(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6986548号
(P6986548)
(45)発行日　令和3年12月22日(2021.12.22)　(24)登録日　令和3年12月1日(2021.12.1)

(51)Int.Cl.　F I
G06F 21/35 (2013.01)　G06F 21/35

請求項の数 20　(全 53 頁)

(21)出願番号　特願2019-503553(P2019-503553)
(86)(22)出願日　平成29年7月28日(2017.7.28)
(65)公表番号　特表2019-526122(P2019-526122A)
(43)公表日　令和1年9月12日(2019.9.12)
(86)国際出願番号　PCT/US2017/044371
(87)国際公開番号　WO2018/022993
(87)国際公開日　平成30年2月1日(2018.2.1)
審査請求日　令和2年7月27日(2020.7.27)
(31)優先権主張番号　62/368,969
(32)優先日　平成28年7月29日(2016.7.29)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　517305861
トゥルソナ，インコーポレイテッド
アメリカ合衆国，アリゾナ州　８５２６０，スコッツデール，イースト　シー　ブールバード　８７７６，スイート　１０６，ナンバー６０３
(74)代理人　100079108
弁理士　稲葉　良幸
(74)代理人　100109346
弁理士　大貫　敏史
(74)代理人　100117189
弁理士　江口　昭彦
(74)代理人　100134120
弁理士　内藤　和彦

最終頁に続く

(54)【発明の名称】アンチリプレイ認証のシステムおよび方法

(57)【特許請求の範囲】
【請求項１】
ユーザまたは取引を認証する方法であって、
ユーザデバイスを使用して物理トークンの画像データをキャプチャすることであって、前記画像データがグラフィカルコードを含むことと、
前記画像データから前記ユーザに関する識別情報を取得することと、
ローカルデータが収集される瞬間の（１）前記ユーザデバイスの物理的状態または（２）前記ユーザデバイスに一意の前記画像データの特性についての複数タイプの前記ローカルデータを収集することと、
前記複数タイプのローカルデータを結びつけることによって、ノンスデータを生成することと、
（１）前記識別情報および（２）前記ノンスデータに基づいて、前記ユーザまたは前記取引を１つまたは複数のプロセッサを用いて認証することと
を含む、方法。
【請求項２】
前記物理トークンが、前記ユーザに関する前記識別情報を含む前記グラフィカルコードを含む、請求項１に記載の方法。
【請求項３】
前記物理トークンが、権限エンティティによって発行され、前記ユーザのアイデンティティと関連付けられる、請求項１に記載の方法。

【請求項４】
前記複数タイプのローカルデータが、（ｉ）前記画像データをキャプチャする動作のために前記ユーザデバイスに連結された画像デバイスの１つまたは複数の動作パラメータ、または（ｉｉ）前記画像データがキャプチャされる瞬間の前記画像デバイスに一意の前記画像データのキャプチャの１つまたは複数の特性に関する、請求項１に記載の方法。
【請求項５】
前記ユーザデバイスの前記物理的状態に関する前記複数タイプのローカルデータが、１つまたは複数のセンサによって収集されたデータを含む、請求項１に記載の方法。
【請求項６】
前記ユーザデバイスの前記物理的状態が、前記ユーザデバイスの構成要素の物理的状態を示すデータを含み、前記構成要素が、画像デバイス、電源ユニット、プロセッサ、およびメモリを含むグループから選択される、請求項１に記載の方法。
【請求項７】
前記画像データの前記特性が、前記ユーザに関する前記識別情報を抽出する前記画像データの画像処理から得られる、請求項１に記載の方法。
【請求項８】
前記画像データのキャプチャの前記１つまたは複数の特性は、前記グラフィカルコードを含む領域の：ひずみ、回転角度、幅、高さ、座標を含むグループから選択される少なくとも１つの項目を含む、請求項４に記載の方法。
【請求項９】
前記ノンスデータおよび識別データが、リプレイアタックの存在を判断するために、以前に収集されたノンスデータおよび以前に収集された識別データと比較される、請求項１に記載の方法。
【請求項１０】
ユーザまたは取引の認証を行うためのシステムであって、
ユーザが取引を行うのを許可するように構成される、ユーザデバイスと通信状態にあるサーバを備え、前記サーバが、（ｉ）ソフトウェア命令のセットを格納するためのメモリと、（ｉｉ）１つまたは複数のプロセッサとを備え、前記１つまたは複数のプロセッサが、
ローカルデータが収集される瞬間の（１）前記ユーザデバイスの物理的状態、および（２）前記ユーザデバイスに一意の画像データの特性についての複数タイプの前記ローカルデータを受け取ることであって、前記画像データがグラフィカルコードを含むこと、
前記複数タイプのローカルデータを結びつけることによって、ノンスデータを生成すること、
前記ユーザによって保有される物理トークンの前記画像データを受け取ること、
前記画像データから前記ユーザに関する識別情報を取得すること、ならびに
（１）前記識別情報および（２）前記ノンスデータに基づいて前記ユーザまたは前記取引を認証すること
を行うソフトウェア命令の前記セットを実行するように構成される、システム。
【請求項１１】
前記物理トークンが、前記ユーザに関する前記識別情報を含む前記グラフィカルコードを含む、請求項１０に記載のシステム。
【請求項１２】
前記物理トークンが、権限エンティティによって発行され、前記ユーザのアイデンティティと一意に関連付けられる、請求項１０に記載のシステム。
【請求項１３】
前記複数タイプのローカルデータが、（ｉ）前記画像データをキャプチャする動作のために前記ユーザデバイスに連結された画像デバイスの１つまたは複数の動作パラメータ、または（ｉｉ）前記画像データがキャプチャされる瞬間の前記画像デバイスに一意の前記画像データのキャプチャの１つまたは複数の特性に関する、請求項１０に記載のシステム

。
【請求項１４】
前記画像デバイスの前記１つまたは複数の動作パラメータのうちの少なくとも１つが、時間によって変えられる、請求項１３に記載のシステム。
【請求項１５】
前記ユーザデバイスの前記物理的状態が、１つまたは複数のセンサによって収集されたデータを含む、請求項１０に記載のシステム。
【請求項１６】
前記ユーザデバイスの前記物理的状態が、前記ユーザデバイスの構成要素の物理的状態を示すデータを含み、前記構成要素が、画像デバイス、電源ユニット、プロセッサ、およびメモリを含むグループから選択される、請求項１０に記載のシステム。
【請求項１７】
前記画像データの前記特性が、前記ユーザに関する前記識別情報を抽出する前記画像データの画像処理から得られる、請求項１０に記載のシステム。
【請求項１８】
前記ノンスデータおよび識別データが、リプレイアタックの存在を判断するために、以前に収集されたノンスデータおよび以前に収集された識別データと比較される、請求項１０に記載のシステム。
【請求項１９】
アンチリプレイ防御によってユーザまたは取引を認証する方法であって、
ユーザデバイスを使用して物理トークンの画像データをキャプチャすることと、
ローカルデータが収集される瞬間の（１）前記画像データをキャプチャする動作に関連した前記ユーザデバイスの物理的状態、または（２）前記ユーザデバイスに一意の前記画像データの特性に関する複数タイプの前記ローカルデータを収集することと、
前記複数タイプのローカルデータを結びつけることによって、ノンスデータを生成することと、
前記ユーザデバイスまたは前記ユーザに関する識別情報を取得することと、
以前に収集されたノンスデータおよび以前に収集された識別情報と前記ノンスデータおよび前記識別情報を１つまたは複数のプロセッサを用いて比較することと、
前記ノンスデータおよび前記以前に収集されたノンス状態データが同一であるかどうかに基づいて、リプレイアタックの存在を前記１つまたは複数のプロセッサを用いて判断することと
を含む、方法。
【請求項２０】
前記複数タイプのローカルデータが、（ｉ）前記画像データをキャプチャする動作中の、前記ユーザデバイスに連結された画像デバイスの１つまたは複数の動作パラメータ、または（ｉｉ）前記画像データがキャプチャされる瞬間の前記画像デバイスに一意の前記画像データのキャプチャの１つまたは複数の特性に関する、請求項１９に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
[0001] 本出願は、その内容全体が参照により本明細書に組み込まれる、２０１６年７月２９日に出願の米国仮出願第６２／３６８，９６９号の優先権および利益を主張する。
【背景技術】
【０００２】
[0002] リプレイアタックは、詐欺的取引、特に電子商取引において大きな役割を演じる。リプレイアタックでは、特にユーザまたはデバイスを認証するために、以前の取引のデータが、新しい取引で詐欺的にまたは悪意をもって繰り返し用いられる。
【０００３】

[0003] 運転免許証または他の任意のタイプのＩＤカード上のバーコードなどの機械可読セキュア識別トークンが、認証に使用されることが知られている。携帯電話のカメラを使用するときに、従来の物理トークンはデジタルカメラによってスキャンされ、認証または識別のために使用されることがある。しかし、このような静的なセキュリティトークンはリプレイアタックにさらされる。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

[0004] したがって、リプレイアタックに対する耐性がある、ユーザアイデンティティの認証のための改善されたシステムおよび方法に対する要望がある。

【課題を解決するための手段】

【０００５】

[0005] 本発明の１つの態様において、アンチリプレイ分析を行う方法が提供される。リプレイアタックに対する耐性があるトークンを使用するユーザ認証のための方法およびシステムが提供される。取引中に、物理トークンの画像を撮るために、カメラを装備したユーザデバイスが使用されてよい。取引中に、画像の状態、カメラの状態、またはユーザデバイスの状態に関するデータが収集されてよい。このようなデータは、繰り返し用いられることがないか、または繰り返し用いられる可能性が極めて低い特異値すなわち「ノンス」を作り出すために使用されてよい。その後の取引でノンスデータが同様に繰り返し用いられる場合、ノンスデータが繰り返し現れる可能性は極めて低いので、その後の取引がリプレイアタックである可能性のあることを示せる注意を促すことができる。

