

(19)日本国特許庁(JP)

(12)公表特許公報(A)

(11)公表番号

特表2024-540510

(P2024-540510A)

(43)公表日 令和6年10月31日(2024.10.31)

(51)国際特許分類

G 0 6 Q 20/40 (2012.01)

F I

G 0 6 Q 20/40

テーマコード (参考)

5 L 0 2 0

審査請求 未請求 予備審査請求 未請求 (全40頁)

(21)出願番号	特願2024-529481(P2024-529481)	(71)出願人	519111877
(86)(22)出願日	令和4年4月19日(2022.4.19)		キャピタル・ワン・サービシーズ・リミ
(85)翻訳文提出日	令和6年7月16日(2024.7.16)		テッド・ライアビリティ・カンパニー
(86)国際出願番号	PCT/US2022/025285		Capital One Service
(87)国際公開番号	WO2023/091182		s, LLC
(87)国際公開日	令和5年5月25日(2023.5.25)		アメリカ合衆国22102バージニア州
(31)優先権主張番号	17/530,837		マククリーン、キャピタル・ワン・ドライ
(32)優先日	令和3年11月19日(2021.11.19)		ブ1680番
(33)優先権主張国・地域又は機関	米国(US)	(74)代理人	100145403
			弁理士 山尾 憲人
(81)指定国・地域	AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA	(74)代理人	100135703
	,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(		弁理士 岡部 英隆
	AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,A	(72)発明者	ルール, ジェフリー
	T,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR		アメリカ合衆国22102バージニア州
	,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,		マククリーン、キャピタル・ワン・ドライ
	最終頁に続く		最終頁に続く

(54)【発明の名称】 非接触カードを用いたアカウント認証に基づくデータの自動記入

(57)【要約】

ウェブブラウザは、ウェブページの支払いフィールドを検出し、非接触カードに関連したアプリケーションが装置にインストールされると決定しうる。ブラウザはアプリケーションのURIを生成しうる。URIは、マーチャント識別子、セッション識別子、及びアクション識別子を含む。モバイルOSは、URIに基づいてアプリケーションを起動しうる。アプリケーションは、URIのアクション識別子パラメータに基づいて、非接触カードによって生成された暗号文に基づいて、非接触カードに関連付けられたアカウントを認証しうる。アプリケーションは、認証に基づいて、非接触カードに関連付けられた支払い情報を受信しうる。アプリケーションのWeb View構成要素は、ウェブページにアクセスし、支払い情報を支払いフィールドへ自動記入しうる。Web View構成要素は、自動記入された支払い情報に基づいたトランザクションを処理しうる。

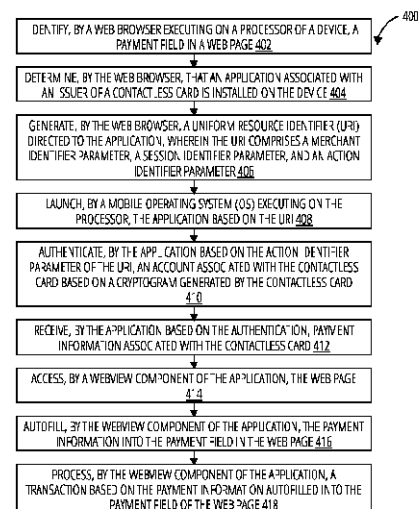


FIG. 4

【特許請求の範囲】

【請求項 1】

コンピュータで実装された方法であって、

装置のプロセッサにおいて実行されるウェブブラウザによって、ウェブページにおける支払いフィールドを識別することと、

上記ウェブブラウザによって、非接触カードの発行者に関連付けられたアプリケーションが上記装置にインストールされることを決定することと、

上記ウェブブラウザによって、上記アプリケーションに向けられたURI (uniform resource identifier) であって、マーチャント識別子パラメータ、セッション識別子パラメータ、及びアクション識別子パラメータを含むURIを生成することと、

10

上記プロセッサにおいて実行されるモバイルオペレーティングシステム (OS) によって、上記URIに基づいて上記アプリケーションを起動することと、

上記アプリケーションによって、上記URIのアクション識別子パラメータに基づいて、上記非接触カードによって生成された暗号文に基づいて、上記非接触カードに関連付けられたアカウントを認証することと、

上記アプリケーションによって、上記認証に基づいて、上記非接触カードに関連付けられた支払い情報を受信することと、

上記アプリケーションのWeb View構成要素によって、上記ウェブページにアクセスすることと、

上記アプリケーションのWeb View構成要素によって、上記ウェブページにおける支払いフィールドへ支払い情報を自動記入することと、

20

上記アプリケーションのWeb View構成要素によって、上記ウェブページの支払いフィールドへ自動記入された支払い情報に基づいて、トランザクションを処理することを含む、

方法。

【請求項 2】

上記方法は、上記アプリケーションによって、上記マーチャント識別子及び上記セッション識別子に基づいて、上記ウェブページのURLを生成することを含み、

上記マーチャント識別子は、上記ウェブページを提供するマーチャントに関連付けられ、

30

上記セッション識別子は、上記ウェブブラウザにおける閲覧セッションに関連付けられ、

上記方法は、上記アプリケーションのWeb View構成要素によって、上記ウェブページの生成されたURLに基づいて上記ウェブページにアクセスすることをさらに含む、請求項 1 記載の方法。

【請求項 3】

上記支払い情報は、認証サーバから受信されたアカウント番号を含む、請求項 1 又は 2 記載の方法。

【請求項 4】

上記支払い情報は、上記ウェブページをホスティングするウェブサーバから受信された支払いトークンを含む、

40

請求項 1 又は 2 記載の方法。

【請求項 5】

上記ウェブブラウザは、上記モバイルオペレーティングシステムによって提供される機能に基づいて、上記アプリケーションが上記装置にインストールされることを決定する、請求項 1 又は 2 記載の方法。

【請求項 6】

上記URIは、上記アプリケーションに対するディープリンクであり、

上記アプリケーションは、上記アクション識別子に基づいて、上記アプリケーションの認証ページをロードする、

50

請求項 1 又は 2 記載の方法。

【請求項 7】

上記認証することは、

上記アプリケーションによって、上記暗号文を認証サーバに送信することと、

上記アプリケーションによって、上記認証サーバから、上記暗号文を復号した認証サーバを指定する情報を受信することを含む、

請求項 1 又は 2 記載の方法。

【請求項 8】

上記アプリケーションが上記装置にインストールされることを決定する前に、

上記ウェブブラウザによって、上記ウェブページの支払いフィールドを選択する入力を受信することと、

上記アプリケーションを用いて上記トランザクションを処理することを指定する情報を表示することと、

上記アプリケーションを用いて上記トランザクションを処理することを指定する入力を受信することとをさらに含む、

請求項 1 又は 2 記載の方法。

【請求項 9】

装置のプロセッサによって実行されたときに上記プロセッサに下記の動作を実行させる命令を含むコンピュータ可読記憶媒体であって、

上記動作は、

ウェブブラウザによって、ウェブページにおける支払いフィールドを識別することと、

上記ウェブブラウザによって、非接触カードの発行者に関連付けられたアプリケーションが上記装置にインストールされることを決定することと、

上記ウェブブラウザによって、上記アプリケーションに向けられた U R I (uniform resource identifier) であって、マーチャント識別子パラメータ、セッション識別子パラメータ、及びアクション識別子パラメータを含む U R I を生成することと、

モバイルオペレーティングシステム (O S) によって、上記 U R I に基づいて上記アプリケーションを起動することと、

上記アプリケーションによって、上記 U R I のアクション識別子パラメータに基づいて、上記非接触カードによって生成された暗号文に基づいて、上記非接触カードに関連付けられたアカウントを認証することと、

上記アプリケーションによって、上記認証に基づいて、上記非接触カードに関連付けられた支払い情報を受信することと、

上記アプリケーションの W e b V i e w 構成要素によって、上記ウェブページにアクセスすることと、

上記アプリケーションの W e b V i e w 構成要素によって、上記ウェブページにおける支払いフィールドへ支払い情報を自動記入することと、

上記アプリケーションの W e b V i e w 構成要素によって、上記ウェブページの支払いフィールドへ自動記入された支払い情報に基づいて、トランザクションを処理することを含む、

コンピュータ可読記憶媒体。

【請求項 10】

上記命令は、上記アプリケーションによって、上記マーチャント識別子及び上記セッション識別子に基づいて、上記ウェブページの U R L を生成することを上記プロセッサにさらに実行させ、

上記マーチャント識別子は、上記ウェブページを提供するマーチャントに関連付けられ、

上記セッション識別子は、上記ウェブブラウザにおける閲覧セッションに関連付けられ、

上記命令は、上記アプリケーションの W e b V i e w 構成要素によって、上記ウェブペ

10

20

30

40

50

ージの生成されたURLに基づいて上記ウェブページにアクセスすることを上記プロセッサにさらに実行させる、

請求項9記載のコンピュータ可読記憶媒体。

【請求項11】

上記支払い情報は、認証サーバから受信されたアカウント番号を含む、

請求項9又は10記載のコンピュータ可読記憶媒体。

【請求項12】

上記支払い情報は、上記ウェブページをホスティングするウェブサーバから受信された支払いトークンを含む、

請求項9又は10記載のコンピュータ可読記憶媒体。

10

【請求項13】

上記ウェブブラウザは、上記モバイルオペレーティングシステムによって提供される機能に基づいて、上記アプリケーションが上記装置にインストールされることを決定する、

請求項9又は10記載のコンピュータ可読記憶媒体。

【請求項14】

上記URIは、上記アプリケーションに対するディープリンクであり、

上記アプリケーションは、上記アクション識別子に基づいて、上記アプリケーションの認証ページをロードする、

請求項9又は10記載のコンピュータ可読記憶媒体。

【請求項15】

上記認証することは、実行されたときに、

上記アプリケーションによって、上記暗号文を認証サーバに送信することと、

上記アプリケーションによって、上記認証サーバから、上記暗号文を復号した認証サーバを指定する情報を受信することとを上記プロセッサに実行させる命令を含む、

請求項9又は10記載のコンピュータ可読記憶媒体。

20

【請求項16】

上記命令は、上記アプリケーションが上記装置にインストールされることを決定する前に、

上記ウェブブラウザによって、上記ウェブページの支払いフィールドを選択する入力を受信することと、

上記アプリケーションを用いて上記トランザクションを処理することを指定する情報を表示することと、

上記アプリケーションを用いて上記トランザクションを処理することを指定する入力を受信することとを上記プロセッサにさらに実行させる、

請求項9又は10記載のコンピュータ可読記憶媒体。

30

【請求項17】

プロセッサと、上記プロセッサによって実行されたときに上記プロセッサに下記の動作を実行させる命令を格納するメモリとを備える計算装置であって、

上記動作は、

ウェブブラウザによって、ウェブページにおける支払いフィールドを識別することと、

上記ウェブブラウザによって、非接触カードの発行者に関連付けられたアプリケーションが上記装置にインストールされることを決定することと、

上記ウェブブラウザによって、上記アプリケーションに向けられたURI (uniform resource identifier) であって、マーチャント識別子パラメータ、セッション識別子パラメータ、及びアクション識別子パラメータを含むURIを生成することと、

上記プロセッサにおいて実行されるモバイルオペレーティングシステム(OS)によって、上記URIに基づいて上記アプリケーションを起動することと、

上記アプリケーションによって、上記URIのアクション識別子パラメータに基づいて、上記非接触カードによって生成された暗号文に基づいて、上記非接触カードに関連付けられたアカウントを認証することと、

40

50

上記アプリケーションによって、上記認証に基づいて、上記非接触カードに関連付けられた支払い情報を受信することと、

上記アプリケーションのWeb View構成要素によって、上記ウェブページにアクセスすることと、

上記アプリケーションのWeb View構成要素によって、上記ウェブページにおける支払いフィールドへ支払い情報を自動記入することと、

上記アプリケーションのWeb View構成要素によって、上記ウェブページの支払いフィールドへ自動記入された支払い情報に基づいて、トランザクションを処理することとを含む、

計算装置。

10

【請求項 18】

上記命令は、上記アプリケーションによって、上記マーチャント識別子及び上記セッション識別子に基づいて、上記ウェブページのURLを生成することを上記プロセッサにさらに実行させ、

上記マーチャント識別子は、上記ウェブページを提供するマーチャントに関連付けられ、

上記セッション識別子は、上記ウェブブラウザにおける閲覧セッションに関連付けられ、

上記命令は、上記アプリケーションのWeb View構成要素によって、上記ウェブページの生成されたURLに基づいて上記ウェブページにアクセスすることを上記プロセッサにさらに実行させる、

20

請求項 17 記載の計算装置。

【請求項 19】

上記支払い情報は、認証サーバから受信されたアカウント番号を含む、

請求項 17 又は 18 記載の計算装置。

【請求項 20】

上記支払い情報は、上記ウェブページをホスティングするウェブサーバから受信された支払いトークンを含む、

請求項 17 又は 18 記載の計算装置。

【請求項 21】

上記ウェブブラウザは、上記モバイルオペレーティングシステムによって提供される機能に基づいて、上記アプリケーションがインストールされることを決定する、

請求項 17 又は 18 記載の計算装置。

【請求項 22】

上記URLは、上記アプリケーションに対するディープリンクであり、

上記アプリケーションは、上記アクション識別子に基づいて、上記アプリケーションの認証ページをロードする、

請求項 17 又は 18 記載の計算装置。

【請求項 23】

上記認証することは、上記プロセッサによって実行されたとき、

上記アプリケーションによって、上記暗号文を認証サーバに送信することと、

上記アプリケーションによって、上記認証サーバから、上記暗号文を復号した認証サーバを指定する情報を受信することとを上記プロセッサに実行させる命令を含む、

請求項 17 又は 18 記載の計算装置。

【請求項 24】

上記命令は、上記アプリケーションがインストールされることを決定する前に、

上記ウェブブラウザによって、上記ウェブページの支払いフィールドを選択する入力を受信することと、

上記アプリケーションを用いて上記トランザクションを処理することを指定する情報を表示することと、

50

上記アプリケーションを用いて上記トランザクションを処理することを指定する入力を受信することとを上記プロセッサにさらに実行させる、
請求項 17 又は 18 記載の計算装置。

【発明の詳細な説明】

【技術分野】

【0001】

関連出願

本願は、2021年11月19日に出願された、「非接触カードを用いたアカウント認証に基づくデータの自動記入 (AUTOFILLING DATA BASED ON ACCOUNT AUTHENTICATION USING A CONTACTLESS CARD)」のタイトルを有する、米国特許出願シリアル番号第 17 / 530837 号の優先権を主張し、前述の出願の内容の全体は参照によって本願に援用される。

【0002】

本開示は、非接触カードを用いたアカウント認証に基づくデータの自動記入に関する。

【背景技術】

【0003】

支払いカードのためのアカウント識別子は、長い数値及び／又は文字の列を含む可能性がある。このように、ユーザがアカウント識別子を手動で正しく入力することは困難である可能性がある。実際に、ユーザはしばしば誤りを犯し、正しくないアカウント番号を計算装置上の支払いインターフェースへ入力する。さらに、装置に入力されるアカウント識別子をカメラ又は他の悪意のあるエンティティが取り込んで識別することを可能にし、それによって、セキュリティリスクを生じる処理が開発されている。

【発明の概要】

【発明が解決しようとする課題】

【0004】

本開示は、非接触カードを用いたアカウント認証に基づくデータの自動記入を提供する。

【課題を解決するための手段】

【0005】

1つの態様において、方法は、

装置のプロセッサにおいて実行されるウェブブラウザによって、ウェブページにおける支払いフィールドを識別することと、

ウェブブラウザによって、非接触カードの発行者に関連付けられたアプリケーションが装置にインストールされることを決定することと、

ウェブブラウザによって、アプリケーションに向けられたURI (uniform resource identifier) であって、マーチャント識別子パラメータ、セッション識別子パラメータ、及びアクション識別子パラメータを含むURIを生成することと、

プロセッサにおいて実行されるモバイルオペレーティングシステム (OS) によって、URIに基づいてアプリケーションを起動することと、

アプリケーションによって、URIのアクション識別子パラメータに基づいて、非接触カードによって生成された暗号文に基づいて、非接触カードに関連付けられたアカウントを認証することと、

