてもよく、本開示は、非接触型カードが決済カードに実装されることを必要としないことが理解される。

【００７４】

非接触型カード１０１は、カードの前面および／または背面に表示される識別情報１０１５と、接触パッド１０２０とを含み得る。接触パッド１０２０は、モバイルデバイス１

１０、ユーザデバイス、スマートフォン、ラップトップ、デスクトップ、またはタブレットコンピュータなどの別の通信デバイスとの接触を確立するように構成され得る。非接触型カード１０１は、図１０Ａに示されていない処理回路、アンテナ、および他のコンポーネントを含み得る。これらのコンポーネントは、接触パッド１０２０の背後または基板１０１０上の他の場所に配置され得る。非接触型カード１０１は、カードの背面に配置され得る磁気ストリップまたはテープを含み得る（図１０Ａには示されていない）。

【００７５】

図１０Ｂに示すように、非接触型カード１０１の接触パッド１０２０は、マイクロプロセッサ１０３０およびメモリ１０２を含む、情報を格納および処理するための処理回路１０２５を含み得る。処理回路１０２５は、本明細書に記載の機能を実行するために必要に応じて、プロセッサ、メモリ、エラーおよびパリティ／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、および改ざん防止ハードウェアを含む、追加のコンポーネントを含み得ることが理解される。

【００７６】

メモリ１０２は、読み取り専用メモリ、ライトワンス／リードマルチプルメモリ、または読み取り／書き込みメモリ、例えば、ＲＡＭ、ＲＯＭ、およびＥＥＰＲＯＭであってもよく、非接触型カード１０１は、これらのメモリのうちの１つまたは複数を含み得る。読み取り専用メモリは、工場で読み取り専用としてプログラム可能であってもよいし、または１回のみプログラム可能であってもよい。１回のみプログラム可能な場合、一度書き込みを行った後、何度も読み取ることができる。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出荷時後の、ある時点でプログラム可能である。一度メモリがプログラムされると、書き換えられないが、何度も読み取ることができる。読み取り／書き込みメモリは、工場出荷後に何度もプログラムおよび再プログラムされ得る。読み取り／書き込みメモリもまた、工場出荷後に何度も読み取られ得る。

【００７７】

メモリ１０２は、カードデータ１０３、１つまたは複数のアプレット（認可アプレット１０４、決済アプレット１０６、およびその他のアプレットを含む）、秘密鍵１００８、暗号化データ１０８、規則１０７－１、および１つまたは複数の顧客（またはユーザ）識別子（ＩＤ）１００７を格納するように構成され得る。１つまたは複数のアプレット１０３は、Ｊａｖａ（登録商標）カードアプレットなど、１つまたは複数の非接触型カード上で実行するように構成された１つまたは複数のソフトウェアアプリケーションを含み得る。しかしながら、アプレット１０３は、Ｊａｖａカードアプレットに限定されず、代わりに、非接触型カードまたは限られたメモリを有する他のデバイス上で動作可能な任意のソフトウェアアプリケーションであり得ることが理解される。顧客ＩＤ１００７は、非接触型カード１０１のユーザに割り当てられた一意の英数字の識別子を含んでもよく、識別子により、非接触型カードのユーザを他の非接触型カードのユーザから区別し得る。いくつかの例では、顧客ＩＤ１００７は、顧客およびその顧客に割り当てられたアカウントの両方を識別してもよく、さらに、顧客のアカウントに関連付けられた非接触型カードを識別し得る。いくつかの実施形態では、認可アプレット１０４（または別のアプレット）は、暗号化データ１０８を生成するために、秘密鍵１００８を用いた暗号アルゴリズムへの入力として顧客ＩＤ１００７を使用してもよい。

【００７８】

前述の例示的な実施形態のプロセッサおよびメモリ要素は、接触パッドを参照して説明されるが、本開示はそれに限定されない。これらの要素は、パッド１０２０の外側に実装されるか、パッド１０２０から完全に分離されるか、または接触パッド１０２０内に配置されるプロセッサ１０３０およびメモリ１０２要素に加えて、さらなる要素として実装され得ることが理解される。