【０００６】

[0006] １つの態様において、ユーザまたは取引を認証する方法が提供される。方法は、ユーザデバイスを使用して物理トークンの画像データをキャプチャすることであって、画像データがグラフィカルコードを含む、キャプチャすることと、画像データからユーザに関する識別情報を取得することと、ノンスデータが収集される瞬間の（１）ユーザデバイスの物理的状態、または（２）ユーザデバイスに一意の画像データの特性を含むノンスデータを収集することと、（１）識別情報および（２）ノンスデータに基づいて、ユーザまたは取引を１つまたは複数のプロセッサを用いて認証することとを含む。

【０００７】

[0007] いくつかの実施形態において、物理トークンは、ユーザに関する識別情報を含むグラフィカルコードを含む。いくつかの実施形態において、物理トークンは、権限エンティティによって発行され、ユーザのアイデンティティと関連付けられる。

【０００８】

[0008] いくつかの実施形態において、ノンスデータは、（ｉ）画像データをキャプチャする動作のためにユーザデバイスに連結された画像デバイスの１つまたは複数の動作パラメータ、（ｉｉ）画像デバイスまたはユーザデバイスに関する位置情報、および（ｉｉｉ）画像データの画像処理から導出された画像データの特性のうちの少なくとも２つを含む。いくつかのケースにおいて、ユーザデバイスの物理的状態に関するノンスデータは、１つまたは複数のセンサによって収集されたデータを含む。いくつかのケースにおいて、ユーザデバイスの物理的状態は、ユーザデバイスの構成要素の物理的状態を示すデータを含み、いくつかの状況において、構成要素は、画像デバイス、電源ユニット、プロセッサ、およびメモリを含むグループから選択される。いくつかの実施形態において、画像データの特性は、（ｉ）画像処理中に生み出される１つまたは複数のパラメータ、（ｉｉ）未加工の画像データの１つまたは複数のプロパティ、および（ｉｉｉ）処理された画像データの１つまたは複数のプロパティのうちの少なくとも１つを含む。

【０００９】

[0009] いくつかの実施形態において、ノンスデータが２つ以上のファクタを含むときに、これらのファクタが１つまたは複数のプロセッサによってアクセスできないように、ノンスデータが暗号化される。いくつかの実施形態において、ノンスデータおよび識別デー

タは、リプレイアタックの存在を判断するために、以前に収集されたノンスデータおよび以前に収集された識別データと比較される。

【００１０】

[0010] 別の態様において、ユーザまたは取引の認証を行うためのシステムが提供される。システムは、ユーザが取引を行うのを許可するように構成される、ユーザデバイスと通信状態にあるサーバを備え、サーバが、（ｉ）ソフトウェア命令のセットを格納するためのメモリと、１つまたは複数のプロセッサとを備え、１つまたは複数のプロセッサが、（ｉｉ）ノンスデータが収集される瞬間の（１）ユーザデバイスの物理的状態、および（２）ユーザデバイスに一意の画像データの特性を含むノンスデータを受け取ることであって、画像データがグラフィカルコードを含む、ノンスデータを受け取ること、ユーザによって保有される物理トークンの画像データを受け取ること、画像データからユーザに関する識別情報を取得すること、ならびに（１）識別情報および（２）ノンスデータに基づいてユーザまたは取引を認証することを行うソフトウェア命令のセットを実行するように構成される。

【００１１】

[0011] いくつかの実施形態において、物理トークンは、ユーザに関する識別情報を含むグラフィカルコードを含む。いくつかの実施形態において、物理トークンは、権限エンティティによって発行され、ユーザのアイデンティティと一意に関連付けられる。

【００１２】

[0012] いくつかの実施形態において、ノンスデータは、（ｉ）画像データをキャプチャする動作のためにユーザデバイスに連結された画像デバイスの１つまたは複数の動作パラメータ、（ｉｉ）画像デバイスまたはユーザデバイスに関する位置情報、および（ｉｉｉ）画像データの画像処理から導出された画像データの特性のうちの少なくとも２つを含む。いくつかのケースにおいて、画像デバイスの１つまたは複数の動作パラメータのうちの少なくとも１つが、システムによって生成された命令に応答して変えられる。いくつかの実施形態において、ユーザデバイスの物理的状態は、１つまたは複数のセンサによって収集されたデータを含む。いくつかの実施形態において、ユーザデバイスの物理的状態は、ユーザデバイスの構成要素の物理的状態を示すデータを含み、構成要素は、画像デバイス、電源ユニット、プロセッサ、およびメモリを含むグループから選択される。いくつかの実施形態において、画像データの特性は、（ｉ）画像処理中に生み出される１つまたは複数のパラメータ、（ｉｉ）未加工の画像データの１つまたは複数のプロパティ、および（ｉｉｉ）処理された画像データの１つまたは複数のプロパティのうちの少なくとも１つを含む。いくつかの実施形態において、ノンスデータおよび識別データは、リプレイアタックの存在を判断するために、以前に収集されたノンスデータおよび以前に収集された識別データと比較される。

【００１３】

[0013] 別の態様において、アンチリプレイ防御によってユーザまたは取引を認証する方法が提供される。方法は、ユーザデバイスを使用して物理トークンの画像データをキャプチャすることと、ノンスデータが収集される瞬間の（１）画像データをキャプチャする動作に関連したユーザデバイスの物理的状態、または（２）ユーザデバイスに一意の画像データの特性に関するノンスデータを収集することと、ユーザデバイスまたはユーザに関する識別情報を取得することと、以前に収集されたノンスデータおよび以前に収集された識別情報とノンスデータおよび識別情報を１つまたは複数のプロセッサを用いて比較することと、ノンスデータおよび以前に収集されたノンス状態データが同一であるかどうかに基づいて、リプレイアタックの存在を１つまたは複数のプロセッサを用いて判断することとを含む。いくつかの実施形態において、ノンスデータは、（ｉ）画像データをキャプチャする動作中の、ユーザデバイスに連結された画像デバイスの１つまたは複数の動作パラメータ、（ｉｉ）画像デバイスまたはユーザデバイスに関する位置情報、および（ｉｉｉ）画像データの画像処理から導出された画像データの１つまたは複数の特性のうちの少なくとも１つを含む。

【００１４】
参照による組込み
[0014] 本明細書で言及されるすべての文献、特許、および特許出願は、それぞれの個別の文献、特許、または特許出願が参照により組み込まれるものとして具体的かつ個別に示されたかのように、同じ広がりに対して本明細書に参照により組み込まれる。
【００１５】
[0015] 本発明の諸原理が利用される例証的な実施形態を示す以下の詳細な説明、および添付の図面を参照することによって、本発明の特徴および利点のよりよい理解が得られる。
【図面の簡単な説明】
【００１６】
【図１】[0016]本発明の実施形態による、認証を要する取引の実行を支援できるデバイスの例を示す図である。
【図２】[0017]本発明の実施形態による、認証のためにユーザデバイスを使用して物理トークンをキャプチャする例を示す図である。
【図３】[0018]本発明の実施形態による、ノンスデータとして使用され得る、画像キャプチャおよび画像処理中に生成されるデータの例を示す図である。
【図４】[0019]本発明の実施形態による、どのようにしてノンスデータが生成または格納され得るかについての例を示す図である。
【図５】[0020]本発明の実施形態による、様々な取引に対して、どのようにしてデータが格納され得るかについての例を示す図である。
【図６】[0021]本発明の実施形態による、どのようにしてノンスデータおよび識別データが認証パラメータを形成するために使用され得るかを示す図である。
【図７】[0022]本発明の実施形態による、識別データおよびノンスデータを使用して、ユーザおよび／またはデバイスを識別する例を示す図である。
【図８】[0023]本発明の実施形態による、ノンスデータを使用して、ユーザおよび／またはデバイスを識別する例を示す図である。
【図９】[0024]本発明の実施形態による、認証イベントに関わるエンティティの例を提供する図である。
【発明を実施するための形態】
【００１７】
[0025] 本発明の好ましい実施形態が本明細書で示され、説明されたが、このような実施形態がほんの一例として提供されるということが当業者には明らかであろう。非常に多くの変形、変更、および代用が、本発明から逸脱することなく、すぐに当業者に想起されるであろう。本明細書で説明される本発明の実施形態に対する様々な代替が、本発明を実践する際に用いられてよいということを理解されたい。
【００１８】
[0026] 本発明は、リプレイアタックに対する耐性があるトークンを使用する、ユーザ認証のためのシステムおよび方法を提供する。本明細書で説明される本発明の様々な態様が、下記に示される特定の応用例のいずれかに適用されてよい。本発明は、認証システムとして、あるいはスタンドアロンのアンチリプレイシステム、詐欺行為検出ソフトウェア、またはアイデンティティの確認もしくは認証を要する任意の取引処理として適用されてよい。本発明の様々な態様が、個別に、まとめて、または互いに組み合わされて理解されてよいということが理解されよう。
【００１９】
[0027] 取引は、ユーザ認証または本人確認を要するイベントまたは活動であってよい。ユーザアイデンティティ情報は、機械可読セキュア識別トークン（例えばユーザのＩＤカード上のバーコード）などの物理トークンに基づいて提供されてよい。オンライン取引上に関して、ユーザは、本人確認のために物理トークンをスキャンし、サービス提供者にＩＤ情報を伝送することができる。取引はオンラインで発生させることができるが、この場

合、データは簡単に傍受されることもある。例えば、最初の取引中のユーザに関する情報が記録されることがある。記録された情報は、最初の取引に現れた同じユーザに見えるように、またはその後の取引が通り抜けることを許可するように、リプレイアタックにおけるその後の取引の中で使用されることがある。最初の取引の中で使用されたスキャン画像データまたは画像デバイスの状態に関連したノンスデータなどの記録された情報は、最初の取引の状況に関係することがある。ノンスデータの繰返しを検出することは、リプレイアタックが発生していることを示すことができる。