アプリケーションによって、認証に基づいて、非接触カードに関連付けられた支払い情報を受信することと、

アプリケーションのWeb View構成要素によって、ウェブページにアクセスすることと、

アプリケーションのWeb View構成要素によって、ウェブページにおける支払いフィールドへ支払い情報を自動記入することと、

アプリケーションのWeb View構成要素によって、ウェブページの支払いフィールドへ自動記入された支払い情報に基づいて、トランザクションを処理することを含む。

他の実施形態は説明され主張される。

【図面の簡単な説明】

【0006】

【図1A】一実施形態に係る主題の態様を示す。

【図1B】一実施形態に係る主題の態様を示す。

【図1C】一実施形態に係る主題の態様を示す。

【図1D】一実施形態に係る主題の態様を示す。

【図1E】一実施形態に係る主題の態様を示す。

【図2A】一実施形態に係る主題の態様を示す。

【図2B】一実施形態に係る主題の態様を示す。

【図2C】一実施形態に係る主題の態様を示す。

【図2D】一実施形態に係る主題の態様を示す。

【図2E】一実施形態に係る主題の態様を示す。

【図3A】一実施形態に係る主題の態様を示す。

【図3B】一実施形態に係る主題の態様を示す。

【図3C】一実施形態に係る主題の態様を示す。

【図3D】一実施形態に係る主題の態様を示す。

【図4】一実施形態に係るルーチン400を示す。

【図5】一実施形態に係るルーチン500を示す。

【図6A】一実施形態に係る非接触カードを示す。

【図6B】一実施形態に係る非接触カード104を示す。

【図7】一実施形態に係るデータ構造700を示す。

【図8】一実施形態に係るコンピュータアーキテクチャ800を示す。

【発明を実施するための形態】

【0007】

任意の特定の構成要素又は動作についての説明を容易に識別するために、参照番号の上位数字は、その構成要素が最初に導入される図番号を示す。

【0008】

本願で開示する実施形態は、非接触カードを用いてウェブブラウザにデータを安全に自動記入するための技術を提供する。概して、ウェブブラウザは、1つ又は複数の支払いフォームフィールドを含むウェブページをロードすることがある。ブラウザは、支払いフォームフィールドを検出し、非接触カードの発行者に関連付けられるアプリケーション（例えば、非接触カードに関連付けられた金融機関によって提供されるアカウント管理アプリケーション）が装置にインストールされているか否かを決定してもよい。アプリケーションがインストールされているとブラウザが決定する場合、ブラウザは、アプリケーションに向けられたURI（uniform resource identifier）を生成してもよい。ブラウザは、URIのパラメータとして、マーチャント識別子（ID）パラメータ、セッションIDパラメータ、及びアクションIDパラメータを含んでもよい。

【0009】

装置上のオペレーティングシステムは、URIを処理してアカウントアプリケーションを起動してもよい。アプリケーションは、URIのパラメータを処理し、アクション識別子に基づいて、アプリケーションのアカウント認証ページを出力することを決定してもよい。認証ページは、例えば、ログイン／パスワード、バイオメトリクス、又は、装置へのカードのタップに基づいて非接触カードによって生成される暗号文に基づいたワンタップ認証を介して、アカウントを認証する1つ又は複数の機能を含んでもよい。

【0010】

少なくとも1つの実施形態では、いったんアカウントが認証されると、アプリケーションは、アプリケーションのWeb View構成要素におけるウェブページにリロードしてもよい。URIのマーチャントID及びセッションIDを用いることによって、Web View構成要素は、ウェブブラウザにおいて開始されたユーザの閲覧セッションを受信及

10

20

30

40

50

び復元する。アカウントアプリケーションは、非接触カードに関連付けられた支払い情報（例えば、アカウント番号、有効期限、及びカード検証値（card verification value：C V V））を、（例えば、サーバ及び／又は非接触カードから）受信してもよく、さもなければ格納してもよい。支払い情報は、Web View構成要素における支払いフォームへ自動記入されてもよい。いったん自動記入されると、Web View構成要素におけるフォームを提出することで購入が完了しうる。

【0011】

少なくとも1つの実施形態では、いったんアカウントが認証されると、アプリケーションは、装置上でローカルサーバを開始してもよい。ここで、ローカルサーバは、ローカルサーバと同じ装置において実行中のアプリケーションにのみアクセス可能である。ローカルサーバ及びウェブブラウザの間の接続が確立されてもよい。ウェブブラウザは、ローカルサーバから支払い情報を受信し、ウェブブラウザにおけるフォームフィールドへ支払い情報を自動記入してもよい。いったん自動記入されると、ウェブブラウザにおけるフォームを提出することで購入が完了しうる。

【0012】

優位点として、本願で開示する実施形態は、ウェブブラウザにおけるデータの安全な自動記入を提供する。非接触カードによって生成された暗号文にてこ入れすることで、本開示の実施形態は、不正な活動のリスクを最小化しながら、ユーザの身元情報を安全に検証しうる。さらに、そうすることは、ユーザが非接触カードへのアクセスを有する場合にのみ自動記入動作が実行されることを保証し、このことは、サーバに対する暗号文検証を容易にする。さらに、Web View構成要素又はローカルサーバにてこ入れすることで、ウェブブラウザに課される所定の制限が回避されうる。例えば、いくつかのオペレーティングシステム及び／又はウェブブラウザは、ウェブブラウザがアカウントアプリケーションと直接的に通信することを許可しない可能性がある。従って、Web View構成要素及び／又はローカルサーバを用いることによって、これらの制限を克服しうる可能性があり、ユーザは、購入のための支払い情報を安全に自動記入できるようになる。さらに、開示した自動記入機能をするウェブブラウザに提供することで、多数の異なるウェブサイトが、すべてのウェブサイト又はアプリケーションに統合することを必要とすることなく、自動記入にてこ入れすることができる。

【0013】

本願で使用される記法及び命名法を概して参照すると、この後で述べる詳細な説明のうちの1つ又は複数の部分は、コンピュータ又はコンピュータネットワークで実行されるプログラム手順に関して提示されることがある。これらの手順の説明及び表現は、当業者によって、彼らの仕事の内容を他の当業者に最も有効に伝えるために使用される。本願では、また概して、手順は、所望の結果をもたらすための首尾一貫した一連の動作と考えられる。これらの動作は、物理量の物理的操作を必要とする。必ずしもではないが、通常、これらの量は、格納、転送、結合、比較、及びさもなければ操作されることが可能な、電氣的、磁氣的、又は光学的な信号の形式をとる。主に一般的な用法を理由として、これらの信号をビット、値、要素、シンボル、キャラクタ、項、番号などと呼ぶことが時々便利であることがわかる。しかしながら、これらの用語及び同様の用語のすべては、適切な物理量に関連付けられるべきであり、単に、それらの量に適用される便利なラベルであるということに注意すべきである。

【0014】

さらに、これらの操作は、多くの場合、人間であるオペレータによって実行される精神活動に一般的に関連付けられる、加算又は比較といった用語によって表される。しかしながら、1つ又は複数の実施形態の一部を形成する、本願で説明する動作のいずれにおいても、人間のオペレータのそのような能力は、不要であるか、又は、ほとんどの場合において望ましくない。むしろ、これらの動作はマシン動作である。様々な実施形態の動作を実行するための有用なマシンは、本願の開示内容に従って記述されて内部に格納されたコンピュータプログラムによって選択的に起動又は構成されるようなデジタルコンピュータ

を含み、及び／又は、必要とされる目的のために特に構成された装置又はディジタルコンピュータを含む。また、様々な実施形態は、これらの動作を実行するための装置又はシステムに関する。これらの装置は、必要とされる目的のために特に構成されてもよい。さまざまなこれらのマシンのための必要な構造は、提示した説明から明らかになるであろう。

【0015】

ここで図面を参照すると、図面全体にわたって、同様の参照符号は同様の構成要素を示すために使用される。下記の説明では、説明の目的で、多数の特定の詳細事項が、それらについての詳細な理解をもたらすために説明される。しかしながら、新規な実施形態はこれらの特定の詳細事項なしで実施されてもよいことが明らかとなりうる。他の例では、公知の構造物及び装置は、それらについての説明を容易にするために、ブロック図の形式で示される。特許請求の範囲内においてすべての変更、等価物、及び代替物をカバーすることを意図している。

【0016】

図1Aは、開示した実施形態に一致する、例示的な計算アーキテクチャ100を示し、これをシステムとも呼ぶ。図1A～図1Eに示す計算アーキテクチャ100は、所定のトポロジにおける限られた個数の構成要素を有するが、計算アーキテクチャ100は、所与の実施例での所望により、代替のトポロジにおいてより多数又はより少数の構成要素を含んでもよいことが認識されうる。

【0017】

計算アーキテクチャ100は、1つ又は複数の計算装置102、1つ又は複数の認証サーバ106、1つ又は複数の非接触カード104、及び1つ又は複数のマーチャントサーバ108を備える。非接触カード104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、支払いカード、スマートカードなどのような、任意のタイプのカードを表す。非接触カード104は、NFC、EMV標準、又は無線通信における他の短距離のプロトコルを介して、計算装置102の通信インターフェース126（本願では、「カードリーダー」、「無線カードリーダー」、及び／又は「無線通信インターフェース」とも呼ばれる）と通信するように構成された、無線周波識別（RFID）チップのような1つ又は複数の通信インターフェース126を備えてもよい。本願ではNFCを例示的な通信プロトコルとして使用しているが、本開示は、EMV標準、Bluetooth（登録商標）、及び／又はWi-Fi（登録商標）のような他のタイプの無線通信にも同様に適用可能である。

【0018】

計算装置102は、スマートフォン、タブレットコンピュータ、ウェアラブル装置、ラップトップ、携帯型ゲーム装置、仮想化された計算システム、マーチャント端末、POSシステム、サーバ、デスクトップコンピュータなどのような、任意個数及び任意タイプの計算装置を表す。計算装置102の一例としてモバイル装置が使用されてもよいが、本開示を制限するとみなされるべきでない。認証サーバ106及びマーチャントサーバ108は、サーバ、ワークステーション、計算クラスタ、クラウド計算プラットフォーム、仮想化された計算システムなどのような、任意のタイプの計算装置を表す。明確性のために図示していないが、計算装置102、非接触カード104、認証サーバ106、及びマーチャントサーバ108は各々、例えば、プログラム、コード、及び／又は命令を実行するための、1つ又は複数のプロセッサ回路を含む。

【0019】

図示するように、非接触カード104のメモリ110は、アプレット112、カウンタ114、マスタ鍵116、多様化鍵（diversified key）118、及び一意の顧客識別子（ID）120を含む。アプレット112は、本願で説明する動作を実行するように構成された、実行可能なコードである。カウンタ114、マスタ鍵116、多様化鍵118、及び顧客ID120は、詳細後述するように、システム100におけるセキュリティを提供するために使用される。

【0020】

10

20

30

40

50

図示するように、認証サーバ106のメモリ128は、認証アプリケーション130及びアカウントデータベース132を含む。アカウントデータベース132は、概して、アカウント保有者（例えば、1人又は複数人のユーザ）、アカウント保有者の1つ又は複数のアカウント、及びアカウントの1つ又は複数の非接触カード104に関連する情報を含む。認証サーバ106に関連付けられた金融機関に関連付けられた各非接触カードに関して、認証サーバ106は、マスタ鍵116及びカウンタ114の対応するインスタンスを格納してもよい。

【0021】

図示するように、計算装置102のメモリ136は、オペレーティングシステム138のインスタンスを含む。例示的なオペレーティングシステムは、Android（登録商標）OS、iOS（登録商標）、macOS（登録商標）、Linux（登録商標）、及びWindows（登録商標）オペレーティングシステムを含む。図示するように、オペレーティングシステム138は、アカウントアプリケーション140及びウェブブラウザ142を含む。アカウントアプリケーション140は、支払いカードのアクティベート、勘定残高の閲覧、品目の購入、支払いの処理などのような、様々なアカウント関連の動作をユーザが実行することを可能にする。いくつかの実施形態では、ユーザは、アカウントアプリケーション140の所定の機能にアクセスするために、認証クレデンシャルを用いて認証してもよい。例えば、認証クレデンシャルは、ユーザ名（又はログイン）及びパスワード、バイオメトリッククレデンシャル（例えば、指紋、顔IDなど）、などを含んでもよい。ウェブブラウザ142は、計算装置102がネットワーク148を介して（例えばインターネットを介して）情報にアクセスすることを可能にするアプリケーションである。例えば、ウェブブラウザ142を用いて、ユーザは、マーチャントサーバ108のメモリ144に格納されたウェブページ146のような、マーチャントサーバ108の1つ又は複数のリソースにアクセスしてもよい。それは、マーチャントサーバ108（又は他のホスティングするエンティティ）によってホスティングされた複数のウェブページのうちの1つであってもよい。

【0022】

マーチャントサーバ108によって提供されるウェブページ又は他の内容にアクセスするとき、ユーザは、ウェブブラウザ142を介して、購入するための1つ又は複数の製品、サービス、又は他の品目を選択してもよい。例えば、ユーザは、バスケットボール及びサッカーボールを購入することを希望してもよく、これらの品目を彼／彼女のショッピングカートに追加してもよい。購入を完了するために、ウェブページ146は、1つ又は複数の支払いフィールドを有するフォームを含んでもよい。支払いフィールドは、アカウント番号、有効期限、CVV、顧客名、及び顧客請求書発行住所のためのフィールドを含んでもよい。しかしながら、これらの支払いフィールドヘータが自動記入されることを防ぐ所定の制限が存在してもよい。例えば、OS及び／又はウェブブラウザ142は、支払いデータをフォームへ自動記入しないようにアカウントアプリケーション140を制限してもよい。しかしながら、優位点として、本願で開示する実施形態は、支払い情報をフォームのフォームフィールドへ自動記入するためのソリューションを提供する。

【0023】

自動記入処理を開始するために、ウェブブラウザ142は、例えば、フォームフィールドのメタデータ、フォームフィールドのうちの1つの受信選択、などに基づいて、ウェブページ146のフォームにおける1つ又は複数の支払いフィールドを識別してもよい。ウェブブラウザ142及び／又はウェブページ146は、次いで、アカウントアプリケーション140が計算装置102にインストールされているか否かを決定してもよい。ウェブブラウザ142及び／又はウェブページ146はアカウントアプリケーション140がインストールされているか否かを決定するために、任意の実行可能な技術を使用してもよい。例えば、iOSでは、ウェブブラウザ142及び／又はウェブページ146は、アカウントアプリケーション140に向けられたURIを開くことができるか否かを決定するために、canOpenURL（）メソッドを使用してもよい。本方法は、概して、URI

を開くことが可能であるか否かを示す情報を返してもよい。そうすることで、ウェブブラウザ142及び／又はウェブページ146は、アカウントアプリケーション140が計算装置102にインストールされることを決定できるようになる。

【0024】

Android OSのようないくつかのオペレーティングシステムでは、ウェブブラウザ142及び／又はウェブページ146は、アカウントアプリケーション140が装置102にインストールされているか否かを決定するために、コンテンツプロバイダサービスを使用してもよい。例えば、ウェブブラウザ142及び／又はウェブページ146は、アカウントアプリケーション140に向けられたURIをコンテンツプロバイダサービスに提供してもよく、それは、URIを開くことができるか否かを示す情報を返してもよい。そうすることで、ウェブブラウザ142及び／又はウェブページ146は、アカウントアプリケーション140が計算装置102にインストールされることを決定できるようになる。

10

【0025】

いくつかの実施形態では、任意のタイプのオペレーティングシステムに関してアカウントアプリケーション140が装置102にインストールされているか否かを決定するために、追加及び／又は代替の技術が使用されてもよい。例えば、いくつかのオペレーティングシステムは、ネイティブアプリケーションのネイティブコードが、所定の関数、例えば、iOSのcanOpenURL()メソッド又はAndroidのコンテンツプロバイダサービスを呼ぶことを必要としてもよい。そのような実施形態では、ウェブブラウザ142及び／又はウェブページ146は、アカウントアプリケーション140がインストールされていない場合を取り扱うウェブページ（例えば、概して、アカウントアプリケーション140がインストールされていないことを示すページ）にリダイレクトするコールバックとともに、タイムアウトしきい値（100ミリ秒、1秒、など）を有するタイマをスタートするコード（例えばJavaScript（登録商標））を実行してもよい。次いで、ウェブブラウザ142及び／又はウェブページ146は、アカウントアプリケーション140を起動しようとしてもよい。タイマが満了する前にアカウントアプリケーション140の起動に成功した場合、タイマはキャンセルされ、自動記入処理は本願で説明するように進む。しかしながら、タイマが満了する前にアカウントアプリケーション140が起動されない場合、ウェブブラウザ142はタイムアウトページにリダイレクトされ、自動記入処理は終了する。

20

30

【0026】

いったん、アカウントアプリケーション140がインストールされているとウェブブラウザ142及び／又はウェブページ146が決定すると、ウェブブラウザ142及び／又はウェブページ146は、アカウントアプリケーション140に向けられたURI152を生成してもよい。URI152の少なくとも一部は、OSに登録されているアカウントアプリケーション140に基づいて、アカウントアプリケーション140に向けられてもよい。実施例は、「example://auth」又は「www.example.com/auth」を含んでもよい。さらに、URI152は、1つ又は複数のパラメータを含んでもよい。パラメータは、マーチャントIDパラメータ、セッションIDパラメータ、及びアクションIDパラメータを含んでもよい。マーチャントIDパラメータは、マーチャントサーバ108に関連付けられた商人のような特定の商人に関連付けられてもよい。従って、アカウントアプリケーション140は、複数のマーチャントIDパラメータの各マーチャントIDパラメータを用いて、複数の商人のそれぞれを一意的に識別してもよい。そうすることで、アカウントアプリケーション140が、マーチャントIDに関連付けられたマーチャントサーバ108のアドレスを識別すること、及び／又は、マーチャントにIDに関連付けられた任意のウェブページ146のアドレスを識別することを可能にする。セッションIDパラメータは、マーチャントサーバ108に関して、ウェブブラウザ142における閲覧セッションを識別してもよい。例えば、セッションIDパラメータは、ショッピングカート、カート中の品目、以前に訪れられたページ、ウェブブラウザ142に表示された現在の