【００７９】

いくつかの例では、非接触型カード１０１は、１つまたは複数のアンテナ１０５５を備

え得る。１つまたは複数のアンテナ１０５５は、非接触型カード１０１内、および接触パッド１０２０の処理回路１０２５の周囲に配置され得る。例えば、１つまたは複数のアンテナ１０５５は、処理回路１０２５と一体であり得、１つまたは複数のアンテナ１０５５は、外部ブースターコイルと共に使用され得る。別の例として、１つまたは複数のアンテナ１０５５は、接触パッド１０２０および処理回路１０２５の外部にあってもよい。

【００８０】

一実施形態では、非接触型カード１０１のコイルは、空芯変成器の二次側として機能し得る。端子は、電力または振幅変調をカットすることによって（by cutting power or amplitude modulation）非接触型カード１０１と通信し得る。非接触型カード１０１は、１つまたは複数のコンデンサを介して機能的に維持されている非接触型カードの電源接続のギャップを使用して、端子から送信されたデータを推測し得る。非接触型カード１０１は、非接触型カードのコイルの負荷を切り替えるか、または負荷変調することによって、通信文を取り戻し（communicate back）得る。負荷変調は、干渉によって端子のコイルで検出され得る。より一般的には、アンテナ１０５５、処理回路１０２５、および／またはメモリ１０２を使用して、非接触型カード１０１は、ＮＦＣ、Ｂｌｕｅｔｏｏｔｈ、および／またはＷｉ‐Ｆｉ通信を介して通信するための通信インタフェースを提供する。

【００８１】

上述したように、非接触型カード１０１は、スマートカードまたはＪａｖａＣａｒｄなどの限られたメモリを有する他のデバイス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、１つまたは複数のアプリケーションまたはアプレットが安全に実行され得る。アプレットは、様々なモバイルアプリケーションベースのユースケースにおいて、多要素認証（ＭＦＡ）用のワンタイムパスワード（ＯＴＰ）を提供するように、非接触型カードに追加され得る。アプレットは、モバイルＮＦＣリーダー（例えば、デバイス１１０の通信インタフェース１０５－１）などのリーダーからの近接場データ交換要求などの１つまたは複数の要求に応答し、モバイルＮＦＣリーダーなどのリーダー（例えば、デバイス１１０の通信インタフェース１０５－１）からの近距離データ交換要求などの１つ以上の要求に応答し、ＮＤＥＦテキストタグとしてエンコード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得る。

【００８２】

種々の実施形態は、ハードウェア要素、ソフトウェア要素、または両方の組み合わせを用いて実施され得る。ハードウェア要素の例には、プロセッサ、マイクロプロセッサ、回路、回路素子（トランジスタ、抵抗、コンデンサ、インダクタなど）、集積回路、特定用途向け集積回路（ＡＳＩＣ）、プログラマブル・ロジック・デバイス（ＰＬＤ）、デジタル・シグナル・プロセッサ（ＤＳＰ）、フィールド・プログラマブル・ゲート・アレイ（ＦＰＧＡ）、論理ゲート、レジスタ、半導体デバイス、チップ、マイクロチップ、チップセットなどが含まれ得る。ソフトウェアの例には、ソフトウェアコンポーネント、プログラム、アプリケーション、コンピュータプログラム、アプリケーションプログラム、システムプログラム、マシンプログラム、オペレーティングシステムソフトウェア、ミドルウェア、ファームウェア、ソフトウェアモジュール、ルーチン、サブルーチン、ファンクション、メソッド、プロシージャ、ソフトウェアインターフェース、アプリケーションプログラムインターフェース（ＡＰＩ）、命令セット、コンピューティングコード、コンピュータコード、コードセグメント、コンピュータコードセグメント、ワード、バリュー、シンボル、またはこれらの組み合わせが含まれ得る。ある実施形態をハードウェア要素および／またはソフトウェア要素を使用して実装するかどうかの判断は、所望の計算速度、電力レベル、熱耐性、処理サイクル割当量（ｂｕｄｇｅｔ）、入力データレート、出力データレート、メモリリソース、データバス速度、その他の設計または性能上の制限など、さまざまな要因に応じて異なる。