【００２０】

[0028] いくつかの実施形態において、最初の取引中のスキャン画像または画像デバイスの状態に関するノンスデータが収集されてよい。ノンスデータは、現実的には一度しか発生することがなく、当然、繰り返し用いられないであろう特異値（例えばノンスファクタ）の１つまたは複数のセットを含むことができる。したがって、ノンスデータの繰返しは、リプレイアタックが発生している可能性があるという疑いの根拠であってよい。ノンスデータは、画像デバイスまたは画像デバイスの構成要素の内部状態に関係してよく、またはユーザの識別データを収める、スキャン画像に関して収集され得るデータを含んでもよい。ノンスデータは、メタデータ、位置情報、または画像デバイスに関する他の任意の情報などの画像キャプチャ情報を含むことができる。ノンスデータは、コンテキスト分析のために画像の処理中に生成されるデータ含むこともできる。

【００２１】

[0029] ノンスデータは、１つまたは複数のセンサおよび１つまたは複数のプロセッサを用いて収集されてよい。センサおよびプロセッサは、デバイスに搭載されていてよい。センサおよびプロセッサは、デバイスの外部から収集される外部信号またはデータの使用を必要としても、しなくてもよい。

【００２２】

[0030] 図１は、本発明の実施形態による、認証を要する取引の実行を支援できるデバイス１００の例を示す。デバイスは、ディスプレイ１０２を含むユーザデバイスであってよく、デバイスを使用して取引を行うためのインターフェース１０４を含むことができる。デバイスは、１つもしくは複数のメモリストレージユニット１０６、１つもしくは複数のプロセッサ１０８、１つもしくは複数の通信ユニット１１０、１つもしくは複数の電力源１１２、および／または１つもしくは複数のセンサ１１４、１１６を含むことができる。

【００２３】

[0031] ユーザデバイス１００は、取引またはユーザの識別および／もしくは認証を支援できる電子デバイスであってよい。ユーザデバイスは、モバイルデバイス（例えば、スマートフォン、タブレット、ポケットベル、パーソナルデジタルアシスタント（PDA: personal digital assistant））、コンピュータ（例えば、ラップトップコンピュータ、デスクトップコンピュータ、サーバ、または他の任意のタイプのデバイスであってよい。ユーザデバイスは任意選択により携帯型であってよい。ユーザデバイスは手持ち型であってよい。ユーザデバイスは軽量であってよい。いくつかの実施形態において、ユーザデバイスは、重さ１０、８、６、５、４、３、２、１．５、１、０．７、０．５、０．３、０．１、０．０５、０．０１、０．００５、もしくは０．００１ｋｇ、またはそれ以下であってよい。

【００２４】

[0032] ユーザデバイスは、ローカルエリアネットワーク（LAN: local area network）、インターネット、テレコミュニケーションネットワーク、データネットワーク、または他の任意のタイプのネットワークなどの広域ネットワーク（WAN: wide area network）などのネットワークに接続できるネットワークデバイスであってよい。ユーザデバイスは、直接または間接のワイヤレス通信ができてよい。ユーザデバイスは、ピアツーピア（P2P: peer-to-peer）通信および／またはクラウドベースのインフラストラクチャとの通信ができてよい。

【００２５】

[0033] ユーザデバイスは、取引エンティティとの（金融取引などの）取引中に使用されてよい。取引は、資金（例えば、金銭、手形、負債、ローン等）のやりとりを含むことができる。取引は、商品またはサービスのやりとりを含むことができる。取引は、情報のやりとりを含むことができる。取引は、ユーザが情報または場所にアクセスするためのユーザの本人確認または認証を含むことができる。いくつかの例において、取引は、機密のデータおよび／または公然と利用できないデータのやりとりを含むことができる。取引エンティティは、取引に関わる任意のエンティティを含むことができる。取引エンティティは、個人、カンパニー、共同事業、コーポレーション、組織、グループ、主催者、または他の任意のタイプのエンティティであってよい。いくつかの例において、取引エンティティは、金融機関（例えば、銀行、財務管理会社）、商人（例えば、店、オンライン商人）、ソーシャルネットワーキング企業、非営利的組織、医療組織、教育機関、行政体もしくは行政機関、または他の任意のタイプのエンティティを含むことができる。ユーザデバイスは、取引エンティティと直接的または間接的に通信することができてよい。いくつかの実施形態において、取引エンティティは、サーバもしくは他のタイプのオンラインホストを使用することができ、またはこれらであってもよい。ユーザデバイスは、取引エンティティのサーバおよび／または他のホストデバイスと通信することができる。

【００２６】

[0034] ユーザデバイスは、ディスプレイ１０２を含むことができる。ディスプレイは、画像デバイスによってキャプチャされた１つまたは複数の静止画像（例えば写真）および／または動画像（例えばビデオ）をリアルタイムに示すことができる。ディスプレイは、ユーザに情報を提示できてよい。ディスプレイは、情報を視覚的に示すことができる。ディスプレイ上に示される情報は、変えることができてよい。ディスプレイは、液晶ディスプレイ（LCD: liquid crystal display）画面、発光ダイオード（LED: light-emitting diode）画面、有機発光ダイオード（OLED: organic light-emitting diode）画面、プラズマ画面、電子インク（e-ink: electronic ink）画面、タッチスクリーン、または他の任意のタイプの画面もしくはディスプレイなどの画面を含むことができる。ディスプレイは、ユーザ入力を受け入れても、受け入れなくてもよい。

【００２７】

[0035] ディスプレイは、グラフィカルユーザインターフェース１０４を示すことができる。グラフィカルユーザインターフェースは、デバイスを使用してユーザが取引を行うのを支援できるブラウザ、ソフトウェア、またはアプリケーションの一部であってよい。インターフェースは、ユーザがデバイスを使用して自分で識別できるようにすることができる。ユーザは、デバイスを使用してユーザアカウントにアクセスすることができる。ユーザアカウントは、取引中に使用されてよい。ユーザデバイスは、１つまたは複数のソフトウェアアプリケーションを動作させることができてよい。１つまたは複数のアプリケーションは、電子取引に関連するものであってよく、またそうでなくてもよい。１つまたは複数のアプリケーションは、ユーザ識別および／または認証を要するか、または使用することができる。

【００２８】

[0036] ユーザデバイスは、ユーザ対話デバイスを介して入力を受け入れることができる。このようなユーザ対話デバイスの例は、キーボード、ボタン、マウス、タッチスクリーン、タッチパッド、ジョイスティック、トラックボール、カメラ、マイクロフォン、運動センサ、熱センサ、慣性センサ、または他の任意のタイプのユーザ対話デバイスを含むことができる。

【００２９】

[0037] ユーザデバイスは、１つまたは複数の工程を行うためのコード、ロジック、または命令を含む非一時的コンピュータ可読媒体を備えることができる１つまたは複数のメモリストレージユニット１０６を備えることができる。ユーザデバイスは、例えば、非一時的コンピュータ可読媒体に従って、１つまたは複数の工程を実行できる１つまたは複数のプロセッサ１０８を備えることができる。１つまたは複数のメモリストレージユニットは

、１つもしくは複数のソフトウェアアプリケーション、またはソフトウェアアプリケーションに関するコマンドを格納することができる。１つまたは複数のプロセッサは、ソフトウェアアプリケーションの工程を個別にまたはまとめて実行することができる。

【００３０】

[0038] 通信ユニット１１０はデバイス上に提供されてよい。通信ユニットは、ユーザデバイスが外部デバイスと通信できるようにすることができる。外部デバイスは、取引エンティティのデバイス、サーバであってよく、またはクラウドベースのインフラストラクチャであってもよい。通信は、ネットワーク上の通信、または直接の通信を含むことができる。通信ユニットは、ワイヤレスまたは有線の通信を許可することができる。ワイヤレス通信の例は、ＷｉＦｉ、３Ｇ、４Ｇ、ＬＴＥ、無線周波数、Ｂｌｕｅｔｏｏｔｈ、赤外線、または他の任意のタイプの通信を含むことができるがこれらに限定されない。通信ユニットは、ノンスデータを判断するために使用されるデータの収集を支援できても、できなくてもよい。

【００３１】

[0039] デバイスは、オンボード電力源１１２を有することができる。代替として、外部電力源は、ユーザデバイスに電力供給するための電力を提供することができる。外部電力源は、有線接続またはワイヤレス接続を介してユーザデバイスに電力を提供することができる。オンボード電力源は、ユーザデバイスの全体、またはワイヤレスデバイスの１つもしくは複数の個別の構成要素に電力供給することができる。いくつかの実施形態において、デバイスの様々な構成要素に電力供給できる複数のオンボード電力源が提供されてよい。例えば、デバイスの１つまたは複数のセンサは、デバイスの１つまたは複数のメモリストレージユニット、プロセッサ、通信ユニット、および／またはディスプレイとは別のソースを使用して電力供給されてよい。

【００３２】

[0040] ユーザデバイスは、画像デバイス１１４として機能する画像センサを備えることができる。画像デバイス１１４は、ユーザデバイスに搭載されていてよい。画像デバイスは、ハードウェア要素および／またはソフトウェア要素を含むことができる。いくつかの実施形態において、画像デバイスは、ユーザデバイスに動作可能なように連結されたカメラであってよい。いくつかの代替実施形態において、画像デバイスは、ユーザデバイスの外部に配置されてよく、バーコードなどのグラフィカル要素の画像データは、本明細書の他の場所で説明されるような通信手段を介してユーザデバイスに伝送されてよい。画像デバイスは、視覚コードをスキャンするように構成されたアプリケーション／ソフトウェアによって制御されてよい。いくつかの実施形態において、カメラは、ＩＤカード、パスポート、文書上のバーコード、または外部ディスプレイ上に表示されたバーコードをスキャンするように構成されてよい。いくつかの実施形態において、ソフトウェアおよび／またはアプリケーションは、コードをスキャンするためにユーザデバイス上のカメラを起動させるように構成されてよい。他の実施形態において、カメラは、ユーザデバイスに元々組み込まれているプロセッサによって制御されてよい。