40

50

ページ（例えばウェブページ146）、などを識別するために使用されてもよい。アクションIDは、概して、実行されるアクション又は動作をアカウントアプリケーション140に指定してもよい。例えば、いくつかの実施形態では、アクションIDは、認証ページを開くようにアカウントアプリケーション140に命令してもよい。従って、URI152は、アカウントアプリケーション140の1つ又は複数のページに対するディープリンクであってもよい。URI152の実施例は、「example://auth?merchID=123&sessionId=ABC&actID=456」又は「www.example.com/?merchID=123&sessionId=ABC&actID=456」を含んでもよい。

【0027】

いったん生成されると、OSはURI152を処理してもよく、これにより、OSにアカウントアプリケーション140を開く、アクセスする、又はさもなければ表示することを実行させる。そうすることで、さらに、パラメータを含むURI152をアカウントアプリケーション140に提供する。URI152のアクションIDパラメータに基づいて、アカウントアプリケーション140は、本願で説明する自動記入技術を容易にするためのアカウント認証ページを開いてもよい。

【0028】

しかしながら、いくつかの実施形態では、ウェブブラウザ142及び／又はウェブページ146は、アカウントアプリケーション140がインストールされていることを決定することなく、URI152を生成及びアクセスする。URI152が、アクセスされたとき、アカウントアプリケーション140の起動に成功した場合、自動記入処理は、（アカウントアプリケーション140がインストールされているというウェブブラウザ142及び／又はウェブページ146による明示的な決定とともに、又は、当該決定なしで）本願で説明するように進む。さもなければ、アカウントアプリケーション140はインストールされず、ウェブブラウザ142は、アカウントアプリケーション140がインストールされていないことを示すタイムアウトページにリダイレクトされる。

【0029】

図1Bは、OSがURI152にアクセスし、アカウントアプリケーション140がアカウント認証ページをロードした場合の実施形態を示す。概して、アカウント認証ページは、例えば、ログイン及びパスワード、バイオメトリックス、又は非接触カード104によって生成された暗号文122に基づくワンタップ認証を介して、ユーザが彼らのアカウントを認証することを可能にする。

【0030】

図1Bに示す実施形態では、ユーザは、非接触カード104を計算装置102にタップしてもよい（又はさもなければ、非接触カード104を装置102の通信インターフェース126の通信範囲内に移動させてもよい）。非接触カード104のアプレット112は、次いで、暗号文122を生成してもよい。

【0031】

暗号文122は、非接触カード104の顧客ID120に基づいてもよい。暗号文122は、任意の適切な暗号技術に基づいて生成されてもよい。いくつかの実施形態では、アプレット112は、暗号文122を含むデータパッケージの一部として、暗号化されていない識別子（例えば、顧客ID120、非接触カード104の識別子、及び／又は他の任意の一意の識別子）を含んでもよい。少なくとも1つの実施形態では、データパッケージはNDEFファイルである。

【0032】

前述したように、計算アーキテクチャ100は、鍵多様化（key diversification）を実施してデータのセキュリティを確保するように構成される。このことは、本願では、鍵多様化技術とも呼ばれることがある。概して、認証サーバ106（又はもう1つの計算装置）及び非接触カード104には、同じマスタ鍵116（マスタ対称鍵とも呼ばれる）が提供されてもよい。より具体的には、各非接触カード104には、認証サーバ106において対応するペアを有する別個のマスタ鍵116がプログラミングされる。例えば、非

接触カード 104 が製造されるとき、非接触カード 104 のメモリ 110 に一意のマスタ鍵 116 がプログラミングされてもよい。同様に、一意のマスタ鍵 116 は、認証サーバ 106 のアカウントデータベース 132 における非接触カード 104 に関連付けられた顧客の記録に格納されてもよい（及び／又は、ハードウェアセキュリティモジュール（hardware security module: HSM）134 のような、異なる安全な場所に格納されてもよい）。マスタ鍵 116 は、非接触カード 104 及び認証サーバ 106 以外のすべての当事者に対して秘密にされ、それによって、システム 100 のセキュリティを向上させる。いくつかの実施形態では、非接触カード 104 のアプレット 112 は、暗号アルゴリズムへの入力としてマスタ鍵 116 及びデータを用いて、データ（例えば顧客 ID 120）を暗号化及び／又は復号してもよい。例えば、マスタ鍵 116 を用いて顧客 ID 120 を暗号化することで、暗号文 122 をもたらしてもよい。同様に、認証サーバ 106 は、対応するマスタ鍵 116 を用いて、非接触カード 104 に関連付けられたデータを暗号化及び／又は復号してもよい。

10

【0033】

いくつかの実施形態では、非接触カード 104 及び認証サーバ 106 のマスタ鍵 116 は、鍵多様化を用いてセキュリティを向上させるために、カウンタ 114 に関連して使用されてもよい。カウンタ 114 は、非接触カード 104 及び認証サーバ 106 の間で同期される値を含む。例えば、カウンタ 114 は、非接触カード 104 及び認証サーバ 106 の間で（及び／又は、非接触カード 104 及び計算装置 102 の間で）データが交換されるごとに变化する番号を含んでもよい。概して、アプレット 112 は、暗号アルゴリズムへの入力としてマスタ鍵 116、一意の顧客 ID 120、及び多様化ファクタを提供し、それによって、多様化鍵 118 を生成してもよい。いくつかの実施形態では、多様化ファクタはカウンタ 114 である。多様化鍵 118 は、次いで、多様化ファクタ（例えばカウンタ 114）又は他の機密性データのような何らかのデータを暗号化するために使用されてもよい。アプレット 112 及び認証サーバ 106 は、同じタイプのデータを暗号化することで暗号文 122 の復号及び／又は検証処理を容易にするように構成されてもよい。

20

【0034】

より一般的には、（例えば、認証サーバ 106 及び／又は計算装置 102 への）データの送信を準備するとき、非接触カード 104 のアプレット 112 は、カウンタ 114 をインクリメントしてもよい。非接触カード 104 のアプレット 112 は、次いで、暗号アルゴリズムへの入力としてマスタ鍵 116、顧客 ID 120、及びカウンタ 114 を提供してもよく、それは多様化鍵 118 を出力として生成する。暗号アルゴリズムは、暗号化アルゴリズム、ハッシュに基づくメッセージ認証コード（hash-based message authentication code: HMAC）アルゴリズム、暗号に基づくメッセージ認証コード（cipher-based message authentication code: CMAC）アルゴリズムなどを含んでもよい。暗号アルゴリズムの非限定的な実施例は、3DES 又は AES 107 のような対称暗号化アルゴリズム、HMAC-SHA-256 のような対称 HMAC アルゴリズム、及び AES-CMAC のような対称 CMAC アルゴリズムを含んでもよい。鍵多様化技術の実施例は、2018 年 11 月 29 日に出願された、米国特許出願第 16 / 205119 号においてより詳しく説明されている。前述の特許出願全体は、援用によって本願に組み込まれる。

30

40

【0035】

アプレット 112 は、次いで、暗号アルゴリズムへの入力として多様化鍵 118 及びデータを用いて、何らかのデータ（例えば、一意の顧客 ID 120、カウンタ 114、コマンド、及び／又は他の任意のデータ）を暗号化してもよい。例えば、一意の顧客 ID 120、多様化鍵 118 を暗号化することで、暗号化された一意の顧客 ID 120（例えば暗号文 122）をもたらしてもよい。

【0036】

いくつかの実施形態では、例えば、暗号機能に対する入力のうちの 1 つ又は複数の部分に基づいて、2 つの多様化鍵 118 が生成されてもよい。いくつかの実施形態では、2 つ

50

の多様化鍵 118 は、2 つの別個のマスタ鍵 116、一意の顧客 ID 120、及びカウンタ 114 に基づいて生成される。そのような実施形態では、メッセージ認証コード (message authentication code: MAC) は、多様化鍵 118 の一方を用いて生成され、MAC は、多様化鍵 118 の他方を用いて暗号化されてもよい。MAC は、機密性データ、一意の顧客 ID 120、カウンタ 114 などのような、MAC アルゴリズムに対する任意の適切なデータ入力に基づいて生成されてもよい。より一般的には、アプレット 112 及び認証サーバ 106 は、同じデータに基づいて MAC を生成するように構成されてもよい。いくつかの実施形態では、暗号文 122 は、NDEF ファイルのようなデータパッケージに含まれる。アカウントアプリケーション 140 は、次いで、計算装置 102 の通信インターフェース 126 を介して、暗号文 122 を含むデータパッケージを読み出してもよい。

10

【0037】

図 1C は、アカウントアプリケーション 140 が、暗号文 122 を含むデータパッケージを認証サーバ 106 に送信する場合の実施形態を示す。認証サーバ 106 は、認証サーバ 106 によって格納されたマスタ鍵 116 のインスタンスに少なくとも部分的に基づいて、検証のために、暗号文 122 を認証アプリケーション 130 及び／又は HSM 134 に提供してもよい。いくつかの実施形態では、認証アプリケーション 130 及び／又は HSM 134 は、暗号文 122 とともにサーバ 106 に提供された、暗号化されていない顧客 ID 120 を用いて、マスタ鍵 116 及びカウンタ 114 を識別してもよい。いくつかの実施例では、認証アプリケーション 130 は、暗号アルゴリズムへの入力としてマスタ鍵 116、一意の顧客 ID 120、及びカウンタ 114 を提供してもよく、それは 1 つ又は複数の多様化鍵 118 を出力として生成する。結果として生じる多様化鍵 118 は、非接触カード 104 の多様化鍵 118 に対応してもよく、それは、暗号文 122 を復号するため、及び／又は、いったん復号されると MAC を検証するために使用されてもよい。例えば、認証サーバ 106 は、アプレット 112 と同じデータ、例えば、機密性データ、一意の顧客 ID 120、及び／又はカウンタ 116 に基づいて、MAC を生成してもよい。認証サーバ 106 によって生成された MAC が、暗号文 122 における復号された MAC と一致する場合、認証サーバ 106 は暗号文 122 を検証し、又はさもなければ認証してもよい。

20

【0038】

使用される検証技術にかかわらず、認証アプリケーション 130 及び／又は HSM 134 は、暗号文 122 の復号及び MAC の検証に成功し、それによって、暗号文 122 を検証又は認証しうる。

30

【0039】

復号に成功した場合、認証アプリケーション 130 は、復号結果 150 をアカウントアプリケーション 140 に送信してもよい。いくつかの実施形態では、復号結果 150 は、マーチャントサーバ 108 に係る購入で支払うために、支払いフォームへ自動記入されるデータを含んでもよい。しかしながら、認証アプリケーション 130 が、暗号文 122 を復号して予期する結果 (例えば、非接触カード 104 に関連付けられたアカウントの顧客 ID 120) を得られない場合、認証アプリケーション 130 は暗号文 122 を検証しない。そのような実施例では、認証アプリケーション 130 は、自動記入処理を終了すると決定する。認証アプリケーション 130 は、復号に失敗したことを示す情報を計算装置 102 に送信してもよい。

40

【0040】

図 1D は、認証アプリケーション 130 が復号結果 150 をアカウントアプリケーション 140 に送信する場合の実施形態を示す。復号結果 150 は、概して、暗号文 122 が復号されたか否かを反映する。図 1D に示す実施例では、復号結果 150 は、認証サーバ 106 が暗号文 122 を復号したことを示してもよい。そうすることで、アカウントアプリケーション 140 が、自動記入処理を継続する前に、暗号文 122 の復号に成功したと決定することを可能にし、それによって、セキュリティを向上させる。

50

【0041】

図示するように、認証サーバ106はさらに、自動記入データ124をアカウントアプリケーション140に送信してもよい。復号結果150とともに送信されるように示したが、自動記入データ124は、復号結果150と別個に送信されてもよい。さらに、いくつかの実施形態では、自動記入データ124は、計算装置102に対する非接触カード104の他のタップに応答してサーバ106から受信されてもよい。それは他の暗号文を生成させ、それは認証サーバ106によって検証される。他の実施形態では、自動記入データ124は、非接触カード104から直接的に（例えば、通信インターフェース126を介した直接的な読み取りを介して）受信される。他の実施形態では、アカウントアプリケーション140は、計算装置102上に格納されたローカルデータベースにおける自動記入データ124を検索する。自動記入データ124は、概して、非接触カード104のアカウント番号、非接触カード104の有効期限、非接触カード104のC V V、非接触カード104に関連付けられた顧客名、及び非接触カード104に関連付けられた顧客請求書発行住所を含んでもよい。いくつかの実施形態では、アカウント番号は、非接触カード104に関連付けたワンタイム使用の仮想アカウント番号であってもよい。

10

【0042】

いくつかの実施形態では、認証サーバ106は、自動記入データ124として支払いトークンを生成してもよい。そのような実施形態では、認証サーバ106は、マーチャントサーバ108及び／又は計算装置102に支払いトークンを提供してもよい。

【0043】

図示するように、復号結果150を受信することに応答して、アカウントアプリケーション140は、Web View構成要素154を起動してもよい。Web View構成要素154は、概して、ウェブページ146のようなウェブコンテンツにアクセス及び表示するように構成されるが、ウェブブラウザ142のいくつかの機能を欠いている。言いかえると、Web View構成要素154は、ウェブブラウザ142とは異なる、アカウントアプリケーション140のアプリ内ウェブブラウザである。概して、アカウントアプリケーション140は、アカウントアプリケーション140内のWeb View構成要素154を起動することで、アカウントアプリケーション140内のウェブに基づくコンテンツをロードしてもよい。

20

【0044】

アカウントアプリケーション140は、Web View構成要素154により、マーチャントサーバ108に対するウェブブラウザ142からのユーザの閲覧セッションを受信及び復元させてもよい。例えば、アカウントアプリケーション140は、URI152のマーチャントID及びセッションIDを用いて、ウェブページ146に向けられたURL（及び／又はURI）を生成してもよい。ウェブページ146に向けられたURLは、ウェブブラウザ142からの閲覧セッションを維持しながら、ウェブページが146 Web View構成要素154においてロードされることを可能にするためのパラメータを含んでもよい。例えば、マーチャントIDはベースURL（例えば、www.example.com）に関連付けられてもよく、セッションIDは、ウェブページ146及び／又はマーチャントサーバ108に向けられるURLを生成するように、ベースURLのパラメータとして含まれてもよい。実施例は、「www.example.com/page.html?sessionId=ABC」を含んでもよい。いったんアカウントアプリケーション140によって生成されたURLがWeb View構成要素154によってアクセスされると、Web View構成要素154は、ウェブページ146をロードして、ウェブブラウザ142からのユーザの閲覧セッションを複製してもよい。例えば、支払いフォームを含むウェブページ146が、Web View構成要素154においてレンダリングされてもよく、これにより、ユーザは、ウェブブラウザ142における彼／彼女のショッピングカートに以前に追加した1つ又は複数の品目を購入できるようになる。引き続き前述の実施例を参照すると、Web View構成要素154は、バスケットボール及びサッカーボールを含む、ユーザのショッピングカートを反映するウェブページ146をロードしてもよい。

30

40

50

【0045】

優位点として、Web View構成要素154は、ウェブページ146の1つ又は複数の支払いフィールドへ自動記入データ124を自動記入してもよい。いくつかの実施形態では、Web View構成要素154は、アカウントアプリケーション140によって提供される自動記入サービスを使用する。いくつかの実施形態では、Web View構成要素154は、オペレーティングシステム138によって提供される自動記入サービスを使用する。使用される自動記入技術にかかわらず、ユーザは、自動記入されたデータを含むフォームを提出して購入を完了してもよい。

【0046】

認証サーバ106が支払いトークンを生成する実施形態では、Web View構成要素154によってロードされたウェブページ146は、支払いトークンを含んでもよい。支払いトークンは、マーチャントサーバ108によってWeb View構成要素154に提供されてもよく、又は、アカウントアプリケーション140によってWeb View構成要素154に提供されてもよい。支払いトークンは、購入を処理するために使用されてもよい。

10

【0047】

図1Eは、Web View構成要素154が、ウェブページ146のフォームフィールドへ記入された自動記入データ124を用いて支払いを処理するためのトランザクションパッケージ156を生成する場合の実施形態を示す。概して、トランザクションパッケージ156は、ハイパーテキスト転送プロトコル（HTTP）に従って送信されてもよい。いったん受信されると、マーチャントサーバ108は、自動記入データ124を用いて、トランザクションに関する支払いを処理してもよい。マーチャントサーバ108は、次いで、トランザクションデータベース158においてトランザクションに関するトランザクションレコード160を生成してもよい。しかしながら、前述したように、いくつかの実施形態では、トランザクションに関して支払うために、自動記入データ124の代わりに支払いトークンが使用される。

20

【0048】

図2Aは、様々な実施形態に係る、ローカルサーバを用いてウェブブラウザ142へデータを自動記入するための例示的な概略図200を示す。図2A～図2Eに示す計算アーキテクチャ200は、所定のトポロジにおける限られた個数の構成要素を有するが、計算アーキテクチャ200は、所与の実施例での所望により、代替のトポロジにおいてより多数又はより少数の構成要素を含んでもよいことが認識されうる。