【００８３】

少なくとも１つの実施形態の１つまたは複数の態様は、機械可読媒体に格納された、プロセッサ内の様々な論理を表す代表的な命令によって実装できる。この代表的な命令は、

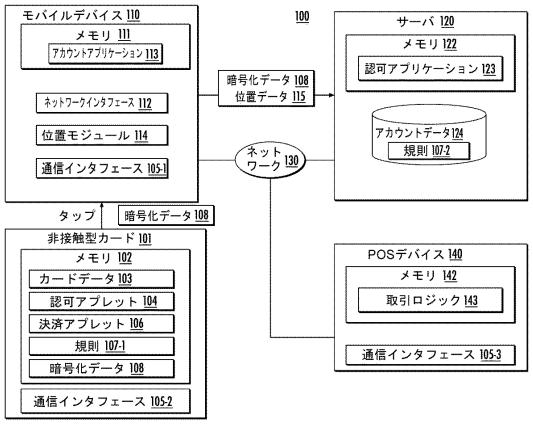
機械によって読み取られると、その機械に、本明細書に記載の技術を実行する論理を組み立てさせる。このような表現は「ＩＰコア」として知られ、有形の機械可読媒体に格納されて、論理またはプロセッサを作る製造機械に搭載するように、様々な顧客または製造施設に提供され得る。いくつかの実施形態は、例えば、機械によって実行されると実施形態に従った方法および／または操作を機械に実行させる命令または命令セットを格納した、機械可読媒体または物品を用いて実装され得る。このような機械は、例えば、任意の適切な処理プラットフォーム、コンピューティングプラットフォーム、コンピューティングデバイス、処理デバイス、コンピューティングシステム、処理システム、コンピュータ、プロセッサなどを含み、ハードウェアおよび／またはソフトウェアの任意の適切な組み合わせを用いて実装され得る。機械可読媒体または物品は、例えば、任意の適切なタイプのメモリユニット、メモリデバイス、メモリ物品、メモリ媒体、ストレージデバイス、ストレージ物品、ストレージ媒体および／またはストレージユニットを含み得、例えば、メモリ、取り外し可能または取り外し不可能な媒体、消去可能または消去不可能な媒体、書き込み可能または再書き込み可能な媒体、ハードディスク、フロッピーディスク、コンパクトディスク読み取り専用メモリ（ＣＤ－ＲＯＭ）、コンパクトディスク記録可能（ＣＤ－Ｒ）、コンパクトディスク再書き込み可能（ＣＤ－ＲＷ）、光ディスク、磁気メディア、光磁気メディア、リムーバブルメモリカードまたはディスク、各種タイプのデジタル多用途ディスク（ＤＶＤ）、テープ、カセットなどが挙げられる。命令は、ソースコード、コンパイルされたコード、インタプリタコード、実行可能コード、静的コード、動的コード、暗号化されたコードなど、任意の適切なタイプのコードを含むことができ、任意の適切な高レベル、低レベル、オブジェクト指向、ビジュアル、コンパイルおよび／またはインタプリタのプログラミング言語を使用して実装される。

【００８４】

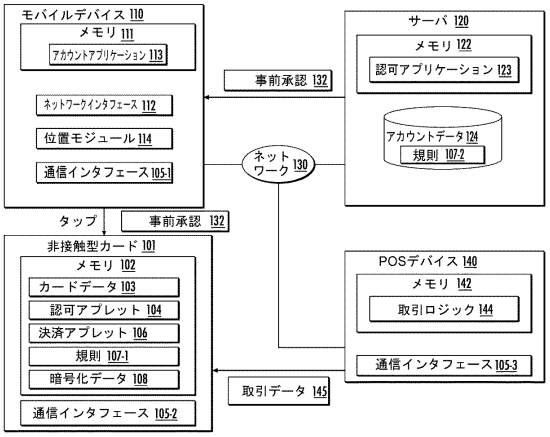
例示的な実施形態の前述の説明は、例示および説明の目的で提示され、網羅的であること、または本開示を開示された正確な形式に限定することを意図していない。本開示に照らして、多くの修正および変形が可能である。本開示の範囲は、この詳細な説明によってではなく、本明細書に添付された特許請求の範囲によって限定されることが意図されている。本出願の優先権を主張する将来の出願は、開示された主題を異なる方法で主張でき、一般に、本明細書で様々に開示される、または他の方法で示されるような１つまたは複数の制限の任意のセットを含むことができる。