【００３３】

[0041] 画像デバイス１１４は、固定焦点レンズまたは自動焦点レンズのカメラであってよい。画像デバイスは、光の波長に応答して電気信号を生成する相補型金属酸化膜半導体（CMOS: complementary metal oxide semiconductor）センサを使用することができる。結果として生じた電気信号は、画像データを生み出すために処理されてよい。画像デバイスは、画像センサ上に光を向けるように構成されたレンズを含むことができる。カメラは、動画像データ（例えばビデオ）をキャプチャするムービーカメラまたはビデオカメラであってよい。カメラは、静止画像（例えば写真）をキャプチャするスチルカメラであってよい。カメラは、動画像データと静止画像の両方をキャプチャすることができる。カメラは、動画像データのキャプチャと静止画像のキャプチャとの間で切り替えることができる。本明細書で提供される一定の実施形態はカメラに関して説明されるが、本開示は、任意の適切な画像デバイスに適用されてよく、カメラに関する本明細書におけるいずれかの説

明が、任意の適切な画像デバイスに適用されてもよく、カメラに関する本明細書における任意の説明が、他のタイプの画像デバイスに適用されてもよいということが理解されよう。カメラは、光学的な要素（例えば、レンズ、ミラー、フィルタ等）を備えることができる。カメラは、カラー画像、グレースケール画像、および同様のものをキャプチャすることができる。

【００３４】

[0042] 画像デバイス１１４は、デバイスの近くの視覚画像をキャプチャするために使用されるカメラであってよい。デバイスの近くの熱画像をキャプチャするために使用されることがある赤外線センサなどの他の任意のタイプのセンサが使用されてよい。画像センサは、電磁スペクトルに沿ったどこかの情報を収集することができ、対応する画像を適宜生成することができる。

【００３５】

[0043] いくつかの実施形態において、画像デバイスは、かなり高い解像度で動作させることができてよい。画像センサは、約１００μｍ、５０μｍ、１０μｍ、５μｍ、２μｍ、１μｍ、０．５μｍ、０．１μｍ、０．０５μｍ、０．０１μｍ、０．００５μｍ、０．００１μｍ、０．０００５μｍ、または０．０００１μｍ以上の解像度を有することができる。画像センサは、４Ｋ以上の画像を収集することができてよい。

【００３６】

[0044] 画像デバイスは、特定の画像解像度で画像フレームまたは一連の画像フレームをキャプチャすることができる。いくつかの実施形態において、画像フレームの解像度は、フレーム内のピクセル数によって定義されてよい。いくつかの実施形態において、画像解像度は、約３５２ｘ４２０ピクセル、４８０ｘ３２０ピクセル、７２０ｘ４８０ピクセル、１２８０ｘ７２０ピクセル、１４４０ｘ１０８０ピクセル、１９２０ｘ１０８０ピクセル、２０４８ｘ１０８０ピクセル、３８４０ｘ２１６０ピクセル、４０９６ｘ２１６０ピクセル、７６８０ｘ４３２０ピクセル、または１５３６０ｘ８６４０ピクセル以上であってよい。

【００３７】

[0045] 画像デバイス１１４は、特定のキャプチャレートで一連の画像フレームをキャプチャすることができる。いくつかの実施形態において、一連の画像は、約０．０００１秒、０．０００２秒、０．０００５秒、０．００１秒、０．００２秒、０．００５秒、０．０１秒、０．０２秒、０．０５秒、０．１秒、０．２秒、０．５秒、１秒、２秒、５秒、または１０秒ごとに１画像以下のレートでキャプチャされてよい。いくつかの実施形態において、キャプチャレートは、ユーザ入力および／または外部条件（例えば光源の明るさ）に応じて変化させることができる。

【００３８】

[0046] 画像デバイスの状態１１４は、画像がキャプチャされるとき、またはバーコードがスキャンされるときの、カメラ、または画像デバイスの画像センサの１つまたは複数の動作パラメータに関する情報を含むことができる。例えば、カメラの状態は、露出時間、ＩＳＯ感度率、焦点距離、フラッシュの使用、ライトバランシング、解像度、または時間、ライトニングなどの環境条件、カメラの方向もしくは位置によって変えられることがある他の任意の情報を含むことができる。いくつかの実施形態において、画像デバイスの状態に関連した追加情報を供給するために、１つまたは複数の追加センサが提供されてよい。

【００３９】

[0047] ユーザデバイスは、画像デバイスの、ある瞬間の位置情報および姿勢情報を提供するために、デバイスに搭載された１つまたは複数のセンサ１１６を有することができる。いくつかの実施形態において、位置情報および姿勢情報は、位置センサ（例えば全地球測位システム（GPS: Global Positioning System））、慣性センサ（例えば、加速度計、ジャイロスコープ、慣性計測ユニット（IMU: inertial measurement unit））、高度センサ、姿勢センサ（例えば方位計）、圧力センサ（例えば気圧計）、および／またはフィー

ルドセンサ（例えば、磁力計、電磁気センサ）、ならびに同様のものなどのセンサによって提供されてよい。

【００４０】

[0048] １つまたは複数のセンサ１１６は、位置センサ（例えば全地球測位システム（GPS）センサ、位置の三角測量を可能にするモバイルデバイス送信機）、視覚センサ（例えば、カメラなど、可視光線、赤外線、もしくは紫外線を検出できる画像デバイス）、近接センサ（例えば、超音波センサ、ライダー、飛行時間型カメラ）、慣性センサ（例えば、加速度計、ジャイロスコープ、慣性計測ユニット（IMU））、高度センサ、圧力センサ（例えば気圧計）、オーディオセンサ（例えばマイクロフォン）、時間センサ（例えば時計）、温度センサ、メモリ使用量および／もしくはプロセッサ使用量を検出できるセンサ、またはフィールドセンサ（例えば、磁力計、電磁気センサ）を含むことができるがこれらに限定されない。１つ、２つ、３つ、４つ、５つ以上のセンサなど、任意の適切な数のセンサ、およびセンサの組合せが使用されてよい。任意選択により、データは、様々なタイプ（例えば、２つ、３つ、４つ、５つ以上のタイプ）のセンサから受け取られてよい。様々なタイプのセンサが、様々なタイプの信号もしくは情報（例えば、位置、方向、速度、加速度、近接、圧力等）を計測することができ、および／または様々なタイプの計測技法を利用してデータを取得することができる。例えば、センサは、能動的センサ（例えば、センサ自体のソースからエネルギーを生成および計測するセンサ）と、受動的センサ（例えば、利用可能なエネルギーを検出するセンサ）の任意の適切な組合せを含むことができる。

【００４１】

[0049] ユーザデバイスに搭載された任意の数のセンサが提供されてよい。センサは、異なるタイプのセンサ、または同じタイプのセンサを含むことができる。センサ、および／もしくは本明細書で説明される他の任意の構成要素は、デバイスの筐体内に取り囲まれるか、デバイスの筐体に組み込まれるか、またはデバイスの筐体の外部にあってよい。筐体は、筐体の内部および／または筐体の外部を隔てる流体密封（例えば水密または気密）の封止を形成しても、しなくてもよい。

【００４２】

[0050] １つもしくは複数のセンサ１１６は、リアルタイムで継続的に情報を収集してよく、または定期的に情報を収集していてもよい。いくつかの実施形態において、センサは、規則的な時間間隔または不規則な時間間隔で情報を収集することができる。センサは、高い頻度で（例えば、分ごともしくはさらに頻繁に、１０秒ごともしくはさらに頻繁に、１秒ごともしくはさらに頻繁に、０．５秒ごともしくはさらに頻繁に、０．１秒ごともしくはさらに頻繁に、０．０５秒ごともしくはさらに頻繁に、０．０１秒ごともしくはさらに頻繁に、０．００５秒ごともしくはさらに頻繁に、０．００１秒ごともしくはさらに頻繁に、０．０００５秒ごともしくはさらに頻繁に、または０．０００１秒ごともしくはさらに頻繁に）情報を収集することができる。センサは、規則的または不規則なスケジュールに従って情報を収集することができる。

【００４３】

[0051] センサは、検出イベントに応答して情報を収集することができる。いくつかの実施形態において、センサは、ユーザの識別／認証を要する取引が始められつつあるか、完了されつつあるか、またはその間の任意の状態にあるときに情報を収集することができる。センサは、ユーザが認証されつつあるときに情報を収集することができる。例えば、センサは、ユーザがログインしつつあるときに情報を収集することができる。センサは、画像をキャプチャするために画像デバイスが起動されるときに情報を収集することができる。センサは、ユーザがユーザアカウントにアクセスしようとしているときに情報を収集することができる。センサは、ユーザが取引の完了をリクエストするときに情報を収集することができる。センサは、ユーザが金銭を受け取るか、または送ることをリクエストするときに情報を収集することができる。

【００４４】

[0052] センサは、ただ１つの時点または複数の時点で情報を収集することができる。いくつかの実施形態において、センサは、時間間隔にわたって（例えば、定期的、継続的、等で）情報を収集することができる。いくつかの実施形態において、時間間隔は、１０秒、５秒、３秒、２秒、１秒、０．５秒、０．３秒、０．１秒、０．０５秒、０．０１秒、０．００５秒、０．００１秒、０．０００５秒、または０．０００１秒以下であってよい。一方、時間間隔は、本明細書で説明される値のいずれか以上であってよく、または本明細書で説明される値のうちのいずれか２つの間の範囲に含まれてもよい。

【００４５】

[0053] 画像デバイスの状態は、画像デバイスに関する位置情報を含むことができる。例えば、位置情報は、画像デバイスの空間的位置（例えば地理位置情報）を含むことができる。いくつかの実施形態において、位置情報は、画像デバイスの緯度、経度、および／または高度を含むことができる。いくつかの実施形態において、位置情報は座標として表現されてよい。位置情報は、画像デバイスの方向を含むことができる。例えば、位置情報は、１軸、２軸、または３軸（例えば、ヨー軸、ピッチ軸、および／またはロール軸）に対するデバイスの方向を含むことができる。位置情報は、画像デバイスの姿勢であってよい。位置情報は、慣性基準系（例えば、環境、地球、重力）、および／または局所基準系について判断されてよい。