30

【0049】

図2Aに示すように、ユーザは、ウェブブラウザ142を用いることで、マーチャントサーバ108を介して購入する1つ又は複数の品目を選択してもよい。例えば、ユーザは、オレンジ及びりんごを購入することを希望し、彼／彼女のショッピングカートにおいてこれらの品目を有してもよい。購入を完了するために、ウェブページ146は、1つ又は複数の支払いフィールドを有するフォームを含んでもよい。支払いフィールドは、アカウント番号、有効期限、CVV、顧客名、及び顧客請求書発行住所のためのフィールドを含んでもよい。しかしながら、前述したように、これらの支払いフィールドへデータが自動記入されることを防ぐ所定の制限が存在してもよい。例えば、OS及び／又はウェブブラウザ142は、支払いデータをフォームへ自動記入しないようにアカウントアプリケーション140を制限してもよい。しかしながら、優位点として、アカウントアプリケーション140は、ローカルサーバを用いて、ウェブページ146のフォームのフォームフィールドへ支払い情報を自動記入してもよい。

40

【0050】

自動記入処理を開始するために、ウェブブラウザ142は、ウェブページ146のフォームにおける1つ又は複数の支払いフィールドを識別してもよい。ウェブブラウザ142及び／又はウェブページ146は、次いで、アカウントアプリケーション140が計算装置102にインストールされているか否かを決定してもよい。ウェブブラウザ142及び

50

／又はウェブページ146はアカウントアプリケーション140がインストールされているか否かを決定するために、任意の実行可能な技術を使用してもよい。例えば、iOSのようないくつかのオペレーティングシステムでは、ウェブブラウザ142及び／又はウェブページ146は、アカウントアプリケーション140に向けられたURIを開くことができるか否かを決定するために、canOpenURL()メソッドを使用してもよい。本方法は、概して、URIを開くことが可能であるか否かを示す情報を返してもよい。そうすることで、ウェブブラウザ142及び／又はウェブページ146は、アカウントアプリケーション140が計算装置102にインストールされることを決定できるようになる。

【0051】

さらに、Android OSのようないくつかのオペレーティングシステムでは、ウェブブラウザ142及び／又はウェブページ146は、アカウントアプリケーション140が装置102にインストールされているか否かを決定するために、コンテンツプロバイダサービスを使用してもよい。例えば、ウェブブラウザ142及び／又はウェブページ146は、アカウントアプリケーション140に向けられたURIをコンテンツプロバイダサービスに提供してもよく、それは、URIを開くことができるか否かを示す情報を返してもよい。そうすることで、ウェブブラウザ142及び／又はウェブページ146は、アカウントアプリケーション140が計算装置102にインストールされることを決定できるようになる。

【0052】

いったん、アカウントアプリケーション140がインストールされているとウェブブラウザ142及び／又はウェブページ146が決定すると、ウェブブラウザ142及び／又はウェブページ146は、アカウントアプリケーション140に向けられたURI202を生成してもよい。URI202は、URI152を生成する場合と同じ技術に基づいて生成されてもよい。URI202の少なくとも一部は、OSに登録されているアカウントアプリケーション140に基づいて、アカウントアプリケーション140に向けられてもよい。さらに、URI202は、1つ又は複数のパラメータを含んでもよい。パラメータは、マーチャントIDパラメータ、セッションIDパラメータ、及びアクションIDパラメータを含んでもよい。前述したように、マーチャントIDパラメータは、マーチャントサーバ108に関連付けられた商人のような特定の商人に関連付けられてもよい。従って、前述したように、複数のマーチャントのそれぞれは、各マーチャントIDパラメータによって一意的に識別されてもよい。そうすることで、アカウントアプリケーション140が、マーチャントIDに関連付けられたマーチャントサーバ108を識別すること、及び／又は、マーチャントにIDに関連付けられた任意のウェブページ146を識別することを可能にする。セッションIDパラメータは、マーチャントサーバ108に関して、ウェブブラウザ142における閲覧セッションを識別してもよい。例えば、セッションIDパラメータは、ショッピングカート、ショッピングカート中の品目、以前に訪れられたページ、ウェブブラウザ142に表示された現在のページ（例えばウェブページ146）、などを識別するために使用されてもよい。アクションIDは、概して、実行されるアクション又は動作をアカウントアプリケーション140に指定してもよい。例えば、いくつかの実施形態では、アクションIDは、認証ページを開くようにアカウントアプリケーション140に命令してもよい。従って、URI202は、アカウントアプリケーション140の1つ又は複数のページに対するディープリンクであってもよい。

【0053】

いったん生成されると、OSはURI202を処理してもよく、これにより、OSにアカウントアプリケーション140を開く、アクセスする、又はさもなければ表示することを実行させる。そうすることで、さらに、パラメータを含むURI202をアカウントアプリケーション140に提供する。URI202のアクションIDパラメータに基づいて、アカウントアプリケーション140は、本願で説明する自動記入技術を容易にするためのアカウント認証ページを開いてもよい。

【0054】

前述したように、いくつかの実施形態では、ウェブブラウザ142及び／又はウェブページ146は、アカウントアプリケーション140がインストールされていると予め決定することなく、タイマを使用し、URI202の起動を試みてもよい。そのような実施形態では、URI202に基づくアカウントアプリケーション140の起動に成功した場合、自動記入処理は本願で説明するように進む。しかしながら、アカウントアプリケーション140が装置上で起動することなく時間が満了した場合、自動記入処理は終了する。

【0055】

図2Bは、OSがURI202にアクセスし、アカウントアプリケーション140がアカウント認証ページをロードした場合の実施形態を示す。概して、アカウント認証ページは、例えば、ログイン及びパスワード、バイオメトリックス、又は非接触カード104によって生成された暗号文122に基づくワンタップ認証を介して、ユーザが彼らのアカウントを認証することを可能にする。

10

【0056】

図2Bに示す実施形態では、ユーザは、非接触カード104を計算装置102にタップしてもよい（又はさもないければ、非接触カード104を装置102の通信インターフェース126の通信範囲内に移動させてもよい）。非接触カード104のアプレット112は、次いで、前述したように、他の暗号文122を生成してもよい。アカウントアプリケーション140は、次いで、通信インターフェース126を介して他の暗号文122を読み出してもよい。

20

【0057】

図2Cは、アカウントアプリケーション140が、他の暗号文122を含むデータパッケージを認証サーバ106に送信する場合の実施形態を示す。認証サーバ106は、前述したように、暗号文122を検証するか、又はさもないければ認証してもよい。

【0058】

復号の成功に基づいて、認証アプリケーション130は、他の復号結果をアカウントアプリケーション140に送信してもよい。前述したように、復号結果は、マーチャントサーバ108に係る購入で支払うために、支払いフォームへ自動記入されるデータを含んでもよい。

【0059】

30

図2Dは、認証アプリケーション130が復号結果204をアカウントアプリケーション140に送信する場合の実施形態を示す。図2Dに示す実施例では、復号結果204は、認証サーバ106が図2B～図2Cの他の暗号文122を復号したことを示してもよい。そうすることで、アカウントアプリケーション140が、自動記入処理を継続する前に、他の暗号文122の復号に成功したと決定することを可能にし、それによって、セキュリティを向上させる。

【0060】

図示するように、認証サーバ106はさらに、自動記入データ124をアカウントアプリケーション140に送信してもよい。復号結果204とともに送信されるように示したが、自動記入データ124は、復号結果204と別個に送信されてもよい。さらに、いくつかの実施形態では、自動記入データ124は、計算装置102に対する非接触カード104の他のタップに応答して送信されてもよい。それは、認証サーバ106によって他の暗号文を生成及び検証させる。他の実施形態では、自動記入データ124は、非接触カード104から直接的に受信される。他の実施形態では、アカウントアプリケーション140は、計算装置102上に格納されたローカルデータベースにおける自動記入データ124を検索する。自動記入データ124は、概して、非接触カード104のアカウント番号、非接触カード104の有効期限、非接触カード104のC V V、非接触カード104に関連付けられた顧客名、及び非接触カード104に関連付けられた顧客請求書発行住所を含んでもよい。いくつかの実施形態では、アカウント番号は、非接触カード104に関連付けたワンタイム使用の仮想アカウント番号であってもよい。

40

50

【0061】

図示するように、復号結果204を受信することに対応して、アカウントアプリケーション140は、ローカルサーバ210を起動してもよい。ローカルサーバ210は、TCP/IPサーバ、HTTPサーバ、HTTPS（Hypertext Transfer Protocol Secure）サーバ、ストリーミングサーバなどのような、任意のタイプのサーバであってもよい。しかしながら、ローカルアプリケーション（例えば、計算装置102において実行されるアプリケーション）のみが、ローカルサーバ210にアクセスしてもよい。OSは、外部ソースから（例えばネットワーク148を介して）ローカルサーバ210にアクセスする試みを制限してもよい。アカウントアプリケーション140は、特定のポート番号におけるローカルサーバ210を開始してもよい。アカウントアプリケーション140は、予め決められたポート番号などを用いて、ポート番号をランダムに生成することのような、任意の実行可能な選択方式に従ってポートを選択してもよい。ローカルサーバを用いてデータを交換することは、2020年5月18日に出願された米国特許出願第16／876473号と、2020年5月18日に出願された出願第16／876549号とに詳述される。前述の特許出願全体は、援用によって本願に組み込まれる。

10

【0062】

アカウントアプリケーション140は、ウェブブラウザ142によりローカルサーバ210との接続を確立させてもよい。いくつかの実施形態では、アカウントアプリケーション140は、ウェブブラウザ142に向けられたURIを生成し、ローカルサーバ210との接続を確立するために必要とされる関連パラメータ（例えば、IPアドレス、ユーザー名、パスワード、ポートなど）を含んでもよい。OSはURIにアクセスしてもよく、それは、ウェブブラウザ142を起動し、パラメータをウェブブラウザ142に提供する。ウェブブラウザ142は、マーチャントサーバ108に対する閲覧セッションをなお維持し、次いで、ウェブブラウザ142は、ローカルサーバ210に接続し、ローカルサーバ210から自動記入データ124を受信してもよい。

20

【0063】

優位点として、いったんローカルサーバ210から受信されると、ウェブブラウザ142は、例えば、オレンジ及びりんごに支払うために、ウェブページ146の1つ又は複数の支払いフィールドへ自動記入データ124を自動記入してもよい。いくつかの実施形態では、ウェブブラウザ142は、自動記入データ124をフォームフィールドに自動記入するために、JavaScript（登録商標）、例えば、ウェブブラウザ142によって提供される自動記入サービスを使用する。いくつかの実施形態では、ウェブブラウザ142は、自動記入データ124をフォームフィールドに自動記入するために、オペレーティングシステム138によって提供される自動記入サービスを使用する。使用される自動記入サービスにかかわらず、ユーザは、ウェブブラウザ142を介して、自動記入されたデータを含むフォームを提出して購入を完了してもよい。

30

【0064】

いくつかの実施形態では、認証サーバ106は、自動記入データ124として支払いトークンを生成してもよい。そのような実施形態では、認証サーバ106は、マーチャントサーバ108及び／又は計算装置102に支払いトークンを提供してもよい。そのような実施形態では、アカウントアプリケーション140は、認証サーバ106又はマーチャントサーバ108から支払いトークンを受信してもよい。支払いトークンは、アカウントアプリケーション140によってローカルサーバ210に提供されてもよく、それは、トークンをウェブブラウザ142に提供する。支払いトークンは、ウェブブラウザ142を介して購入を処理するために使用されてもよい。

40

【0065】

いくつかの実施形態では、アカウントアプリケーション140は、ローカルサーバ210を開始するのではなく、オペレーティングシステム138のコンテンツプロバイダサービスに自動記入データ124を提供してもよい。そのような実施形態では、ウェブブラウザ142及び／又はウェブページ146は、コンテンツプロバイダサービスから自動記入

50

データ124を受信してもよい。ウェブブラウザ142は、次いで、ウェブブラウザ142の自動記入サービス及び／又はオペレーティングシステム138の自動記入サービスを用いて、自動記入データ124をフォームフィールドへ自動記入してもよい。

【0066】

図2Eは、ウェブブラウザ142154が、ウェブページ146のフォームフィールドへ記入された自動記入データ124を用いて、りんご及びオレンジの支払いを処理するためのトランザクションパッケージ206を生成する場合の実施形態を示す。概して、トランザクションパッケージ206は、ハイパーテキスト転送プロトコル（HTTP）に従って送信されてもよい。いったん受信されると、マーチャントサーバ108は、自動記入データ124を用いて、トランザクションに関する支払いを処理してもよい。マーチャントサーバ108は、次いで、トランザクションデータベース158においてトランザクションに関するトランザクションレコード208を生成してもよい。しかしながら、前述したように、いくつかの実施形態では、トランザクションに関して支払うために、自動記入データ124の代わりに支払いトークンが使用される。

【0067】

図3Aは、非接触カードを用いてウェブブラウザへデータを自動記入する例示的な実施形態を示す概略図300である。図示するように、図3Aは、ウェブブラウザ142を実行するモバイル計算装置102を含む。ウェブブラウザ142は、ウェブページ146のようなウェブページを表示してもよい。例えば、ウェブページ146は、ユーザが注文して注文に関する支払い情報を提供することを可能にするウェブページ146であってもよい。図示するように、ウェブページ146は、フィールド301～305を有する支払いフォームを含み、ここで、フィールド301は名前フィールドであり、フィールド302はアカウント番号フィールドであり、フィールド303は有効期限フィールドであり、フィールド304はC V Vフィールドであり、フィールド305は住所フィールドである。

【0068】

ウェブページ146は、ユーザが自動記入処理を開始して支払い情報をフォームフィールド301～305へ自動記入することを可能にする、選択可能な構成要素308をさらに含む。Web Viewの実施例を参照して説明したが、図3A～図3Dは、ローカルサーバの実施例にも同様に適用可能である。実施形態は、このコンテキストに限定されない。

【0069】

図3Bは、ユーザが構成要素308を選択して自動記入処理を開始した場合の実施形態を示す概略図310である。概して、そうすることで、ウェブブラウザ142により、アカウントアプリケーション140に向けられたURIを生成させてもよく、これにより、計算装置102によりアカウントアプリケーション140を表示させる。URIのパラメータに基づいて、アカウントアプリケーション140は、通知306によって示すように、ユーザが彼／彼女の非接触カード104を計算装置102にタップすることを要求する認証ページを出力する。そうすることで、非接触カード104により暗号文を生成させ、暗号文は認証サーバ106によって検証される。図示するように、図3Bにおいて、認証サーバ106は暗号文を検証する。そうすることで、認証サーバ106により、支払い情報（例えば、アカウント番号、有効期限、C V V）をアカウントアプリケーション140に送信させてもよい。アカウントアプリケーション140がアカウント所有者の名前及び住所の値をローカルに格納していない場合、認証サーバ106はさらにアカウント所有者の名前及び住所を提供してもよい。

【0070】

図3Cは、非接触カード104によって生成された暗号文をサーバが検証したことを示す情報をアカウントアプリケーション140が認証サーバ106から受信する場合の実施形態を示す概略図320である。前述したように、認証サーバ106は、フォームフィールド301～306に自動記入するための支払い情報を含んでもよい。それに応答して、アカウントアプリケーション140は、Web View構成要素154を起動する。We

10

20

30

40

50

Web View構成要素154は、アカウントアプリケーション140によって生成されたURLを用いて、例えば、図3Aにおいて生成されたURIのマーチャントID及びセッションIDに基づいて、Web View構成要素154において図3Aの閲覧セッションを複製する。

【0071】

図示するように、Web View構成要素154は、支払い情報と任意の個人的に識別可能な情報とをフォームフィールドへ自動記入してもよい。より具体的には、Web View構成要素154は、ユーザの名前を名前フィールド301に、アカウント番号をアカウント番号フィールド302に、有効期限を有効期限フィールド303に、CVVをCVVフィールド304に、及び住所を住所フィールド305に自動記入してもよい。ユーザは、次いで、ボタン311を用いて購入を完了してもよく、このことは、マーチャントサーバ108により、自動記入されたデータを用いて支払いを処理させる。

10

【0072】

図3Dは、Web View構成要素154における確認ページを示す概略図330である。確認ページは、概して、フォームフィールド301～305へ自動記入されたデータを用いて購入が完了したことを反映する。実施形態はこのコンテキストに限定されない。

【0073】

開示された実施形態に関する動作が、下記の図面を参照してさらに説明されうる。図面のうちのいくつかは論理フローを含みうる。本願で提示するそのような図面は特定の論理フローを含むことがあるが、論理フローは、本願で説明する全体機能を実施する方法の例を単に提供するということが認識されうる。さらに、所与の論理フローは、別途示していない限り、提示した順序に実行されることを必ずしも必要としない。また、いくつかの実施形態では、論理フローで説明するすべての動作が必要とされるわけではない可能性がある。さらに、所与の論理フローは、ハードウェア構成要素によって実施されてもよく、プロセッサによって実行されるソフトウェア構成要素によって実施されてもよく、又はそれらの任意の組み合わせによって実施されてもよい。実施形態はこのコンテキストに限定されない。

20

【0074】

図4は、論理フロー400の実施形態を示す。論理フロー400は、本願で説明する1つ又は複数の実施形態によって実行される動作の一部又はすべてを表しうる。例えば、論理フロー400は、Web View構成要素154を用いてデータを自動記入する動作の一部又はすべてを含んでもよい。実施形態は、このコンテキストに限定されない。