【図面】

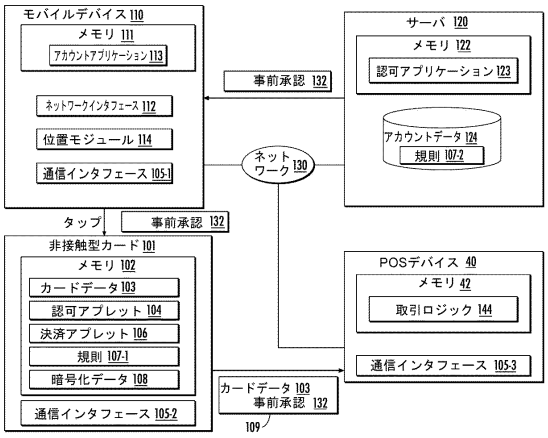
【図１Ａ】



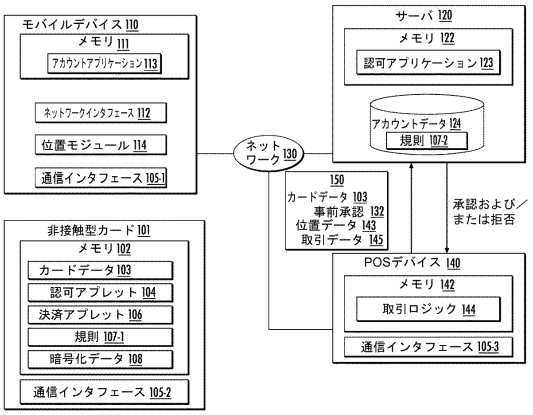
【図１Ｂ】



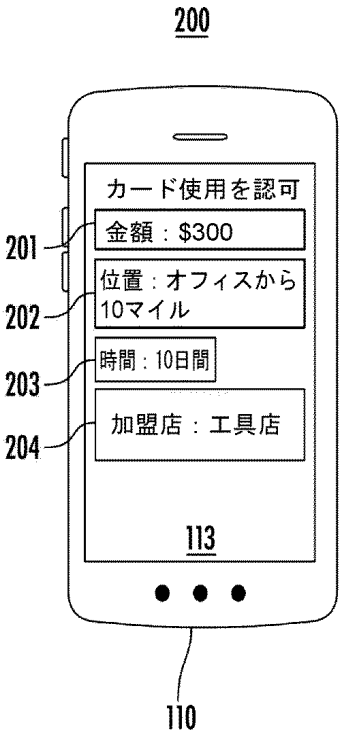
【図１Ｃ】



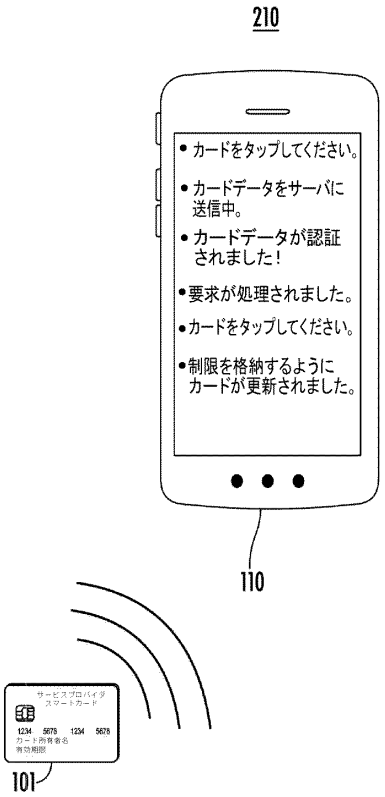
【図１Ｄ】



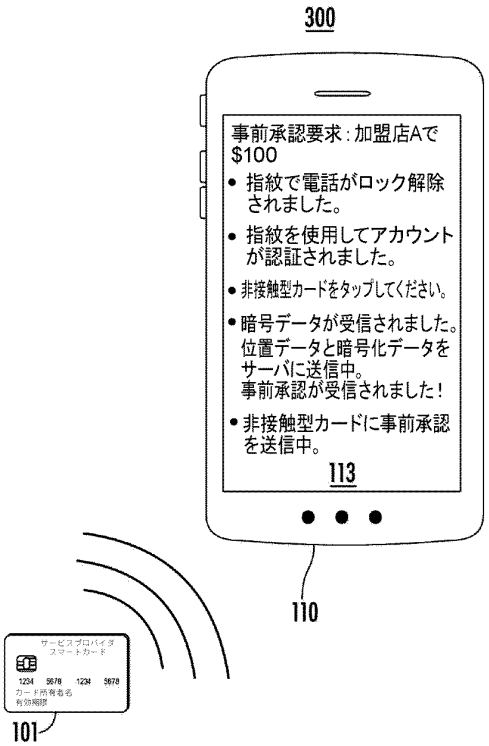
【図２Ａ】



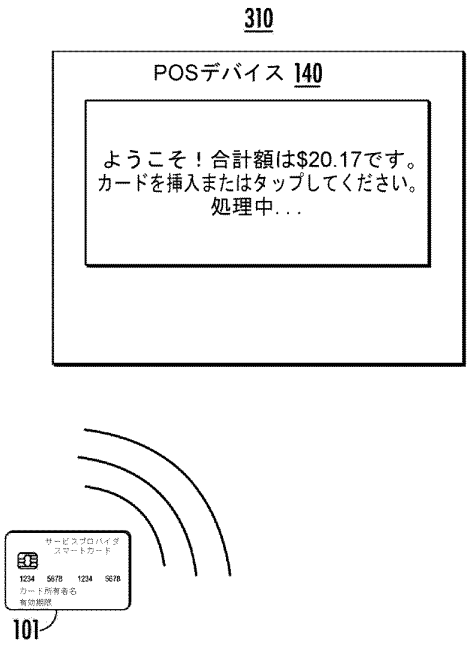