【００４６】

[0054] 位置情報は、画像デバイスの動きの情報を含むことができる。例えば、位置情報は、１軸、２軸、または３軸についてのデバイスの線形速度またはデバイスの線形加速度を含むことができる。位置情報は、１軸、２軸、または３軸についてのデバイスの角速度または角加速度を含むことができる。位置情報は、加速度計、ジャイロスコープ、および／または磁力計などの１つまたは複数の慣性センサを用いて収集されてよい。

【００４７】

[0055] 画像デバイスの状態は、画像がキャプチャされるときにユーザデバイスによって収集される環境情報を含むこともできる。環境情報は、デバイスのマイクロフォンによって収集されるオーディオ情報を含むことができる。環境情報は、運動検出器、超音波センサ、ライダー、温度センサ、圧力センサ、またはデバイスの近くの環境情報を収集できる他の任意のタイプのセンサによって収集される情報を含むことができる。環境情報は、デバイスを保持するユーザのタッチまたは手の位置を検出すること、およびデバイスのどの部分がユーザによってタッチまたは保持されるかを収集することを含むことができる。

【００４８】

[0056] 本明細書で説明されるような画像センサは、画像データをキャプチャするために使用されてよい。画像デバイスによって生成される画像データは、１つまたは複数の画像を含むことができ、これらの画像は、静止画像（例えば写真）、動画像（例えばビデオ）、またはこれらの適切な組合せであってよい。画像データは、多色（例えば、RGB、CMYK、HSV）または単色（例えば、グレースケール、白黒、セピア色）であってよい。画像データは、任意の画像フォーマット（例えば、EPSもしくはSVGベクトルグラフ、PNG、GIF、またはJPEGラスターグラフィックスフォーマット、等）であってよい。認証のために使用される画像データはデータベースに格納されても、されなくてもよい。

【００４９】

[0057] キャプチャ画像の状態は、未加工の画像（例えばメタデータ）または画像処理に関わるデータの情報を含むことができる。いくつかのケースにおいて、画像データは、関心のある領域にエンコードされた情報を抽出するために処理されてよい。キャプチャ画像内の関心のある領域は、ユーザによって操作される画像デバイスからキャプチャされるので、変形した形状、むらのある濃度、解像度、大きさを有することがある。例えば、バーコードなどの物理的表現を収めるスキャン画像が、分析または処理されてよい。バーコードの形状は、様々なアルゴリズムまたは方法を使用して正規化されてよい。例えば、バーコードの形状は最初に、エッジ検出および／またはコーナー検出によって認識され、逆遠近変換によって正規化され、バイナリ画像データに変換され、デコードされてよい。画像

処理動作（例えば、ひずみ除去（de-skewness）、トリミング、正規化、強調、フィルタリング、等）の間に多量のパラメータが生成されてよい。いくつかのケースにおいて、画像処理は、バーコード中にエンコードされたアイデンティティ情報を抽出するために適用されてよい。別の例において、画像の特性またはプロパティ（例えば、強さ、幅、高さ、解像度、等）の分析から大量のパラメータが取得されてよい。画像または画像処理に関連したノンスデータについての詳細は、本明細書において後で説明される。

【００５０】

[0058] 画像デバイスおよび画像データの状態に関する情報は、ノンスデータとして格納されてよい。ノンスデータは、１つまたは複数のセンサ、ならびに１つまたは複数のプロセッサから生成された情報を収めることができる。

【００５１】

[0059] いくつかの実施形態において、ノンスデータは、センサデータから生成された情報を含むことができる。いくつかの実施形態において、ただ１つのセンサからの情報がノンスデータとして格納されてよい。一方、複数のセンサからの情報がノンスデータとして格納されてもよい。ノンスデータは、ただ１つの時点で、または時間間隔にわたって収集されたセンサ情報を含むことができる。ノンスデータは、未加工のセンサ情報を含んでよく、または処理されたセンサ情報を含んでもよい。ノンスデータは、センサ情報に基づいて生成されてよい。いくつかの実施形態において、ノンスデータは、センサ情報のハッシュから導出されてよく、またはセンサ情報のハッシュであってもよい。ノンスデータは、現実的に繰り返し用いられるはずのない少なくともいくつかのセンサ情報から導出されてよい。例えば、画像デバイスの位置（例えば方向）が、高レベルの特異性で正確に繰り返し用いられる可能性は低い。ノンスデータが現実的に繰り返し用いられるはずはない。ノンスデータは現実的には、たった１回だけしか発生しない。ノンスデータは、一度しか生成または使用されない可能性が非常に高い可能性がある特異値を表すことができる。したがって、ノンスデータの何らかの繰返しは、リプレイアタックが発生している可能性があるという信号である可能性がある。

【００５２】

[0060] ノンスデータは、センサデータが収集される同じ頻度で生成されてよい。一方、ノンスデータは、センサデータが収集される頻度より低い頻度で生成されてよい。１つの例において、センサデータは、継続的にまたは高い頻度で情報を収集することができ、一方、ノンスデータは、検出イベントに応答して生成および／または格納されてよい。いくつかの実施形態において、収集されたセンサデータのすべてが、ノンスデータを生成するために使用されてよい。一方、収集されたセンサデータの一部が、ノンスデータを生成するために使用されてもよい。

【００５３】

[0061] いくつかの実施形態において、ノンスデータは、画像データの分析および／または処理に関連した１つまたは複数のプロセッサによって生成されたデータをさらに含むことができる。１つまたは複数のプロセッサは、ユーザデバイスに搭載されていてよい。画像キャプチャデバイスのマイクロプロセッサなどの１つまたは複数のプロセッサは、画像デバイスに搭載されていてよい。いくつかの実施形態において、１つまたは複数のプロセッサは、キャプチャ画像データの事前処理を行うこと、およびメタデータと共に画像データを他のプロセッサに出力することを行うように構成されてよい。いくつかの実施形態において、１つまたは複数のプロセッサは、画像データに収められた視覚トークンからアイデンティティ情報を抽出するためにパターン認識を行うことなど、キャプチャ画像データを処理することを行うように構成されてよい。したがって、視覚トークン画像の様々なパラメータおよび特性が、画像処理動作中および／または画像分析中に生成されてよい。パラメータは、画像キャプチャデバイスによる未加工の画像の自動調節（例えば、バランス補正、ガンマ補正、モザイク除去（de-mosaicing）、スペックル除去（de-speckle）、等）などの事前処理動作中に取得されてよい。画像セグメント化、エッジ検出、コーナー検出、パターン検出、画像のスキュー角および回転の計測、ピクセルコンテンツおよびヒス

トグラムの計測、画像スケーリング、平滑化、形態学的フィルタ、ならびに同様のものなどのパラメータは、物理トークンを認識するため、および／またはトークンをデコードするために画像処理動作中に取得されてよい。動作は、画像全体、または関心のある認識された領域に適用されてよい。

【００５４】

[0062] ノンスデータは、画像デバイスの状態およびキャプチャ画像データの状態に関連したデータを含むことができる。データは、視覚トークンの画像が認証のためにキャプチャされ、処理され、分析されるときに収集されてよい。いくつかの実施形態において、収集データのすべてが、ノンスデータを生成するために使用されてよい。一方、収集データのすべてが、ノンスデータを生成するために使用されてよいわけではない。

【００５５】

[0063] ノンスデータは、デバイス内で生成されてよい。例えば、ノンスデータは、デバイスの１つまたは複数のプロセッサを使用して生成されてよい。ノンスデータは、デバイスの１つまたは複数のメモリストレージユニットに格納されてよい。ノンスデータは、外部デバイスまたはネットワークに通信ユニットを用いて伝送されてよい。一方、ノンスデータは、デバイス外で生成されてもよい。ユーザデバイスに搭載された１つまたは複数のセンサおよび１つまたは複数のプロセッサからのデータは、外部デバイスまたはネットワークに通信ユニットを用いて伝送されてよい。センサおよびプロセッサからのデータは、伝送される前にメモリに格納されても、されなくてもよい。センサおよびプロセッサからのデータは、ノンスデータを生成するために外部デバイスまたはネットワークで使用されてよい。

【００５６】

[0064] 図２は、本発明の実施形態による、認証のためにユーザデバイス２０３を使用して物理トークン２０７をキャプチャする例を示す。ユーザデバイス２０３は、物理トークン２０７の画像をキャプチャすることによって識別データとノンスデータの両方を生成するために使用されてよく、認証のためにこれらのデータを使用してもよい。

【００５７】

[0065] 識別データは、ユーザのアイデンティティを認証または確認するために使用される情報を収めることができる。識別データは、ユーザアイデンティティを表す名前、生年月日、住所、国籍、および同様のものなどの個人情報を収めることができる。識別データは、製品またはサービスのアイデンティティを表す取扱説明、購入オプション、サービス提供者情報、および同様のものなどの製品情報を収めることができる。識別データは、ユーザ、サービス、取引、および同様のものを一意に識別できる任意のタイプの情報を収めることができる。識別データは、同じユーザ、同じサービス、または同じ取引に関係がある情報を収めることができる。いくつかの実施形態において、情報または識別子は、識別データの中で前もって暗号化される暗号文であってよい。情報を解読するために、秘密鍵またはパスワードが要求されることがある。他の実施形態において、識別データは、非暗号化データである平文であってよい。