30

【0075】

ブロック402において、ルーチン400は、計算装置102のプロセッサにおいて実行されるウェブブラウザによって、ウェブページ146における支払いフィールドを識別する。支払いフィールドは、フォームの複数の支払いフィールドのうちの1つであってもよい。ブロック404において、ルーチン400は、ウェブブラウザ142によって、非接触カード104の発行者に関連付けられたアカウントアプリケーション140が計算装置102にインストールされていることを決定する。ウェブブラウザ142は、アカウントアプリケーション140がインストールされていることを決定するために、オペレーティングシステム138によって提供される1つ又は複数の機能を使用してもよい。ブロック406において、ルーチン400は、ウェブブラウザ142によって、アカウントアプリケーション140に向けられたURI (uniform resource identifier) であって、マーチャント識別子パラメータ、セッション識別子パラメータ、及びアクション識別子パラメータを含むURIを生成する。

40

【0076】

ブロック408において、ルーチン400は、プロセッサ上で実行されるOSによって、URIに基づいたアカウントアプリケーション140を起動する。ブロック410において、ルーチン400は、アカウントアプリケーション140によって、URIのアクション識別子パラメータに基づいて、非接触カード104によって生成された暗号文に基づ

50

いて、非接触カードに関連付けられたアカウントを認証する。ブロック 4 1 2 において、ルーチン 4 0 0 は、アカウントアプリケーション 1 4 0 によって、認証に基づいて、非接触カード 1 0 4 に関連付けられた支払い情報を受信する。支払い情報は、非接触カード 1 0 4 のアカウント番号、有効期限、及び C V V を含んでもよい。支払い情報はさらに、アカウント保有者名及び／又は住所を含んでもよい。ブロック 4 1 4 において、ルーチン 4 0 0 は、アカウントアプリケーション 1 4 0 の Web View 構成要素 1 5 4 によって、ウェブページ 1 4 6 にアクセスする。マーチャントサーバ 1 0 8 は、次いで、ユーザの閲覧セッション及びウェブページ 1 4 6 に関連付けられたすべてのデータを Web View 構成要素 1 5 4 に送信してもよい。そうすることで、Web View 構成要素 1 5 4 においてウェブブラウザ 1 4 2 からのユーザの閲覧セッションを複製し、又はさもなければ復元する。ブロック 4 1 6 において、Web View 構成要素 1 5 4 は、ウェブページ 1 4 6 における支払いフィールドへ支払い情報を自動記入する。複数のフィールドが存在する場合、Web View 構成要素 1 5 4 は、情報を適切なフィールドへ自動記入してもよい。ブロック 4 1 8 において、ルーチン 4 0 0 は、Web View 構成要素 1 5 4 によって、ウェブページの支払いフィールドへ自動記入された支払い情報に基づいて、トランザクションを処理する。

10

【0077】

図 5 は、論理フロー 5 0 0 の実施形態を示す。論理フロー 5 0 0 は、本願で説明する 1 つ又は複数の実施形態によって実行される動作の一部又はすべてを表しうる。例えば、論理フロー 5 0 0 は、ローカルサーバ 2 1 0 を用いてデータを自動記入する動作の一部又はすべてを含んでもよい。実施形態は、このコンテキストに限定されない。

20

【0078】

ブロック 5 0 2 において、ルーチン 5 0 0 は、装置のプロセッサにおいて実行されるウェブブラウザによって、ウェブページ 1 4 6 における支払いフィールドを識別する。支払いフィールドは、フォームの複数の支払いフィールドのうちの 1 つであってもよい。ブロック 5 0 4 において、ルーチン 5 0 0 は、ウェブブラウザ 1 4 2 によって、非接触カード 1 0 4 の発行者に関連付けられたアカウントアプリケーション 1 4 0 が装置にインストールされていることを決定する。ウェブブラウザ 1 4 2 は、アカウントアプリケーション 1 4 0 がインストールされていることを決定するために、オペレーティングシステム 1 3 8 によって提供される 1 つ又は複数の機能を使用してもよい。ブロック 5 0 6 において、ルーチン 5 0 0 は、ウェブブラウザ 1 4 2 によって、アカウントアプリケーション 1 4 0 に向けられた URI (uniform resource identifier) であって、マーチャント識別子パラメータ、セッション識別子パラメータ、及びアクション識別子パラメータを含む URI を生成する。

30

【0079】

ブロック 5 0 8 において、ルーチン 5 0 0 は、プロセッサにおいて実行されるモバイルオペレーティングシステム (OS) によって、URI に基づいてアカウントアプリケーション 1 4 0 を起動する。ブロック 5 1 0 において、ルーチン 5 0 0 は、アカウントアプリケーション 1 4 0 によって、URI のアクション識別子パラメータに基づいて、非接触カードによって生成された暗号文に基づいて、非接触カード 1 0 4 に関連付けられたアカウントを認証する。ブロック 5 1 2 において、ルーチン 5 0 0 は、アカウントアプリケーション 1 4 0 によって、認証に基づいて、非接触カード 1 0 4 に関連付けられた支払い情報を受信する。ブロック 5 1 4 において、ルーチン 5 0 0 は、アカウントアプリケーション 1 4 0 によって、計算装置 1 0 2 において実行されるアプリケーションにのみアクセス可能であるローカルサーバ 2 1 0 を開始する。

40

【0080】

ブロック 5 1 6 において、ルーチン 5 0 0 は、ローカルサーバ 2 1 0 及びウェブブラウザ 1 4 2 の間における接続を確立する。ブロック 5 1 8 において、ルーチン 5 0 0 は、ウェブブラウザ 1 4 2 によって、ローカルサーバ 2 1 0 から支払い情報を受信する。ブロック 5 2 0 において、ルーチン 5 0 0 は、ウェブブラウザ 1 4 2 によって、ローカルサーバ

50

210に対して終了コマンドを発行することで、ローカルサーバとの接続を終了する。ブロック522において、ルーチン500は、ウェブブラウザ142によって、支払い情報を支払いフィールドへ自動記入する。複数のフィールドが存在する場合、ウェブブラウザ142は、情報を適切なフィールドへ自動記入してもよい。ブロック524において、ルーチン500は、ウェブブラウザ142によって、ウェブページの支払いフィールドへ自動記入された支払い情報に基づいて、トランザクションを処理する。

【0081】

図6Aは、非接触カード104の例示的な構成を示す概略図600であり、それは、非接触カード104の前面又は後面上にサービスプロバイダのマーク602として表示されるようなサービスプロバイダによって発行された、クレジットカードのような支払いカード、デビットカード、又はギフトカードを含んでもよい。いくつかの実施例では、非接触カード104は、支払いカードに関連せず、限定することなく、識別カードを含んでもよい。いくつかの実施例では、トランザクションカードは、デュアルインターフェースの非接触支払いカード、ポイントカード(rewards card)、などを含んでもよい。非接触カード104は基板604を含んでもよく、それは、プラスチック、金属、及び他の材料からなる単一の層又は1つ又は複数の積層された層を含んでもよい。例示的な基板材料は、ポリ塩化ビニル、ポリ塩化酢酸ビニル、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、陽極処理されたチタン、パラジウム、金、炭素、紙、及び生物分解性材料を含む。いくつかの実施例では、非接触カード104は、ISO/IEC 7816標準のID-1フォーマットに準拠した物理的特性を有してもよく、さもないと、トランザクションカードは、ISO/IEC 14443標準に準拠してもよい。しかしながら、本開示に係る非接触カード104が異なる特性を有してもよく、トランザクションカードが支払いカードとして実装されることを本開示が必要としないということが理解される。

【0082】

非接触カード104は、カードの前面及び／又は背面に表示された識別情報606と、接触パッド608とを含んでもよい。接点パッド608は、1つ又は複数のパッドを含んでもよく、トランザクションカードを介して、ATM、ユーザ装置、スマートフォン、ラップトップ、デスクトップ、又はタブレット型コンピュータのような他のクライアント装置との接触を確立するように構成されてもよい。接点パッドは、ISO/IEC 7816標準のような1つ又は複数の標準によれば設計されてもよく、EMVプロトコルによる通信を可能にしてもよい。非接触カード104は、図6Bにおいてさらに説明する処理回路、アンテナ、及び他の構成要素を含んでもよい。これらの構成要素は、接点パッド608の背後に、又は、基板604上の他の場所に、例えば、基板604の異なる層内に設けられてもよく、接点パッド608に電気的かつ物理的に接続されてもよい。非接触カード104は、磁気ストリップ又はテープを含んでもよく、それは、カードの背面(図6Aには図示せず)に設けられてもよい。非接触カード104はまた、NFCプロトコルを介して通信可能である、アンテナに接続された近距離無線通信(NFC)装置を含んでもよい。実施形態はこのように限定されない。

【0083】

図6Bに示すように、非接触カード104の接点パッド608は、プロセッサ612、メモリ110、及び1つ又は複数の通信インターフェース126を含む、情報を格納、処理、及び伝達するための処理回路610を含んでもよい。処理回路610は、本願において説明した機能を実行するのに必要とされる、プロセッサ、メモリ、エラー及びパリティ/CRCチェッカー、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、追加の構成要素を含んでもよいことが理解される。

【0084】

メモリ110は、読み出し専用メモリ、1回書き込み多数読み出しメモリ、又は読み出し／書き込みメモリ、例えば、RAM、ROM、及びEEPROMであってもよく、非接

10

20

30

40

50

触カード104は、これらのメモリのうちの1つ又は複数を含んでもよい。読み出し専用メモリは、読み出し専用又は1回だけプログラミング可能であるように工場でプログラミング可能である。1回だけのプログラミング可能性は、1回だけ書き込まれ、その後、複数回にわたって読み出される機会を提供する。1回書き込み／多数読み出しメモリは、メモリチップが工場を去った後の時点でプログラミングされてもよい。いったんメモリがプログラミングされると、それは再書き込みされることはないが、複数回にわたって読み出される。読み出し／書き込みメモリは、工場を去った後に複数回にわたってプログラミング及び再プログラミングされてもよい。読み出し／書き込みメモリはまた、工場を去った後に複数回にわたって読み出されてもよい。いくつかの例では、メモリ110は、データを暗号化するためにプロセッサ612によって実行される暗号アルゴリズムを利用する、暗号化されたメモリであってもよい。

10

【0085】

メモリ110は、1つ又は複数のアプレット112、1つ又は複数のカウンタ114、顧客ID120、1つ又は複数のマスタ鍵116、及び1つ又は複数の多様化鍵118を格納するように構成されてもよい。1つ又は複数のアプレット112は、Java（登録商標）カードアプレットのように、1つ又は複数の非接触カード104において実行されるように構成された1つ又は複数のソフトウェアアプリケーションを含んでもよい。しかしながら、アプレット112は、Javaカードアプレットに限定されず、代わりに、非接触カード又は限られたメモリを有する他の装置において動作可能である任意のソフトウェアアプリケーションであってもよいことが理解される。1つ又は複数のカウンタ114は、整数を格納するのに十分な数値カウンタを備えてもよい。顧客ID120は、非接触カード104のユーザに割り当てられた一意の英数字識別子を含んでもよく、識別子は、当該非接触カード104のユーザを他の非接触カード104のユーザから区別してもよい。いくつかの実施例では、顧客ID120は、顧客と、その顧客に割り当てられたアカウントと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カード104を識別してもよい。

20

【0086】

先述した例示的な実施形態のプロセッサ612及びメモリ構成要素は、接触パッド608を参照して説明しているが、本開示はそれに限定されない。これらの構成要素は、接触パッド608の外部又はそれから完全に離れて実装されてもよく、又は、接触パッド608内に設けられたプロセッサ612及びメモリ110構成要素に加えてさらなる構成要素として実装されてもよい。

30

【0087】

いくつかの実施例では、非接触カード104は、1つ又は複数のアンテナ614を備えてもよい。1つ又は複数のアンテナ614は、非接触カード104内において、接触パッド608の処理回路610のまわりに配置されてもよい。例えば、1つ又は複数のアンテナ614は処理回路610に一体化されていてもよく、1つ又は複数のアンテナ614は外部ブースタコイルとともに使用されてもよい。他の実施例として、1つ又は複数のアンテナ614は、接触パッド608及び処理回路610の外部にあってもよい。

【0088】

一実施形態において、非接触カード104のコイルは、空芯トランスの2次巻線として作用してもよい。端末は、電力の遮断又は振幅変調によって非接触カード104と通信してもよい。非接触カード104は、非接触カード104の電力接続におけるギャップを用いて、端末から送信されたデータを推測してもよい。電力接続は、1つ又は複数のキャパシタを介して機能的に保持されてもよい。非接触カード104は、非接触カード104のコイルにおいて負荷をスイッチングすること又は負荷変調によって逆方向に通信してもよい。負荷変調は、干渉を通じて端末のコイルにおいて検出されてもよい。より一般的には、1つ又は複数のアンテナ614、処理回路612、及び／又はメモリ110を用いて、非接触カード104は、NFC、Bluetooth、及び／又はWi-Fi通信を介して通信するための通信インターフェースを提供する。

40

50

【0089】

上で説明したように、非接触カード104は、JavaCardのような、限られたメモリを有する他のスマートカード又は装置において動作可能であるソフトウェアプラットフォームにおいて構成されてもよく、1つ又は複数のアプリケーション又はアプレットが安全に実行されてもよい。移動体アプリケーションに基づく様々な使用状況における多要素認証(multifactor authentication:MFA)のためにワンタイムパスワード(one-time password:OTP)を提供するために、非接触カードにアプレット112が追加されてもよい。アプレット112は、(例えば、POS(point-of-sale)端末のモバイル装置の)移動体NFCリーダーのようなリーダーから、近接場データ交換要求のような1つ又は複数の要求に応答し、NDEFテキストタグとして符号化された暗号学的に安全なOTPを備えるNDEFメッセージを生成するように構成されてもよい。NDEFメッセージは、暗号文122及び他の任意のデータを含んでもよい。

10

【0090】

NDEF OTPの一例は、NDEFショートレコードレイアウト(SR=1)である。そのような実施例では、1つ又は複数のアプレット112は、OTPを、NDEFタイプ4の公知のタイプのテキストタグとして符号化するように構成されてもよい。いくつかの実施例では、NDEFメッセージは、1つ又は複数のレコードを含んでもよい。アプレット112は、OTP記録に加えて、1つ又は複数の静的タグ記録を追加するように構成されてもよい。

20

【0091】

いくつかの実施例では、1つ又は複数のアプレット112は、RFIDタグをエミュレートするように構成されてもよい。RFIDタグは、1つ又は複数の多様な形態のタグを含んでもよい。いくつかの実施例では、タグが読み取られるごとに、非接触カードの真正性を示しうる異なる暗号データが提示される。1つ又は複数のアプレット112に基づいて、タグのNFC読み取りが処理されてもよく、データは、バンキングシステムサーバのようなサーバに送信されてもよく、データはサーバにおいて検証されてもよい。

【0092】

いくつかの実施例では、非接触カード104及びサーバは、カードが適切に識別されるように、所定のデータを含んでもよい。非接触カード104は、1つ又は複数の一意の識別子(図示せず)を含んでもよい。読み取り動作が行なわれるごとに、カウンタ114はインクリメントするように構成されてもよい。いくつかの実施例では、(例えばモバイル装置によって)非接触カード104からデータが読み取られるごとに、カウンタ114は、検証のためにサーバに送信され、カウンタ114がサーバのカウンタに等しいか否かを(検証の一部として)決定する。

30

【0093】

1つ又は複数のカウンタ114は、リプレイ攻撃を防ぐように構成されてもよい。例えば、暗号文が取得されかつ繰り返された場合、その暗号文は、カウンタ114が読み取られるか使用されるかさもなければ無視される場合に直ちに拒絶される。カウンタ114が使用されていない場合、それは繰り返されてもよい。いくつかの実施例では、非接触カード104においてインクリメントされるカウンタは、トランザクションに関してインクリメントされるカウンタとは異なる。非接触カード104においてアプレット112間の通信が存在しないので、非接触カード104は、アプリケーショントランザクションカウンタ114を決定することができない。いくつかの実施例では、非接触カード104は、第1のアプレット440-1及び第2のアプレット440-2を備えてもよく、第1のアプレット440-1はトランザクションアプレットであってもよい。各アプレット440-1及び440-2は、各カウンタ114を備えてもよい。

40

【0094】

いくつかの実施例では、カウンタ114は同期からはずれることがある。いくつかの実施例では、所定角度での読み取りのような、トランザクションを開始する偶発的な読み取りを説明するために、カウンタ114はインクリメントしてもよいが、アプリケーション

50

はカウンタ 1 1 4 を処理しない。いくつかの実施例では、モバイル装置 1 0 がスリープから復帰するとき、N F C がイネーブルにされてもよく、計算装置 1 0 2 は利用可能なタグを読み取るように構成されてもよいが、読み取りに応答して何の動作も行われない。

【0095】

カウンタ 1 1 4 の同期を維持するために、計算装置 1 0 2 がスリープからいつ復帰したかを検出し、バンキングシステムのサーバに同期するように構成されるであろう、バックグラウンドアプリケーションのようなアプリケーションが実行されてもよく、このことは、検出に起因して行われた読み取りが次いでカウンタ 1 1 4 を順方向に進めることを示す。他の実施例では、同期からはずれたウィンドウが受容されうるように、ハッシュされたワンタイムパスワードが利用されてもよい。例えば、1 0 のしきい値の範囲内にある場合、カウンタ 1 1 4 は、順方向に進むように構成されてもよい。しかし、異なるしきい値数の範囲内、例えば、1 0 又は 1 0 0 0 の範囲内にある場合、再同期を実行する要求が処理されてもよい。それは、ユーザがユーザの装置を介して 1 回以上にわたってタップ、ジェスチャー、又はさもなければ示すことを、1 つ又は複数のアプリケーションを介して要求する。カウンタ 1 1 4 は適切なシーケンスで増大し、次いで、それは、ユーザがそうしたことを知ることができる。