【図２Ｂ】



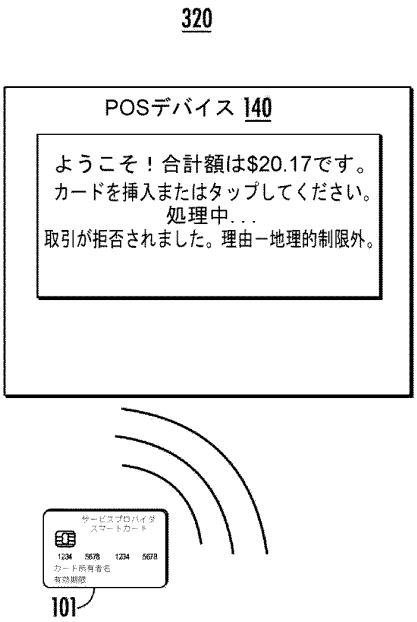
【図３Ａ】



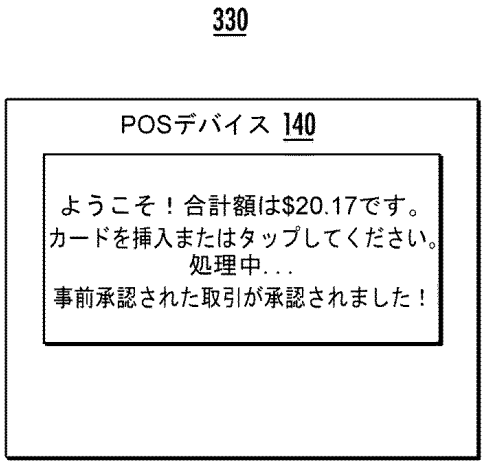
【図３Ｂ】



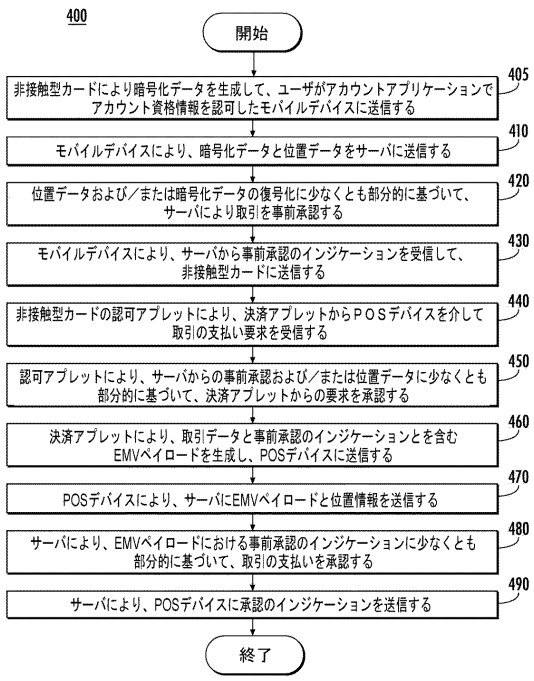
【図３Ｃ】


320
POSデバイス 140
ようこそ！合計額は$20.17です。
カードを挿入またはタップしてください。
処理中...
取引が拒否されました。理由－地理的制限外。
サービスプロバイダ
スマートカード
1234 5678 1234 5678
カード所有者名
有効期限
101