【００５８】

[0066] いくつかの実施形態において、識別データは、物理トークン２０７の中にエンコードされてよい。物理トークンは、適切なデバイス（例えば、バーコードリーダ、光学式スキャナ、カメラ）によってスキャンされることが可能な、または機械可読であることが可能な視覚グラフィカル要素であってよい。視覚グラフィカル要素は、デバイス上でキャプチャおよび／または表示されることが可能なバーコード、テキスト、画像、一連のこれら、または同様のものなどの任意のフォーマットであってよい。視覚グラフィカル要素は、ＰＤＦ４１７、Ａｚｔｅｃ、ＭａｘｉＣｏｄｅ、およびＱＲコード、等などの２次元バーコードであってよい。視覚グラフィカル要素は、Ｉｎｔｅｒｌｅａｖｅｄ２／５、Ｉｎｄｕｓｔｒｉａｌ２／５、Ｃｏｄｅ３９、Ｃｏｄｅ３９　Ｅｘｔｅｎｄｅｄ、Ｃｏｄａｂａｒ、Ｃｏｄｅ１１、Ｃｏｄｅ１２８、Ｃｏｄｅ１２８　Ｅｘｔｅｎｄｅｄ、ＥＡＮ／ＵＣＣ１２８、ＵＰＣ－Ｅ、ＵＰＣ－Ａ、ＥＡＮ－８、ＥＡＮ－１３、Ｃｏｄｅ９３、Ｃｏ

ｄｅ９３ Ｅｘｔｅｎｄｅｄ、ＤａｔａＢａｒ Ｏｍｎｉｄｉｒｅｃｔｉｏｎａｌ（RSS-14）、ＤａｔａＢａｒ Ｔｒｕｎｃａｔｅｄ（RSS-14 Truncated）、ＤａｔａＢａｒ Ｌｉｍｉｔｅｄ（RSS Limited）、ＤａｔａＢａｒ Ｓｔａｃｋｅｄ、ＤａｔａＢａｒ Ｅｘｐａｎｄｅｄ、ＤａｔａＢａｒ Ｅｘｐａｎｄｅｄ Ｓｔａｃｋｅｄ、および同様のものなどの１次元バーコードであってよい。バーコードは、バイナリ、英数字、またはＡＳＣＩＩなどの任意のタイプの適切なフォーマットで様々なタイプの情報をエンコードすることができ、コードは任意の標準に基づいてよい。視覚グラフィカル要素は、一定量のデータをエンコードできる様々なストレージ容量、および可変物理サイズを有してよい。いくつかの実施形態において、バーコードは、標準バーコードリーダによって読み取られることが可能な既知の標準に適合させることができる。他の実施形態において、認証システムによって提供され、認証された認証済アプリケーションによってのみ読み取られることが可能になるように、バーコードは独自のものであってよく、この認証されたアプリケーションはユーザデバイス上で実行することができる。いくつかの例において、認証システムまたは認証アプリケーションだけが、バーコードを暗号化／解読することができる。

【００５９】

[0067] 図２は、物理トークン２０７のある例示的な物理要素２０５を示す。いくつかの実施形態において、物理トークン２０７は、ユーザによって保有される物理要素２０５上の視覚グラフィカルコードであってよい。物理要素２０５は、エンティティまたはサービス提供者によって発行または提供される、カード（ＩＤカード、運転免許証、ペイメントカード、図書館カード、ログインカード、等）、文書（パスポート、法律文書、医療記録、等）、および同様のものであってよい。いくつかのケースにおいて、物理要素は、カード、紙の文書、または政府、ＤＭＶ、連邦政府機関、および同様のものなどの権限エンティティによって発行される他の形式の資格証明書であってよい。いくつかの実施形態において、物理要素は、社会保障カード、パスポート、運転免許証、ｅ－パスポート、出生証明書、従業員アイデンティティカード、および同様のものなどの、一個人の市民資格証明書であってよい。さらに、データベース内のレコード、電子アイデンティティ情報、および同様のものを含むことができる物理要素が、ユーザのアイデンティティを確立するために使用されてよい。

【００６０】

[0068] いくつかの実施形態において、物理トークン２０７は、ディスプレイデバイス上に表示されることが可能な視覚グラフィカルコードであってよい。ディスプレイデバイスは、セッションまたは取引を行うためにユーザの認証または確認を要する、コンピュータ（例えば、ラップトップコンピュータ、デスクトップコンピュータ）、モバイルデバイス（例えば、スマートフォン、タブレット、ポケットベル、パーソナルデジタルアシスタント（PDA））、自動販売機、または同様のものであってよく、これらのディスプレイデバイスを利用してサーバ（すなわちサービス提供者）上で実行する取引を完了させる。ディスプレイデバイスは任意選択により、携帯型であってよい。ディスプレイデバイスは手持ち型であってよい。

【００６１】

[0069] ユーザデバイス２０３は、物理トークン２０７の画像データをキャプチャするために使用される画像デバイス２００を備えることができる。画像デバイスは、図１で説明されたものと同じ画像デバイスであってよい。画像データは、本明細書の他の場所で説明されたように、静止画像データ（例えば写真）または動画像データ（例えばビデオ）であってよい。いくつかの実施形態において、キャプチャされた写真は、ユーザデバイスのディスプレイ２０２上に示されてよい。いくつかの実施形態において、ユーザは、バーコードの写真をキャプチャしなくても、リアルタイムにディスプレイ２０２上のバーコードを可視化できるようにされてよい。いくつかのケースにおいて、ディスプレイは、有効な画像がキャプチャされるかどうかをユーザに通告することができる。不十分な品質の画像は、デコードおよび認証のために使用されることに対して無効化されてよい。ライトニング、フォーカス、安定化、および同様のものなどのファクタは、画像の品質に影響を及ぼす

ことがある。いくつかの実施形態において、ディスプレイは、物理トークンが所定の時間内にデコードされることができない場合に、読取失敗を示すメッセージを提供することができる。いくつかの実施形態において、ユーザは、バーコード領域全体をキャプチャするために、対象物とユーザデバイスの間の距離、方向、または角度を調節するように促されてよい。

【００６２】

[0070] 他の実施形態において、物理トークン全体が認証のために必要とされてよい。他の実施形態において、バーコード領域の一部が、認証するのに十分なことがある。例えば、物理トークンの１０％、２０％、３０％、４０％、５０％、６０％、７０％、８０％、９０％が、ノンスデータの認証および生成のために画像データの中でキャプチャされてよい。

【００６３】

[0071] いくつかの実施形態において、バーコード２０７の写真は、さらなる画像処理およびデコードのためにユーザデバイス２０３のメモリユニット上で入手および格納されてよい。一方、画像デバイス２００は、バーコードの写真をキャプチャしなくても、リアルタイムにバーコードをスキャンすることができる。本実施形態において、画像デバイス２００は、バーコード２０７の画像を絶えず入手し、これらの画像をメモリに格納することができる。これらの画像のそれぞれはその後、バーコードが正しくデコードされるまで処理される。バーコード２０７がデコードされると、画像デバイス２００は、バーコードの画像の入手を停止することができる。

【００６４】

[0072] いくつかのケースにおいて、キャプチャ画像データは、認証のための識別情報を抽出するために処理されてよい。図２に示されるような物理トークン２０７は、識別情報をエンコードする白黒モジュールを含む関心のある領域であってよい。バーコード領域は、長方形、正方形、三角形、円形、楕円形、および同様のものなどの任意の形状であってよい。関心のあるバーコード領域は、境界を有しても、有さなくてもよい。例えば、関心のある領域は、ＰＤＦ４１７コードを収める長方形領域であってよく、ＰＤＦ４１７コードは、名前、住所、生年月日、および同様のものなどのユーザの識別情報をエンコードすることができる。代替ケースにおいて、識別情報は、キャプチャ画像データによって提供されなくてもよい。例えば、識別情報は、ユーザデバイスまたは認証アプリケーションと関連付けられたデバイスＩＤまたはユーザＩＤであってよい。

【００６５】

[0073] いくつかの実施形態において、エンコードされた識別情報は前もって暗号化されてよく、暗号文を解読するために暗号化鍵が必要とされることがある。例えば、運転免許証上のＰＤＦ４１７コードは標準的なリーダによってデコードされることが可能だが、デコードされた識別情報は発行者によって前もって暗号化されてよく、その結果、識別データを解読するために、暗号化鍵および暗号化アルゴリズムが必要とされることがある。いくつかのケースにおいて、権限エンティティまたは特定のサービス提供者だけが暗号化鍵および方法を保有することができる。他の実施形態において、ユーザデバイスが暗号化鍵および方法を保有することができる。鍵および方法は、標準的なものでよい。例えば、データは、１０２４ビットの多形暗号法、またはエクスポート制御に応じて、ＡＥＳ２５６ビット暗号化方法を使用して暗号化されてよい。さらに暗号化は、リモート鍵（シード）またはローカル鍵（シード）を使用して行われてよい。例えば、ＳＨＡ２５６、ＡＥＳ、Ｂｌｏｗｆｉｓｈ、ＲＳＡ、および同様のものといった、当業者によって理解されるような代替の暗号化方法が使用されてもよい。

【００６６】

[0074] いくつかの実施形態において、物理トークンは、識別データを取得するために処理され、デコードされてよい。画像を、ぼやけた、ノイズが入った、ひずんだ、拡大縮小された、ゆがんだ、等の状態にすることがある何らかの方向、大きさ、ライティング条件、および同様のものでキャプチャされた画像から、物理トークンは読み取られることがあ

る。物理トークンを収める画像データの様々な特性が、画像処理の処理中に分析されてよい。キャプチャ画像データおよび画像デバイスの特性は、ノンスデータを生成するために使用されてよい。

【００６７】

[0075] 図３は、本発明の実施形態による、ノンスデータとして使用され得る、画像キャプチャおよび画像処理中に生成されるデータの例を示す。いくつかの実施形態において、データは、画像デバイスの状態についてのものであってよい。パートＡは、画像キャプチャ中に収集されることが可能な画像デバイスに関するローカルデータの例を示す。画像デバイスに関するローカルデータは、画像デバイス、または画像センサ、光学的要素、等などの画像デバイスの構成要素の状態を指してよい。画像デバイスのローカルデータは、デバイスの方向、地理位置情報、および同様のものなどの位置情報を含むことができる。画像デバイスのローカルデータは、画像がキャプチャされる時間、画像が修正される時間、等などのタイムスタンプを含むことができる。画像デバイスのローカルデータは、焦点距離、ＩＳＯ、フレームレート、シャッタースピード、等などのイベントベースの動作パラメータを含むことができる。いくつかの実施形態において、ローカルデータは、本明細書の他の場所で説明されたような、ＧＰＳ、ＩＭＵ、加速度計、および気圧計などの、ユーザデバイスの１つまたは複数のセンサから収集されてよい。