【0096】

カウンタ 1 1 4、マスタ鍵、及び多様化鍵を参照して本願で説明する鍵多様化技術は、鍵多様化技術の暗号化及び／又は復号の一例である。この例示的な鍵多様化技術は、本開示が他のタイプの鍵多様化技術にも同様に適用可能であるので、本開示を限定するものと考えられるべきではない。

【0097】

非接触カード 1 0 4 の生成処理中に、カードごとに、2 つの暗号鍵が一意的に割り当てられてもよい。暗号鍵は、データの暗号化及び復号の両方に使用されうる対称鍵を含んでもよい。トリプル D E S (3 D E S) アルゴリズムが E M V によって使用されてもよく、それは非接触カード 1 0 4 におけるハードウェアによって実装される。鍵多様化処理を用いることによって、鍵を必要とする各エンティティに係る一意的に識別可能な情報に基づいて、マスタ鍵から 1 つ又は複数の鍵が導出されてもよい。

【0098】

いくつかの実施例では、脆弱性の影響を受けやすいかもしれないという 3 D E S アルゴリズムの不備を克服するために、(セッションごとの一意の鍵のような)セッション鍵が導出されてもよいが、マスタ鍵を用いるのではなく、カードにより導出された一意の鍵及びカウンタが多様化データとして使用されてもよい。例えば、動作中に非接触カード 1 0 4 が使用されるごとに、メッセージ認証コード (M A C) の生成及び暗号化の実行のために異なる鍵が使用されてもよい。これにより、三層の暗号をもたらす。セッション鍵は、1 つ又は複数のアプレットによって生成され、(「EMV 4.3 Book 2 A1.3.1 Common Session Key Derivation」で定義されたような) 1 つ又は複数のアルゴリズムを備えたアプリケーショントランザクションカウンタを用いて導出されてもよい。

【0099】

さらに、各カードに係るインクリメントは一意的であってもよく、個人化によって割り当てられてもよく、あるいは、何らかの識別情報によってアルゴリズム的に割り当てられてもよい。例えば、奇数の番号を有するカードは 2 ずつインクリメントされてもよく、偶数の番号を有するカードは 5 ずつインクリメントされてもよい。いくつかの実施例では、1 つのカードが 1、3、5、2、2、…を繰り返す順序でインクリメントされてもよいように、インクリメントは逐次的な読み取りにおいて変化してもよい。特定のシーケンス又はアルゴリズムのシーケンスは、個人化の時点で、又は、一意の識別子から導出される 1 つ又は複数の処理から定義されてもよい。これにより、リプレイ攻撃者がカードインスタンスの小さな番号から一般化することをより困難にすることができる。

【0100】

認証メッセージは、1 6 進 A S C I I フォーマットを有するテキスト N D E F レコード

の内容として送られてもよい。もう1つの実施例では、NDEFレコードは、16進フォーマットで符号化されてもよい。

【0101】

図7は、例示的な実施形態に係るNDEFショートレコードレイアウト（SR=1）データ構造700を示す。1つ又は複数のアプレットは、OTPを、NDEFタイプ4の公知のタイプのテキストタグとして符号化するように構成されてもよい。いくつかの実施例では、NDEFメッセージは、1つ又は複数のレコードを含んでもよい。アプレットは、OTPレコードに加えて、1つ又は複数の静的タグレコードを追加するように構成されてもよい。例示的なタグは、限定することなく、下記を含む。タグタイプ：公知のタイプ、テキスト、エンコーディング英語（en）；アプレットID：D2760000850101；能力：読み出し専用アクセス；エンコーディング：認証メッセージはASCIIの16進数として符号化されうる；タイプ・長さ・値（type-length-value：TLV）データは、NDEFメッセージを生成するために使用されうる個人化パラメータとして提供されうる。一実施形態において、認証テンプレートは、実際の動的認証データを提供するための公知のインデックスを有する、第1のレコードを備えてもよい。データ構造700は、暗号文122と、アプレット112によって提供される他の任意のデータを含んでもよい。

10

【0102】

図8は、前述したように様々な実施形態を実装するために適した例示的なコンピュータアーキテクチャ800の実施形態を示す。一実施形態では、コンピュータアーキテクチャ800は、計算アーキテクチャ100の一部を含むか、又は、計算アーキテクチャ100の一部として実装されてもよい。

20

【0103】

本願において使用されるように、用語「システム」及び「構成要素」は、コンピュータ関連のエンティティ、ハードウェア、ハードウェア及びソフトウェアの組み合わせ、ソフトウェア、又は実行中のソフトウェアのいずれかを示すことが意図され、それらの例は例示的な計算コンピュータアーキテクチャ800によって提供される。例えば、構成要素は、プロセッサにおいて動作する処理、プロセッサ、ハードディスクドライブ、（光学及び／又は磁気記憶媒体の）複数の記憶ドライブ、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、及び／又はコンピュータであってもよいが、それらに限定されない。例示として、サーバにおいて動作するアプリケーションと、サーバとの両方が、構成要素になりうる。1つ又は複数の構成要素が1つの処理／実行スレッド内に存在してもよく、1つの構成要素が、1つのコンピュータにおいて局在してもよく、及び／又は、2つ以上のコンピュータ間で分散されてもよい。さらに、複数の構成要素は、動作を協調させるために、様々なタイプの通信媒体によって互いに通信可能に接続されてもよい。協調動作は、情報の単方向又は双方向交換を伴ってもよい。例えば、構成要素は、通信媒体上で伝送される信号の形式で情報を伝送してもよい。情報は、様々な信号ラインに割り当てられた信号として実装されてもよい。そのような割り当てにおいて、各メッセージが信号である。しかしながら、別の実施形態は、代替としてデータメッセージを使用してもよい。そのようなデータメッセージは、様々な接続を介して送信されてもよい。例示的な接続は、

30

40

【0104】

コンピュータアーキテクチャ800は、1つ又は複数のプロセッサ、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、周辺装置、インターフェース、発振器、タイミング装置、ビデオカード、オーディオカード、マルチメディア入力／出力（I/O）構成要素、電源などのような、様々な一般的な計算要素を含む。しかしながら、実施形態は、計算アーキテクチャ800による実装に限定されない。

【0105】

図8に示すように、コンピュータアーキテクチャ800は、プロセッサ802、システ

50

ムメモリ 804、及びシステムバス 806 を備えるコンピュータ 812 を含む。プロセッサ 802 は、様々な市販のプロセッサのいずれかであってもよい。コンピュータ 812 は、計算装置 102 及び／又は認証サーバ 106 を表しうる。

【0106】

システムバス 806 は、システムメモリ 804 からプロセッサ 802 を含むがそれに限定されない、システム構成要素のためのインターフェースを提供する。システムバス 806 は、さまざまな市販のバスアーキテクチャのうちのいずれかを用いて、メモリバス（メモリコントローラとともに又はメモリコントローラとは別に）、周辺機器バス、及びローカルバスにさらに相互接続しうる、いくつかのタイプのバス構造のいずれかであってもよい。インター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 806 に接続されてもよい。例示的なスロットアーキテクチャは、AGP (Accelerated Graphics Port)、カードバス、(E)ISA ((Extended) Industry Standard Architecture)、MCA (Micro Channel Architecture)、NuBus、PCI (X) (Peripheral Component Interconnect (Extended))、PCI Express、PCMCIA (Personal Computer Memory Card International Association) などを含んでもよいがそれらに限定されない。

【0107】

コンピュータアーキテクチャ 800 は、様々な製品を含むか又は実装してもよい。製品は、論理を格納するためのコンピュータ可読記憶媒体を含んでもよい。コンピュータ可読記憶媒体の例は、揮発性メモリ又は不揮発性メモリ、リムーバブル又は非リムーバブルメモリ、消去可能又は消去不可能メモリ、書き込み可能又は再書き込み可能なメモリ、などを含む、電子データを格納できる任意の有形物媒体を含んでもよい。論理の例は、ソースコード、コンパイルされたコード、インタプリタで処理されたコード、実行可能なコード、静的コード、動的コード、オブジェクト指向コード、視覚的コード、などのような任意の適切なタイプのコードを用いて実装された、実行可能なコンピュータプログラム命令を含んでもよい。実施形態はまた、少なくとも部分的に、非一時的なコンピュータ可読媒体内又はそのような媒体上に含まれる命令として実装されてもよく、それは、1つ又は複数のプロセッサによって読み出されて実行されることで、本願で説明する動作の実行を可能にしてもよい。

【0108】

システムメモリ 804 は、ROM (read-only memory)、RAM (random-access memory)、DRAM (dynamic RAM)、DDRAM (Double-Data-Rate DRAM)、SDRAM (synchronous DRAM)、SRAM (static RAM)、PROM (programmable ROM)、EPROM (erasable programmable ROM)、EEPROM (electrically erasable programmable ROM)、フラッシュメモリ（例えば、1つ又は複数のフラッシュアレイ）、強誘電体ポリマーメモリのようなポリマーメモリ、オボニック (ovonic) メモリ、相変化又は強誘電体メモリ、SONOS (silicon-oxide-nitride-oxide-silicon) メモリ、磁気又は光カード、RAID (array of devices such as Redundant Array of Independent Disks) ドライブ、ソリッドステートメモリ装置（例えば、USBメモリ、SSD (solid state drive)）、及び情報を格納するのに適した他の任意のタイプの記憶媒体のような、1つ又は複数のより高速のメモリユニットの形式を有する様々なタイプのコンピュータ可読記憶媒体を含んでもよい。図 8 に示す実施形態では、システムメモリ 804 は、不揮発性 808 及び／又は揮発性 810 を含んでもよい。BIOS (basic input/output system) は、不揮発性メモリ 808 に格納されてもよい。

【0109】

コンピュータ 812 は、内部（又は外部）ハードディスクドライブ 814 と、着脱可能な磁気ディスク 818 に対して読み出す又は書き込むための磁気ディスクドライブ 816 と、着脱可能な光ディスク 822（例えば、CD-ROM 又は DVD）に対して読み出す又は書き込むための光ディスクドライブ 820 とを含む、1つ又は複数のより低速のメモ

リユニットの形式を有する様々なタイプのコンピュータ可読記憶媒体を含んでもよい。ハードディスクドライブ 814、磁気ディスクドライブ 816、及び光ディスクドライブ 820 は、HDD インターフェース 824、FDD インターフェース 826、及び光ディスクドライブ インターフェース 828 によって、システムバス 806 にそれぞれ接続されてもよい。外部ドライブ実装のための HDD インターフェース 824 は、USB (Universal Serial Bus) 及び IEEE 1394 インターフェース技術の少なくとも一方又は両方を含んでもよい。

【0110】

ドライブ及び関連付けられた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な命令などの揮発性及び／又は不揮発性の記憶装置を提供する。例えば、オペレーティングシステム 830、1つ又は複数のアプリケーション 832、他のプログラムモジュール 834、及びプログラムデータ 836 を含む多数のプログラムモジュールが、ドライブ、不揮発性 808、及び揮発性 810 に格納されてもよい。一実施形態では、1つ又は複数のアプリケーション 832、他のプログラムモジュール 834、及びプログラムデータ 836 は、例えば、システム 100 の様々なアプリケーション及び／又は構成要素を含んでもよい。

10

【0111】

ユーザは、1つ又は複数の有線／無線入力装置、例えば、キーボード 838 と、マウス 840 のようなポインティングデバイスとを介して、コマンド及び情報をコンピュータ 812 に入力してもよい。他の入力装置は、マイクロホン、赤外線 (IR) リモートコントロール、無線周波数 (RF) リモートコントロール、ゲームパッド、スタイラスペン、カードリーダー、 dongle、指紋リーダー、グローブ、グラフィックスタブレット、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 (例えば、容量性、抵抗性など)、トラックボール、トラックパッド、センサ、スタイラスなどを含んでもよい。これら及び他の入力装置は、多くの場合、システムバス 806 に接続される入力装置インターフェース 842 を介してプロセッサ 802 に接続されるが、パラレルポート、IEEE 1394 シリアルポート、ゲームポート、USB ポート、IR インターフェースなどのような他のインターフェースによって接続されてもよい。

20

【0112】

モニター 844 又は他のタイプのディスプレイ装置もまた、ビデオアダプタ 846 のようなインターフェースを介してシステムバス 806 に接続される。モニター 844 は、コンピュータ 812 の内部又は外部にあってもよい。モニター 844 に加えて、コンピュータは、典型的には、スピーカ、プリンタなどのような、他の周辺出力装置を含む。

30

【0113】

コンピュータ 812 は、1つ又は複数の遠隔のコンピュータ 848 のような 1つ又は複数の遠隔のコンピュータへの有線及び／又は無線通信を介して、論理接続を用いて、ネットワーク化された環境において動作してもよい。1つ又は複数の遠隔のコンピュータ 848 は、ワークステーション、サーバコンピュータ、ルータ、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に基づくエンターテインメント機器、ピア装置、又は他の一般的なネットワークノードであってもよく、簡潔さの目的でメモリ／記憶装置 850 のみを図示しているが、典型的には、コンピュータ 812 に関連して説明した構成要素のうちの多数又はすべてを含む。図示した論理接続は、LAN (local area network) 852 及び／又はより大きなネットワーク、例えば WAN (wide area network) 854 への有線／無線接続を含む。そのような LAN 及び WAN ネットワーキング環境は、オフィス及び会社において一般的に存在し、イントラネットのような企業全体にわたるコンピュータネットワークを促進し、それらのすべては、大域的な通信ネットワーク、例えばインターネットに接続されてもよい。

40

【0114】

ローカルエリアネットワーク 852 ネットワーキング環境において使用される場合、コンピュータ 812 は、有線及び／又は無線通信ネットワークインターフェース又はネット

50

ワークアダプタ 856 を介して、ローカルエリアネットワーク 852 に接続される。ネットワークアダプタ 856 は、ローカルエリアネットワーク 852 への有線及び／又は無線通信を容易にすることができ、それは、ネットワークアダプタ 856 の無線機能と通信するために、その上に配置された無線アクセスポイントを含んでもよい。

【0115】

ワイドエリアネットワーク 854 ネットワーキング環境において使用される場合、コンピュータ 812 は、モデム 858 を含んでもよく、又は、ワイドエリアネットワーク 854 における通信サーバに接続されるか、例えばインターネットによって、ワイドエリアネットワーク 854 を介する通信を確立するための他の手段を有する。モデム 858 は、入力装置インターフェース 842 を介してシステムバス 806 に接続される。モデム 858 は、内部又は外部にあってもよく、かつ、有線及び／又は無線装置であってもよい。ネットワーク化された環境において、コンピュータ 812 に関連して図示したプログラムモジュール又はその部分は、遠隔のメモリ／記憶装置 850 に格納されてもよい。図示したネットワーク接続は例示的であり、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可能であることが認識されるであろう。

【0116】

コンピュータ 812 は、無線通信（例えば、IEEE 802.11 の無線変調技術）において動作可能に配置された無線装置のような、IEEE 802 標準のファミリーを用いる有線及び無線装置又はエンティティと通信するように動作可能である。これは、少なくとも、とりわけ、Wi-Fi (Wireless Fidelity)、WiMax、及び Bluetooth 無線技術を含む。従って、通信は、従来技術のネットワークを含むような予め定義された構造であってもよく、又は、単に、少なくとも 2 つの装置間のアドホックな通信であってもよい。Wi-Fi ネットワークは、安全で、信頼性が高く、高速な無線接続を提供するために、IEEE 802.11 (a、b、g、n、ac、ax、など) と呼ばれる無線技術を用いる。Wi-Fi ネットワークは、複数のコンピュータを互いに接続するために、インターネットに接続するために、また、有線ネットワーク (IEEE 802.3 に関連する媒体及び機能を用いる) に接続するために使用可能である。

【0117】

図 1～図 7 を参照して前述したような装置の様々な構成要素は、様々なハードウェア構成要素、ソフトウェア構成要素、又は両者の組み合わせを含んでもよい。ハードウェア構成要素の例は、装置、論理装置、構成要素、プロセッサ、マイクロプロセッサ、回路、回路素子（例えば、トランジスタ、抵抗、キャパシタ、インダクタなど）、集積回路、特定用途向け集積回路 (application specific integrated circuits : ASIC)、プログラマブル論理デバイス (programmable logic device : PLD)、デジタル信号プロセッサ (digital signal processor : DSP)、フィールドプログラマブルゲートアレイ (field programmable gate array : FPGA)、メモリ装置、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、チップセットなどを含んでもよい。ソフトウェア構成要素の例は、ソフトウェア部品、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、ソフトウェア開発プログラム、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、関数、メソッド、手順、ソフトウェアインターフェース、API (application program interface)、命令セット、計算コード、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、値、シンボル、又はそれらの任意の組み合わせを含んでもよい。しかしながら、実施形態がハードウェア構成要素及び／又はソフトウェア構成要素を用いて実装されるか否かを決定することは、所与の実装に関して望まれる、所望の計算レート、電力レベル、耐熱性、処理サイクル予算、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、及び他の設計上又は性能上の制約のような、任意個数のファクタに従って変化する。