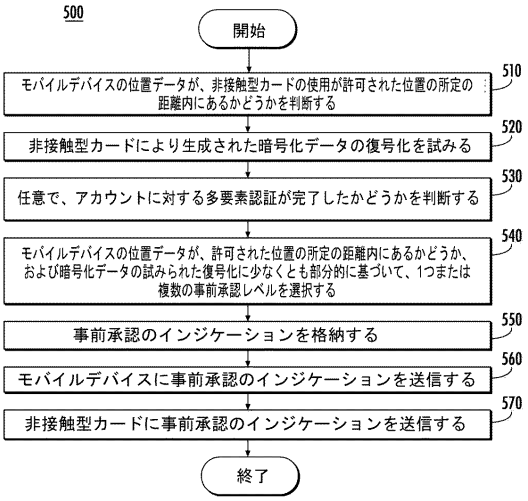
【図３Ｄ】


330
POSデバイス 140
ようこそ！合計額は$20.17です。
カードを挿入またはタップしてください。
処理中...
事前承認された取引が承認されました！

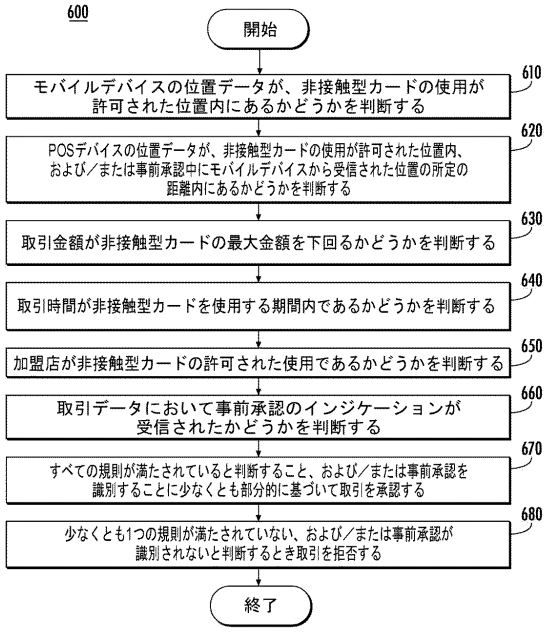
【図４】


400
開始
非接触型カードにより暗号化データを生成して、ユーザがアカウントアプリケーションでアカウント資格情報を認可したモバイルデバイスに送信する
405
モバイルデバイスにより、暗号化データと位置データをサーバに送信する
410
位置データおよび／または暗号化データの復号化に少なくとも部分的に基づいて、サーバにより取引を事前承認する
420
モバイルデバイスにより、サーバから事前承認のインジケーションを受信して、非接触型カードに送信する
430
非接触型カードの認可アプレットにより、決済アプレットからＰＯＳデバイスを介して取引の支払い要求を受信する
440
認可アプレットにより、サーバからの事前承認および／または位置データに少なくとも部分的に基づいて、決済アプレットからの要求を承認する
450
決済アプレットにより、取引データと事前承認のインジケーションとを含むEMVペイロードを生成し、POSデバイスに送信する
460
POSデバイスにより、サーバにEMVペイロードと位置情報を送信する
470
サーバにより、EMVペイロードにおける事前承認のインジケーションに少なくとも部分的に基づいて、取引の支払いを承認する
480
サーバにより、POSデバイスに承認のインジケーションを送信する
490
終了