【００６８】

[0076] いくつかの実施形態において、画像デバイスに関するローカルデータは、画像のメタデータから取得されてよい。メタデータは、写真に自動的に付随したデータであってよい。メタデータは、露出設定、キャプチャ時間、ＧＰＳ位置情報、およびカメラのモデル、等など、画像および画像のキャプチャ方法に関する技術情報を含む可変データを収めることができる。いくつかの実施形態において、メタデータは、画像デバイスに搭載されたマイクロプロセッサによって生成される。

【００６９】

[0077] 画像デバイスのローカルデータは、動作パラメータを含むことができる。いくつかの実施形態において、動作パラメータは、イベントベースのパラメータであってよい。例えば、露出時間は、局所照明光の条件に基づいて変わることがある。画像デバイスの焦点距離は、物理トークンと画像デバイスの間の距離に基づいて自動的に変わることがある。ＩＳＯ感度、シャッタースピード、絞りの開口径は、変わりやすい環境および映し出された物体に対応するように所定のアルゴリズムに従って自動的に調節されることがある。

【００７０】

[0078] 画像デバイスに関する動作パラメータの収集を支援できる、画像デバイスに搭載された１つまたは複数のプロセッサが提供されてよい。例えば、画像デバイスは、物理トークンをキャプチャする第１の時間における動作パラメータの第１のセットを有することができ、同じ物理トークンをキャプチャする第２の時間における動作パラメータの異なるセットを有することができる。前述のように、動作パラメータは、非常に変わりやすい環境に対応するように所定のアルゴリズムに従って自動的に調節されてよい。

【００７１】

[0079] 画像デバイスのローカルデータは位置情報を含むことができる。いくつかの実施形態において、位置情報は、デバイスの緯度、経度、および／または高度を含むことができる。いくつかの実施形態において、位置情報は座標として表現されてよい。位置情報は、デバイスの方向を含むことができる。例えば、位置情報は、１軸、２軸、または３軸（例えば、ヨー軸、ピッチ軸、および／またはロール軸）に対するデバイスの方向を含むことができる。位置情報は、デバイスの姿勢であってよい。位置情報は、慣性基準系（例えば、環境、地球、重力）、および／または局所基準系に関連して判断されてよい。

【００７２】

[0080] 画像デバイスに関する位置情報の収集を支援できる１つまたは複数のセンサが提供されてよい。例えば、デバイスは時間と共に様々な方向に向いてよい。例えば、静的な基準系に対して、デバイスは異なる方向を向いてよい。軸間の角度は時間と共に変化して

よい。上述のように、位置情報（例えば、角度情報、空間的位置情報）は、高い正確さおよび／または精密さで判断されてよい。デバイスの方向は、ただ１つの軸、２つの軸、または３つの軸にわたって評価されてよい。デバイスの空間的位置は、ただ１つの軸、２つの軸、または３つの軸に沿って評価されてよい。

【００７３】

[0081] 画像デバイスのローカルデータは、画像がキャプチャされる時間、画像デバイスに搭載されたプロセッサによって画像が事前処理される時間、画像が格納および／または出力される時間などのタイムスタンプを含むこともできる。

【００７４】

[0082] 認証イベントは様々な時点で発生することがある。ユーザは様々な時点で認証を行い、および／または取引に参加することができる。同じユーザによって同じ物理トークンをキャプチャするために同じ画像デバイスが使用されることがあるという可能性はあるが、これらが、画像デバイスの完全に同一のローカルデータ（例えば、動作パラメータ、位置、姿勢、および／またはタイムスタンプ）を有するという可能性は非常に低い。認証イベント間でローカルデータの少なくともいくつかの小さな変化が予想されることがある。したがって、異なる認証イベントで得られた画像デバイスのローカルデータが完全に同一な場合、リプレイアタックが発生している可能性があり得る。例えば、詐欺師は、画像デバイスのローカルデータを含めて、認証イベント（例えば、以前の取引、ユーザ認証、アカウントアクセス）を以前に記録した可能性があり、以前の認証イベントをリプレイしている。１つの例において、第１の認証イベント中に、画像デバイスのローカルデータは、パートＡに示すように読み取られてよい。第２の認証イベント中に、デバイスのローカルデータが、正確に同じになるように読み取られる場合、これは非常に奇妙であり、リプレイアタックを示す可能性がある。特に、デバイスがモバイルデバイスまたは携帯用デバイスであるとき、画像デバイス情報は変化する可能性がある。認証イベント中にデバイスが、ある面の上に載っていても、デバイスとのユーザの相互作用が、（例えば、フォーカス距離（focus distance）、視線などの）いくつかの画像の条件を変化させることがある。ユーザがデバイスに直接触らなくても、光源などの環境条件が、（例えば、ＩＳＯ感度、絞りの開口径、シャッタースピード、露出時間といった）いくつかのパラメータを変化させることがある。

【００７５】

[0083] パートＢは、ノンスデータとして画像処理から収集され、使用されることが可能なデータの例を示す。収集されるデータは、画像データの状態に関するものであってよい。収集されるデータは、画像データの様々な特性に関するものであってよい。いくつかの実施形態において、キャプチャ画像データ３０１は、関心のある領域３０３を含むことができる。関心のある領域は、アイデンティティ情報をエンコードするパターンを含むバーコード領域であってよい。関心のある領域は、図２で説明されたものと同じであってよい。いくつかの実施形態において、画像データは、エンティティ情報をデコードするために処理されてよい。例えば、キャプチャ画像データは変形またはゆがんでいることがあり、バーコードをデコードするために、キャプチャ画像データは、回転させられること、ひずみを除去されること、バイナリ画像にコンバートされること、トリミングされること、ノイズを除去されること、リサイズされること、見当を合わされること、および同様のものなど、正規化される必要があることがある。様々な動作が、キャプチャされた様々な画像に対して異なる可能性のある特性データを生成することができる。

【００７６】

[0084] 例えば、パートＢに示されるように、スキャン領域３０２に対して回転されたバーコード領域３０３がキャプチャされてよい。画像座標３０５とバーコード座標３０７の間の角度（すなわち、画像フレームに対するバーコードの方向）は、ユーザが画像を撮るたびに変わることがある。例えば、第１の認証イベントでキャプチャされた画像データ３０１がシナリオＢ－１に示され、バーコード領域の左上隅の座標が［ｘ，ｙ］３０９として検出されてよい。第２の認証イベントにおいて、同じグラフィカルコードがキャプチャ

されてよく、画像データ３１１はシナリオＢ－２のように示されてよい。同じグラフィカルコードの左上隅の座標は、第１の認証イベントの座標とは異なる［ｘ’，ｙ’］３１３であってよい。

【００７７】

[0085] 画像データの様々な特性またはプロパティ（例えば、バーコード領域のひずみ、回転／配向角度、幅、高さ）は、認証イベント間で異なることがある。例えば、画像デバイスと対象物との間の距離は、固定サイズの画像センサ上でバーコードが有することができる可能な大きさの広い範囲（倍率）に変換されてよい。別の例において、ある角度でバーコードの画像を撮ることが、見る人にとってのバーコードの見かけの形状を変える（ひずみ）。まっすぐに見られると長方形の形状になるバーコードＢ－１は、ある角度から閲覧されると台形（または不等辺四辺形）Ｂ－２のように見えることがある。側面から、または傾けて見られると、バーコードの画像ピクセルの位置およびアドレスは劇的に変化する。

【００７８】

[0086] キャプチャ画像データは、認証情報をデコードするために処理されてよい。いくつかの実施形態において、画像処理中に生成されたデータはノンスデータとして使用されてよい。ノンスデータは、画像処理から取得されたキャプチャ画像データの様々な特性から生成されてよい。検出されたバーコード領域の隅の座標、キャプチャ画像の重心の位置、関心のあるパターンの大きさ、ひずみ、これらの方向などのキャプチャ画像データの様々な特性は、追加の計算／動作を行わなくても、画像処理中に生成されることが可能である。例えば、分析のためにバーコード領域を整合させるように画像データが処理されると、角度が計算され、記録されることが可能である。画像座標に対するバーコード領域の隅の座標（ｘ，ｙ）３０９が、パターン認識のために検出されてもよい。バーコード領域の高さ、幅、およびヒストグラムなどの他の特性が画像処理中に分析されてもよく、ノンスデータとして使用されてよい。

【００７９】

[0087] 他の例において、特性データは事前処理から生成されてよい。例えば、画像データは、ホワイトバランスについて自動的に補正されてよい。一定の色を正しく描画するために、構成要素ＲＧＢカラーの濃度が調節されてよい。したがって、処理中に濃度が分析され、ノンスデータとして使用されてよい。

【００８０】

[0088] さらに、特性データは、デコード処理から生成されてよい。例えば、バーコードのキャプチャ画像データの明るさおよびコントラストの変化に対応するためのアルゴリズムおよび方法が行われてよい。これは、全体的および局所的に適応できる画像処理動作（例えば、閾値化、フィルタリング、等）を使用して行われてよい。別の例において、バーコードパターンを認識するために、パターン認識技法が行われてよい。この処理中に、画像座標に対するパターンの一部に関する特性が、ノンスデータとして収集され、使用されてよい。例えば、座標、または非正規化画像で認識された第１のバーのパターンの大きさは、ノンスデータとして記録され、使用されてよい。