【0118】

少なくとも1つの実施形態の1つ又は複数の態様は、マシンによって読み出されたとき、本願において説明した技術を実行するロジックをマシンに生成させるプロセッサ内の様々なロジックを表す機械可読媒体上に格納された典型的命令によって実装されてもよい。

「IPコア」として知られたそのような表現は、有形物の機械可読媒体に格納され、様々な顧客又は製造設備に供給されて、ロジック又はプロセッサを作る製造マシンへロードされてもよい。いくつかの実施形態は、例えば、マシンによって実行されたとき、実施形態に係る方法及び／又は動作をマシンに実行せしめる1つの命令又は一組の命令を格納する機械可読媒体又は製品を用いて実装されてもよい。そのようなマシンは、例えば、任意の適切な処理プラットフォーム、計算プラットフォーム、計算装置、処理装置、計算システム、処理システム、コンピュータ、プロセッサなどを含んでもよく、ハードウェア及び／又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てもよい。機械可読媒体又は製品は、例えば、任意の適切なタイプのメモリユニット、メモリ装置、メモリ製品、メモリ媒体、記憶装置、記憶製品、記憶媒体及び／又は記憶装置、例えば、メモリ、着脱可能又は着脱不可の媒体、消去可能又は消去不可の媒体、書き込み可能又は再書き込み可能な媒体、デジタル又はアナログ媒体、ハードディスク、フロッピーディスク、CD-ROM (Compact Disk Read Only Memory)、記録可能なコンパクトディスク (Compact Disk Recordable: CD-R)、再書き込み可能なコンパクトディスク (Compact Disk Rewriteable: CD-RW)、光ディスク、磁気媒体、光磁気媒体、着脱可能なメモリーカード又はディスク、様々なタイプのデジタル多用途ディスク (Digital Versatile Disk: DVD)、テープ、カセットなどを含んでもよい。命令は、任意の適切な高レベル、低レベル、オブジェクト指向、視覚的、コンパイルされた、及び／又はインタプリタ処理されたプログラミング言語を用いて実装された、ソースコード、コンパイルされたコード、インタプリタ処理されたコード、実行可能なコード、静的コード、動的コード、暗号化されたコードなどのような、任意の適切なタイプのコードを含んでもよい。

10

20

30

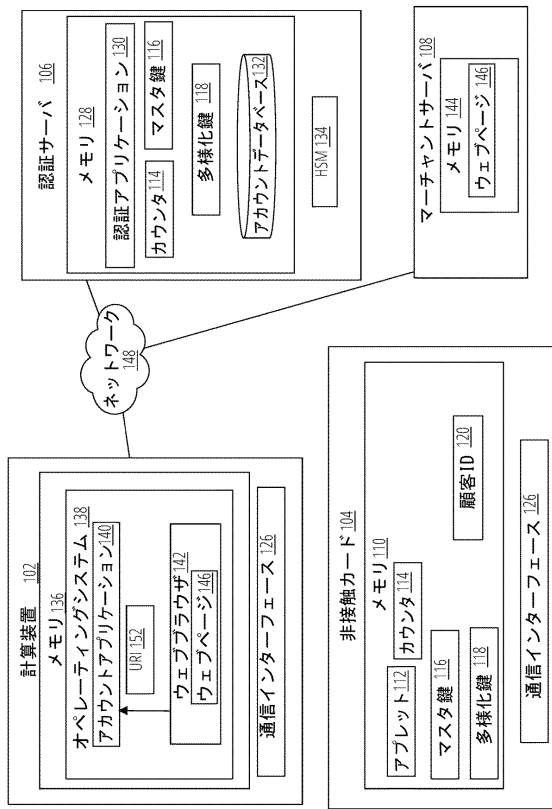
40

50

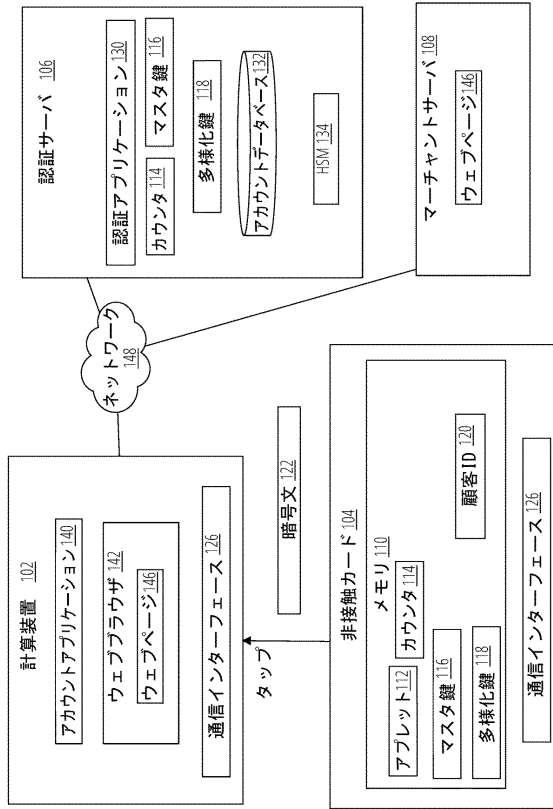
【0119】

例示的な実施形態に係る先の説明を、例示及び説明の目的で提示した。網羅的であることも、本開示を開示した形態そのものに限定することも意図していない。本開示に照らして多くの修正及び変形が可能である。本開示の範囲がこの詳細な説明によっては限定されず、むしろ、ここに添付した特許請求の範囲によって限定されることを意図している。本願への優先権を主張する将来の出願は、開示した主題の権利を異なる方法で主張する可能性があり、また、概して、本願においてさまざまに開示又はさもなければ例証されるような1つ又は複数の制限からなる任意の集合を含む可能性がある。