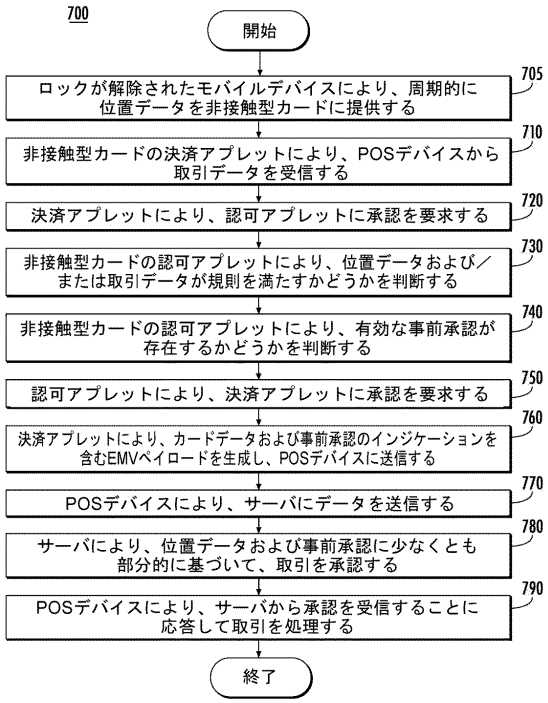
【図５】


500
開始
モバイルデバイスの位置データが、非接触型カードの使用が許可された位置の所定の距離内にあるかどうかを判断する
510
非接触型カードにより生成された暗号化データの復号化を試みる
520
任意で、アカウントに対する多要素認証が完了したかどうかを判断する
530
モバイルデバイスの位置データが、許可された位置の所定の距離内にあるかどうか、および暗号化データの試みられた復号化に少なくとも部分的に基づいて、1つまたは複数の事前承認レベルを選択する
540
事前承認のインジケーションを格納する
550
モバイルデバイスに事前承認のインジケーションを送信する
560
非接触型カードに事前承認のインジケーションを送信する
570
終了

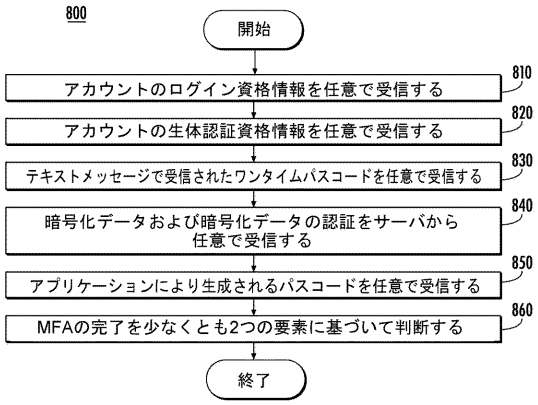
【図６】


600
開始
モバイルデバイスの位置データが、非接触型カードの使用が許可された位置内にあるかどうかを判断する
610
POSデバイスの位置データが、非接触型カードの使用が許可された位置内、および／または事前承認中にモバイルデバイスから受信された位置の所定の距離内にあるかどうかを判断する
620
取引金額が非接触型カードの最大金額を下回るかどうかを判断する
630
取引時間が非接触型カードを使用する期間内であるかどうかを判断する
640
加盟店が非接触型カードの許可された使用であるかどうかを判断する
650
取引データにおいて事前承認のインジケーションが受信されたかどうかを判断する
660
すべての規則が満たされていると判断すること、および／または事前承認を識別することに少なくとも部分的に基づいて取引を承認する
670
少なくとも1つの規則が満たされていない、および／または事前承認が識別されないと判断するとき取引を拒否する
680
終了