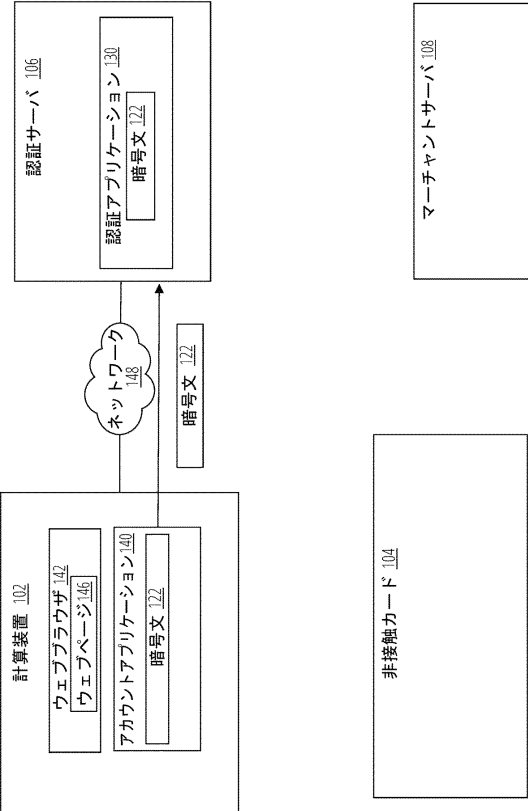
【図面】
【図 1 A】



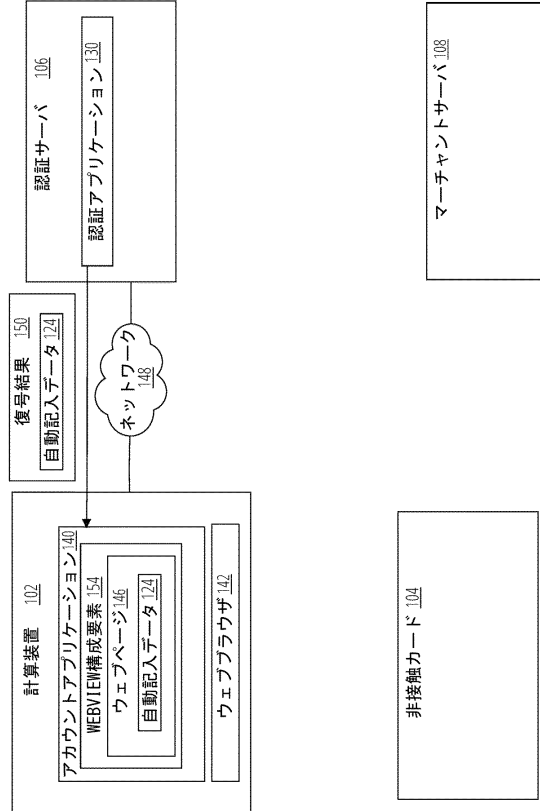
【図 1 B】



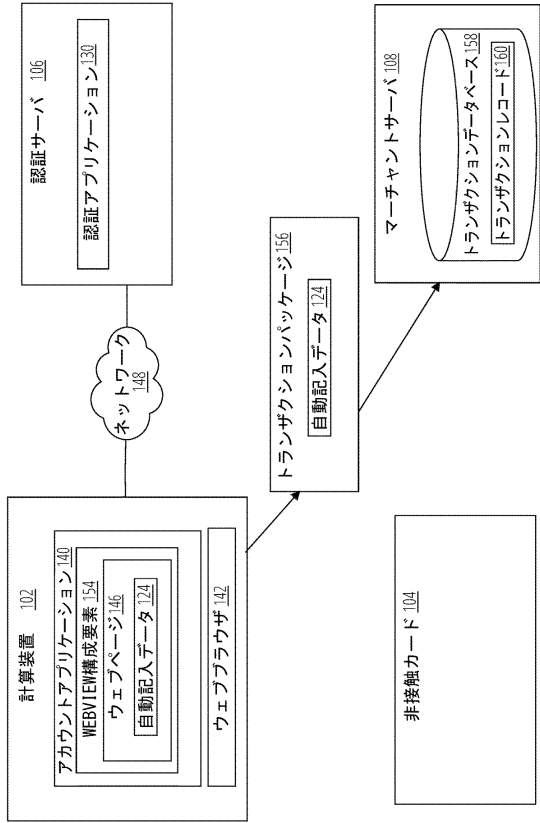
【図 1 C】



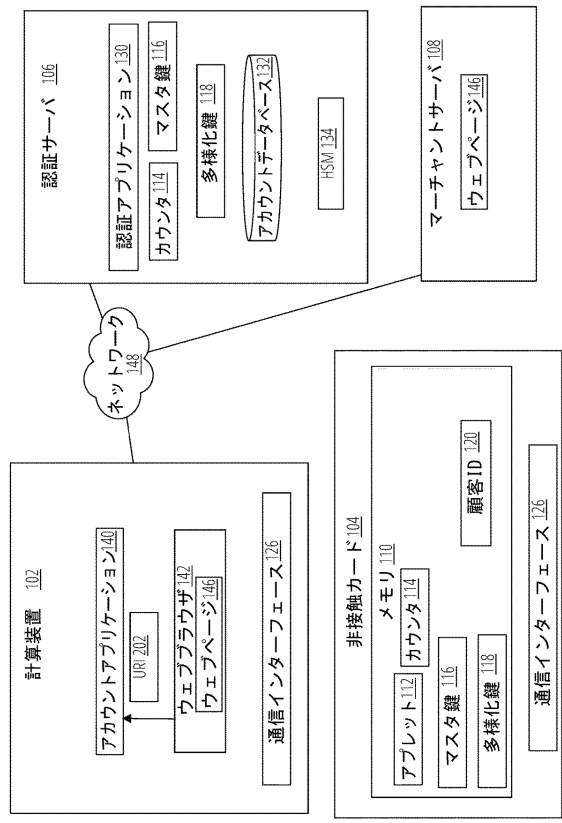
【図 1 D】



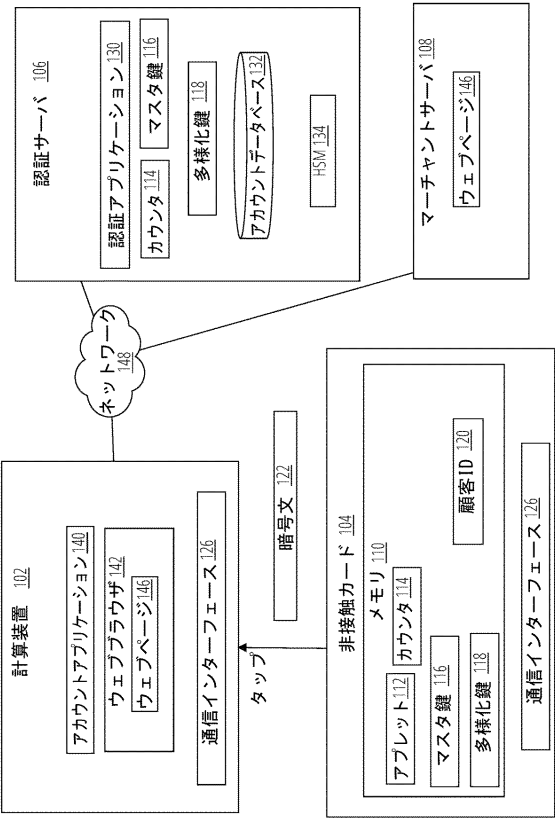
【図 1 E】



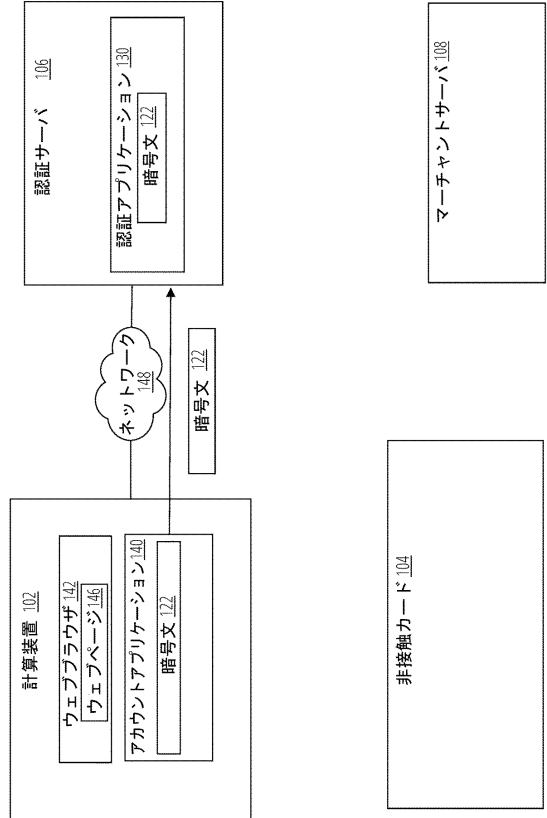
【図 2 A】



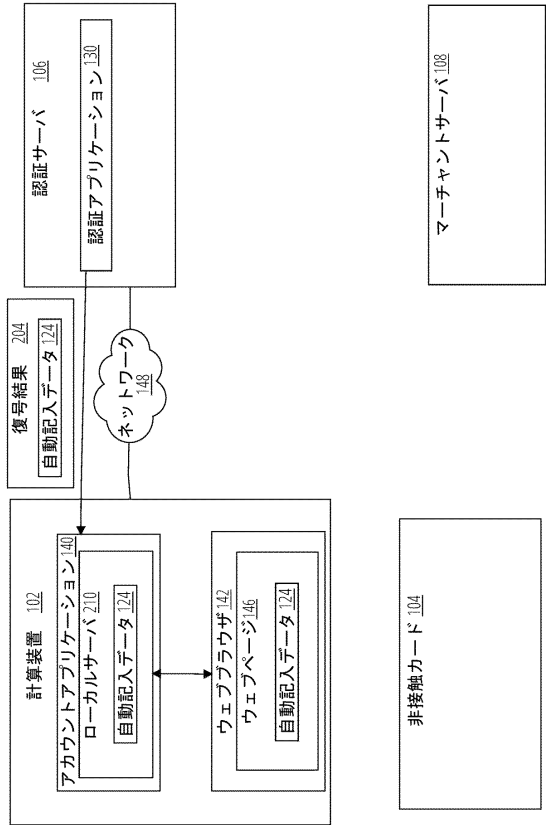
【図 2 B】



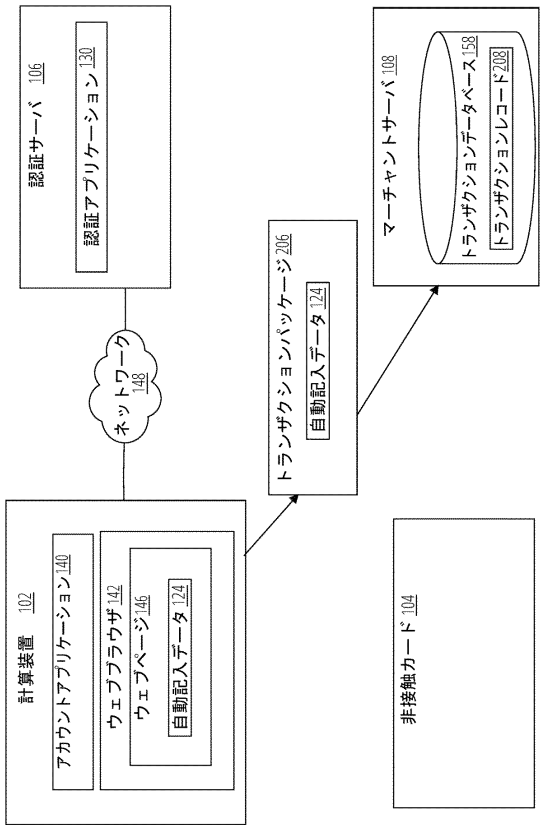
【図 2 C】



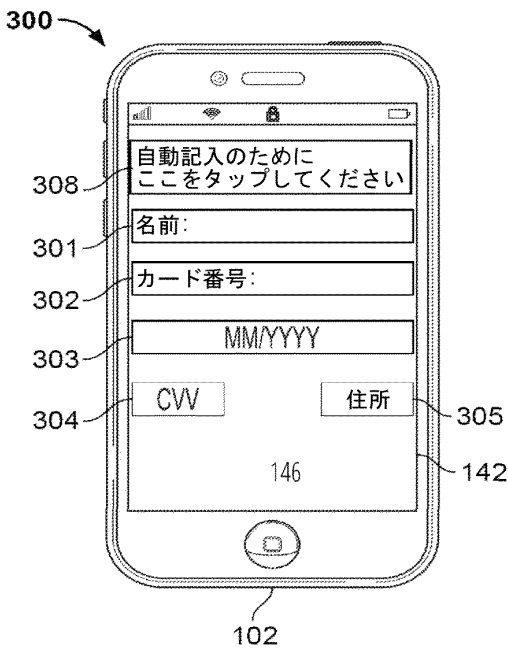
【図 2 D】



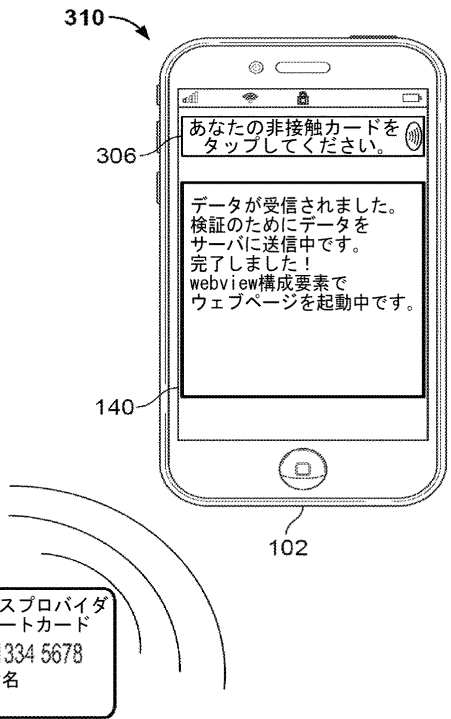
【図 2 E】



【図 3 A】



【図 3 B】



10

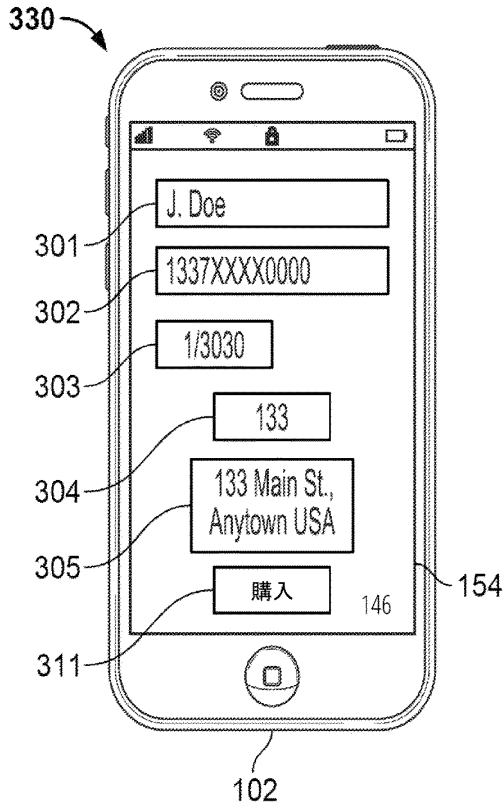
20

30

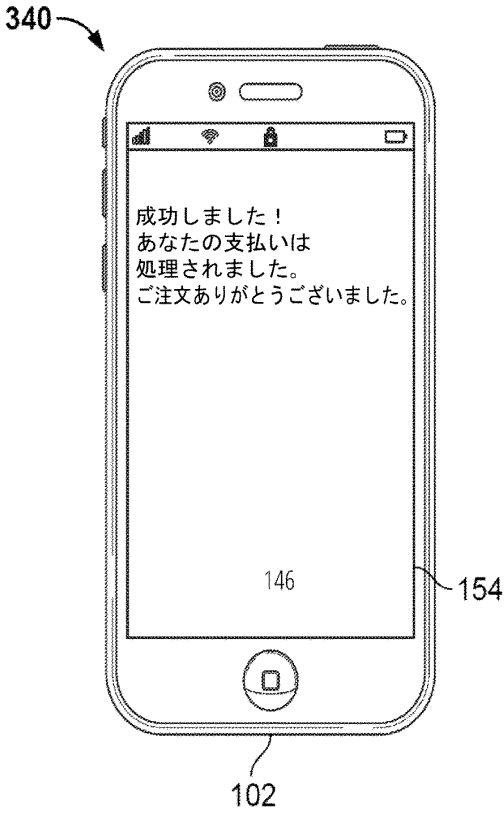
40

50

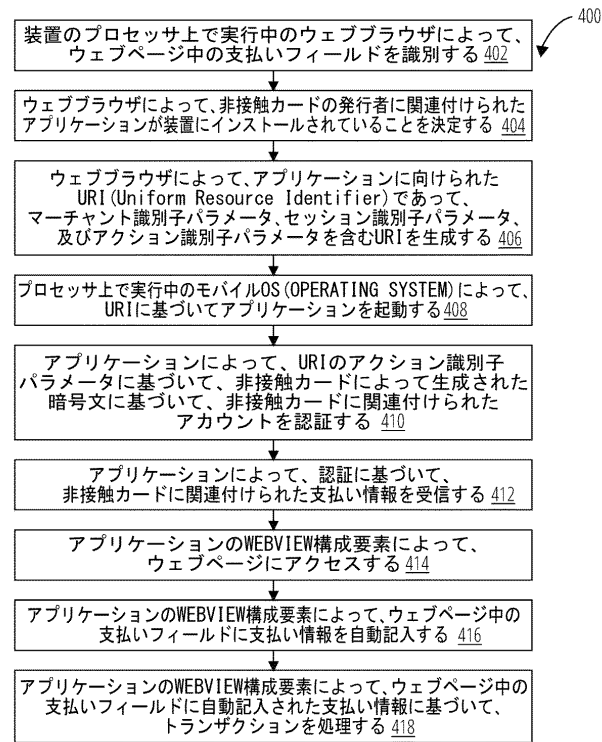
【図 3 C】



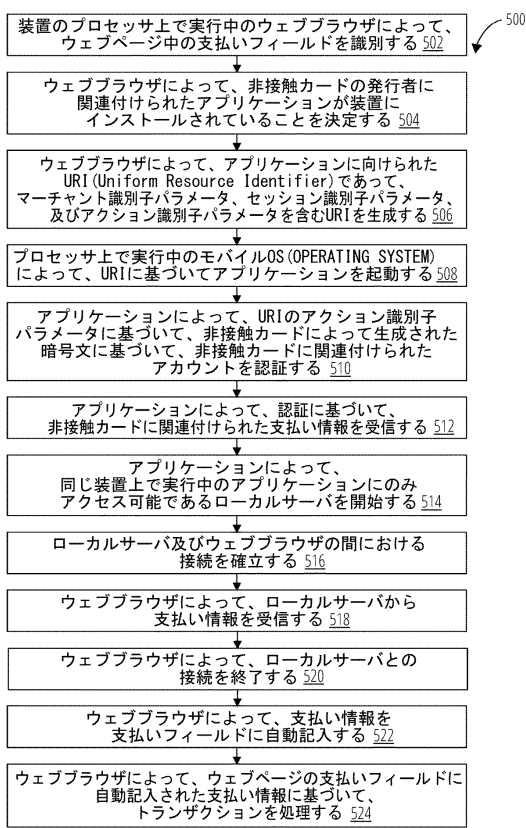
【図 3 D】



【図 4】



【図 5】



10

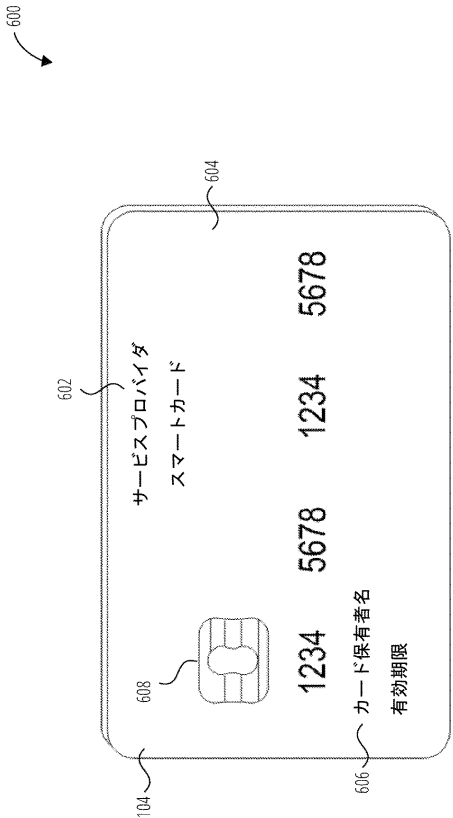
20

30

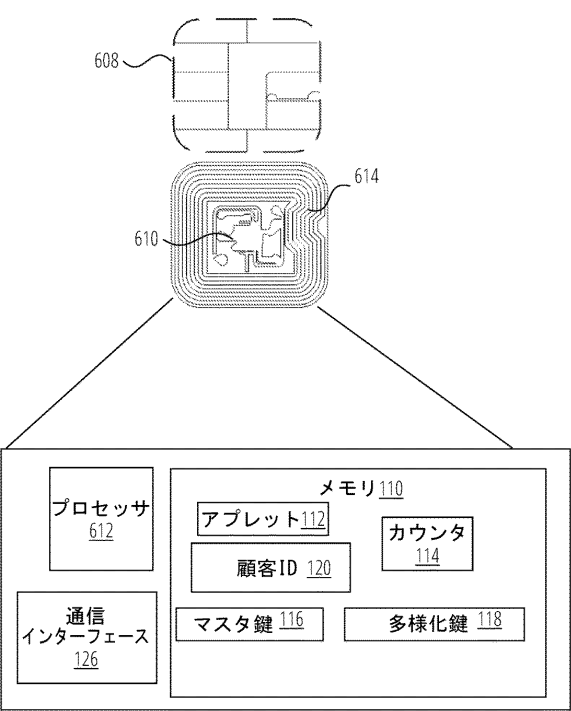
40

50

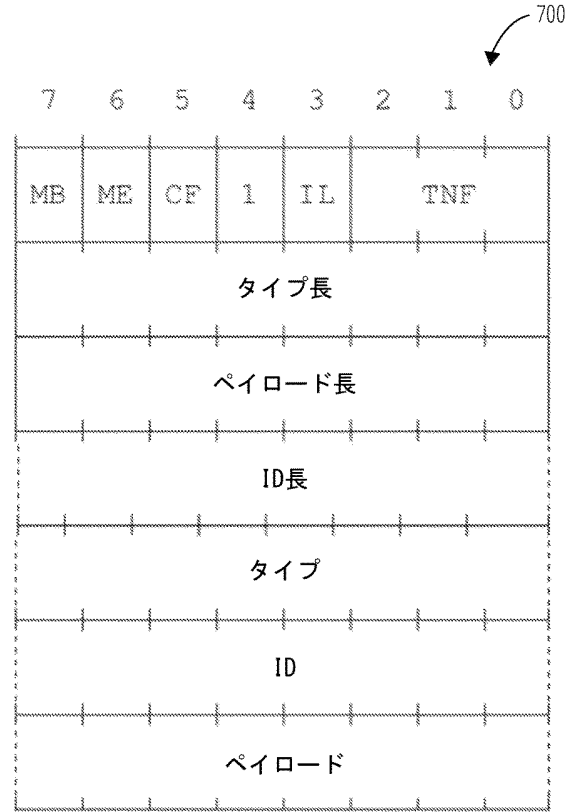
【図 6 A】



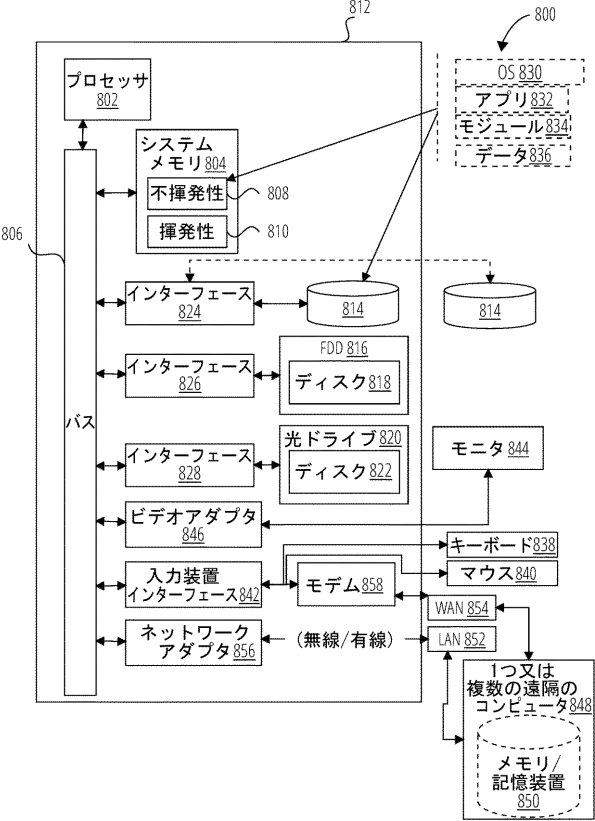
【図 6 B】



【図 7】



【図 8】



10

20

30

40

50

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/025285

A. CLASSIFICATION OF SUBJECT MATTER INV. G06Q20/32 G06Q20/34 G06Q20/40 ADD.		
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) G06F G06Q G07G		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2020/160065 A1 (CAPITAL ONE SERVICES LLC [US]) 6 August 2020 (2020-08-06) abstract; claims 1-16; figures 1A-7 paragraphs [0004], [0012] - [0069] -----	1-24
X	WO 2020/154600 A1 (CAPITAL ONE SERVICES LLC [US]) 30 July 2020 (2020-07-30) abstract; claims 1-20; figures 1A-8 paragraphs [0004], [0013] - [0105] -----	1-24
X	US 2020/014671 A1 (ISAACSON THOMAS M [US] ET AL) 9 January 2020 (2020-01-09) abstract; claims 1-20; figures 1-36 paragraphs [0007] - [0015], [0074] - [0277] ----- -/--	1-24
☒ 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 11 July 2022		Date of mailing of the international search report 19/07/2022
Name and mailing address of the ISA/ European Patent Office, P.B. 5618 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Streit, Stefan

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/025285

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	HAZARIKA PINKU ET AL: "Recommendations for Webview Based Mobile Applications on Android", 2014 IEEE INTERNATIONAL CONFERENCE ON ADVANCED COMMUNICATIONS, CONTROL AND COMPUTING TECHNOLOGIES, IEEE, 8 May 2014 (2014-05-08), pages 1589-1592, XP032727071, DOI: 10.1109/ICACCCT.2014.7019375 [retrieved on 2015-01-23] the whole document -----	1-24

1

10

20

30

40

50

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2022/025285

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2020160065 A1	06-08-2020	AU 2020215026 A1	20-05-2021
		CA 3118911 A1	06-08-2020
		CN 113302954 A	24-08-2021
		EP 3918820 A1	08-12-2021
		JP 2022524269 A	02-05-2022
		KR 20210120978 A	07-10-2021
		SG 11202104525X A	28-05-2021
		US 10467622 B1	05-11-2019
		US 2020250659 A1	06-08-2020
		WO 2020160065 A1	06-08-2020
WO 2020154600 A1	30-07-2020	AU 2020210974 A1	29-04-2021
		BR 112021005781 A2	31-08-2021
		CA 3113670 A1	30-07-2020
		CN 113366516 A	07-09-2021
		DE 202020005732 U1	17-03-2022
		EP 3915076 A1	01-12-2021
		JP 2022517781 A	10-03-2022
		KR 20210118805 A	01-10-2021
		SG 11202102871S A	29-04-2021
		US 2020242588 A1	30-07-2020
		US 2021342821 A1	04-11-2021
		US 2021365929 A1	25-11-2021
		US 2022188808 A1	16-06-2022
		WO 2020154600 A1	30-07-2020
US 2020014671 A1	09-01-2020	US 2019306137 A1	03-10-2019
		US 2020014671 A1	09-01-2020
		US 2020076782 A1	05-03-2020
		US 2020127985 A1	23-04-2020
		US 2020195623 A1	18-06-2020
		US 2020242682 A1	30-07-2020
		US 2020402138 A1	24-12-2020
		US 2021174426 A1	10-06-2021
		US 2021174429 A1	10-06-2021
		US 2021350443 A1	11-11-2021
		US 2022148073 A1	12-05-2022
		US 2022156820 A1	19-05-2022

フロントページの続き

MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,N
E,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,
CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,IT,JM,JO,J
P,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,N
A,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,ST,SV,SY,TH,TJ,
TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

ブ 1 6 8 0、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 2 2 1 0 2 バージニア州マクリーン、キャピタル・ワン・ドライブ 1 6 8 0、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

F ターム (参考) 5L020 AA72