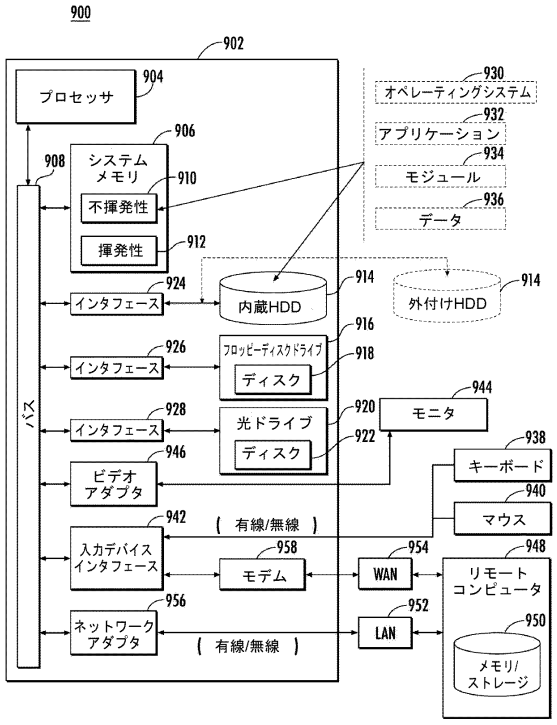
【図７】


700
開始
ロックが解除されたモバイルデバイスにより、周期的に位置データを非接触型カードに提供する
705
非接触型カードの決済アプレットにより、POSデバイスから取引データを受信する
710
決済アプレットにより、認可アプレットに承認を要求する
720
非接触型カードの認可アプレットにより、位置データおよび／または取引データが規則を満たすかどうかを判断する
730
非接触型カードの認可アプレットにより、有効な事前承認が存在するかどうかを判断する
740
認可アプレットにより、決済アプレットに承認を要求する
750
決済アプレットにより、カードデータおよび事前承認のインジケーションを含むEMVペイロードを生成し、POSデバイスに送信する
760
POSデバイスにより、サーバにデータを送信する
770
サーバにより、位置データおよび事前承認に少なくとも部分的に基づいて、取引を承認する
780
POSデバイスにより、サーバから承認を受信することに応答して取引を処理する
790
終了

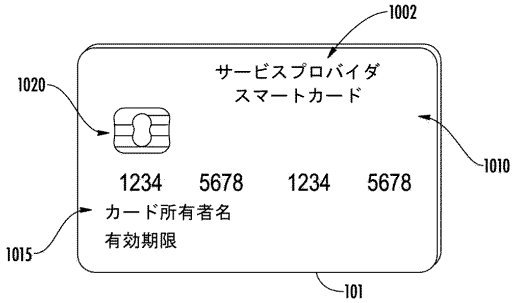
【図８】


800
開始
アカウントのログイン資格情報を任意で受信する
810
アカウントの生体認証資格情報を任意で受信する
820
テキストメッセージで受信されたワンタイムパスコードを任意で受信する
830
暗号化データおよび暗号化データの認証をサーバから任意で受信する
840
アプリケーションにより生成されるパスコードを任意で受信する
850
MFAの完了を少なくとも2つの要素に基づいて判断する
860
終了

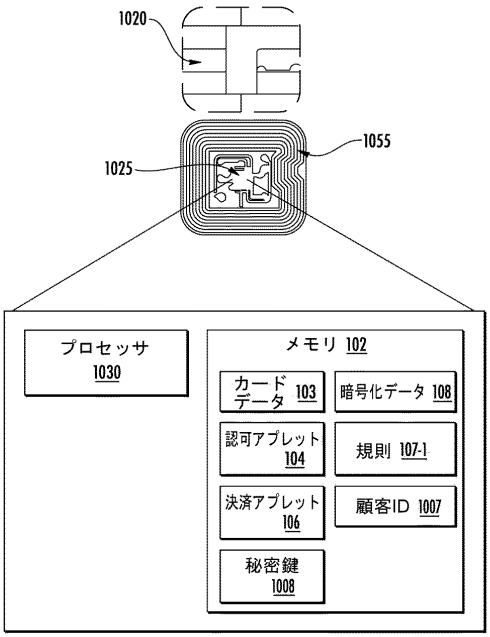
【図９】


900
902
プロセッサ
904
システムメモリ
906
908
不揮発性
910
揮発性
912
バス
インタフェース
924
内蔵HDD
914
外付けHDD
914
インタフェース
926
フロッピーディスクドライブ
916
ディスク
918
インタフェース
928
光ドライブ
920
ディスク
922
ビデオアダプタ
946
入力デバイスインタフェース
942
ネットワークアダプタ
956
モデム
958
WAN
954
LAN
952
リモートコンピュータ
948
メモリ/ストレージ
950
モニタ
944
キーボード
938
マウス
940
有線/無線
有線/無線
オペレーティングシステム
930
アプリケーション
932
モジュール
934
データ
936

【図１０Ａ】


1002
サービスプロバイダ
スマートカード
1020
1010
1234 5678 1234 5678
カード所有者名
有効期限
1015
101

【図１０Ｂ】


1020
1055
1025
プロセッサ
1030
メモリ 102
カードデータ 103
暗号化データ 108
認可アプレット 104
規則 107-1
決済アプレット 106
顧客ID 1007
秘密鍵 1008

フロントページの続き

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　モートン，ポール
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　ルッツ，ウェイン
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　▲柳▼谷 侑
(56)参考文献　特開２０１１－０９５８７０（ＪＰ，Ａ）
特開２００２－２６１７５５（ＪＰ，Ａ）
米国特許出願公開第２００８／００５４０８１（ＵＳ，Ａ１）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／００ － ２１／８８
Ｇ０６Ｑ　１０／００ － ２０／４２