【００８１】

[0089] 画像処理中に生成された、または未加工の画像に関する、様々な特性データは、ノンスデータとして使用されてよい。このデータは、物理トークンがキャプチャされるたびに収集され、アイデンティティ情報をデコードするために処理されてよい。いくつかの実施形態において、データは画像処理動作を行わずに収集されてよい。データは、画像データを交互に入れ替えずに、本明細書の他の場所で説明されるような任意の分析によって生成されてよい。物理トークンは認証イベントのためにキャプチャされ得るので、物理トークンの画像データの処理から生成されるデータは自動的に収集され、ノンスデータとして使用されてよい。

【００８２】

[0090] 画像デバイスの状態およびキャプチャされた画像データの状態に関するデータは

、認証イベントのためにノンスデータとして使用されてよい。認証イベントは、様々な時点で発生することがある。ユーザは様々な時点で認証を行い、および／または取引に参加することができる。同じユーザによって同じ物理トークンをキャプチャするために同じ画像デバイスが使用されることがあるという可能性はあるが、これらが、画像処理から生成された画像および／またはデータに関する完全に同一のデータ（例えば、スキュー角、回転角度、ヒストグラム、濃度、等）を有するという可能性は非常に低い。認証イベント間でデータの少なくともいくつかの小さな変化が予想されることがある。したがって、画像処理からのデータ、または様々な認証イベントで得られた未加工の画像のデータが完全に同一である場合、リプレイアタックが発生している可能性があり得る。例えば、詐欺師は、画像の状態のデータを含めて、認証イベント（例えば、以前の取引、ユーザ認証、アカウントアクセス）を以前に記録した可能性があり、以前の認証イベントをリプレイしている。特に、デバイスが、モバイルデバイスまたは携帯用デバイスであるとき、画像データ情報は変化する可能性がある。

【００８３】

[0091] 認証イベント中にデバイスが、ある面の上に載っていても、画像デバイスとのユーザの相互作用が、フォーカス距離、視野角、安定性、および同様のものなどのいくつかの画像条件を変更させることがある。例えば、画像デバイスと対象物との間の距離は、固定サイズの画像センサ上でバーコードが有することができる可能な大きさの広い範囲（倍率）に変換されてよい。別の例において、ある角度でバーコードの画像を撮ることが、見る人にとってのバーコードの見かけの形状を変える（ひずみ）。

【００８４】

[0092] ユーザがデバイスに直接触らなくても、光源などの環境条件が、（例えば、ノイズ、濃度、ホワイトバランス、等といった）いくつかの変数を変化させることがある。例えば、画像デバイスは、画像データのキャプチャ中に光源のための環境光に単に依存することがある。非常に変わりやすい環境光が、様々な画像デバイスのパラメータを自動調節させることがある。非常に変わりやすい環境光が、影、バーコード長さにわたって陰にすること、露出過度、露出不足、およびキャプチャ画像データの類似の特性の変化を生じることもある。

【００８５】

[0093] したがって、ユーザ認証処理または取引などの認証イベントは、改ざんまたは詐欺行為の見込みに関して評価されてよい。詐欺行為の見込みが増えたことを画像デバイスおよび画像データの情報がもたらさないときに、ユーザのアイデンティティが確認されてよく、および／または取引が認証されてよい。

【００８６】

[0094] 図４は、本発明の実施形態による、どのようにしてノンスデータが生成または格納され得るかについての例を示す。ノンスデータについての本明細書におけるいずれかの説明が、任意のタイプの特異値に適用することができる。繰り返し現れる可能性が低い可能性がある、ノンスデータについてのいずれかの説明が、様々なデバイス計測、インデックス、またはパラメータに適用することができる。繰り返し現れる可能性が低い可能性がある、ノンスファクタについてのいずれかの説明が、様々なデバイス計測、インデックス、またはパラメータに適用することができる。ノンスデータは、１つもしくは複数のノンスファクタを含むことができ、またはこれらから導出されてもよい。

【００８７】

[0095] １つまたは複数のノンスファクタ（例えば、ノンスファクタ１　４０３、ノンスファクタ２　４０５、ノンスファクタ３　４０７、…）が、ノンスデータのセット４０１を形成するために使用されてよい。ノンスファクタは、画像デバイスの状態および／またはキャプチャ画像データの状態について収集された様々なタイプのデータを含むことができる。ノンスファクタは、画像デバイスおよびキャプチャ画像データの様々な特性に関連した様々なタイプのデータを含むことができる。ノンスファクタは、ユーザデバイスの様々なセンサからのデータを含むことができる。ノンスファクタは、ユーザデバイスの状態

について収集された様々なタイプのデータを含むことができる。ノンスファクタはそれぞれ、ただ１つの時点、複数の時点、または時間間隔にわたって得られてよい。ノンスファクタのそれぞれは、様々な時点からのものでもよく、または一致および／もしくは重複する時間からのものでもよい。ノンスファクタのそれぞれは、デバイスの様々なセンサまたは様々なタイプのセンサから収集されたデータを含むことができる。一方、ノンスファクタの２つ以上が、同じセンサまたは同じタイプのセンサから収集されてよい。いくつかの例において、ノンスファクタのすべてが、同じセンサまたは同じタイプのセンサから収集されてよい。

【００８８】

[0096] １つの例において、ノンスデータ４０１は、単一のノンスファクタから導出されることが可能である。いくつかの実施形態において、単一のノンスファクタは、特性のグループに関連した情報であってよい。例えば、単一のノンスファクタは、画像フレームに対するバーコード領域に関連して処理されたデータであってよい。この場合、単一のノンスファクタは、バーコード領域の隅の座標、回転角度、重心、幅および高さ、ならびに同様のものなどのバーコード領域に関する特性のグループを含むことができる。別の例において、単一のノンスファクタは、画像デバイスの未加工の位置データであってよく、したがって単一のノンスファクタは、姿勢、緯度、および同様のものなどの特性のグループを含むことができる。別の例において、単一のノンスファクタは、ＩＳＯ感度、露出時間、または本明細書の他の場所で説明されるような他の任意のタイプのデータなどの画像センサの動作パラメータに関連した情報であってよい。単一のノンスファクタは、任意の数の特性データを含むことができる。ノンスデータは、センサから直接的に読み取られた未加工のデータであってよく、または未加工のデータに基づいて導出もしくは処理されてもよい。特性のグループに関する情報が認証イベント間で同一の場合、ノンスデータも認証イベント間で同一であってよい。

【００８９】

[0097] シナリオＡに示されるように、ノンスデータは複数のノンスファクタから導出されてよい。例えば、第１のノンスファクタは画像デバイスデータを含むことができ、第２のノンスファクタは画像特性データを含むことができる。画像デバイスデータと画像特性データが認証イベント間で同一の場合、ノンスデータも認証イベント間で同一であってよい。画像デバイスデータと画像特性データの両方が認証イベント間で異なる場合、ノンスデータは認証イベント間で異なってよい。画像デバイスデータと画像特性データのうちの少なくとも１つが認証イベント間で異なる場合、ノンスデータは認証イベント間で異なる可能性があってよい。

【００９０】

[0098] 複数のノンスファクタのうちの少なくとも１つのノンスファクタが認証イベント間で異なる場合、ノンスデータはこの相違を反映することができ、認証イベント間で異なってよい。いくつかの例において、ただ１つのノンスファクタでさえ、認証イベント間で異なる場合、ノンスデータは認証イベント間で異なることがある。例えば、ノンスファクタのそれぞれは、認証イベント間で１００％マッチするように、ノンスデータに対して１００％マッチする必要があることがある。これは、ノンスデータが複数のノンスファクタから導出されるときに、特にだいたい真実であることがある。例えば、ノンスデータは、ノンスファクタを考慮するアルゴリズムに基づいて生成されてよい。ノンスデータは、様々なノンスファクタのハッシュであってよい。ノンスデータは、様々なノンスファクタに基づいて導出され得る値または文字列を含むことができる。いくつかの例において、ノンスファクタのそれぞれに関する情報を区別することが、ノンスデータから判断されることはない。例えば、別々のノンスファクタがノンスデータから導出可能であることも、分離されることもない。一方、ノンスファクタのそれぞれに関する情報を区別することが、ノンスデータから判断されてよい。例えば、別々のノンスファクタがノンスデータから導出可能であることも、分離されることもない。

【００９１】

[0099] シナリオＢに示されるように、ノンスデータ４１１は、複数のノンスファクタの集合体を含むことができる。例えば、第１のノンスファクタは画像デバイスデータを含むことができ、第２のノンスファクタは画像特性データを含むことができる。画像デバイスデータと画像特性データが認証イベント間で同一の場合、ノンスデータも認証イベント間で同一であってよい。画像デバイスデータと画像特性データの両方が認証イベント間で異なる場合、ノンスデータは認証イベント間で異なってよい。画像デバイスデータと画像特性データのうちの少なくとも１つが認証イベント間で異なる場合、ノンスデータが認証イベント間で異なる可能性があってよい。しかし、ノンスファクタのどのセットが認証イベント間で異なるか、およびどれが異なるかを区別することが可能なことがある。

【００９２】

[0100] 複数のノンスファクタのうちの少なくとも１つのノンスファクタが認証イベント間で異なる場合、ノンスデータはこの相違を反映することができ、認証イベント間で異なってよい。いくつかの例において、ただ１つのノンスファクタでさえ、認証イベント間で異なる場合、ノンスデータは認証イベント間で異なることがある。例えば、ノンスファクタのそれぞれは、認証イベント間で１００％マッチするように、ノンスデータに対して１００％マッチする必要があることがある。しかし、ノンスファクタのそれぞれは区別できる可能性があるので、どのノンスファクタがマッチし、どのノンスファクタがマッチしないかが判断されることが可能である。例えば、ノンスデータは単に、様々なノンスファクタの集合体であってよく、または互いに様々なノンスファクタを付け加えてもよい。いくつかの例において、ノンスファクタのそれぞれに関する情報を区別することは、ノンスデータから判断されてよい。例えば、別々のノンスファクタがノンスデータから導出可能であってもよく、または分離されてもよい。一方、ノンスファクタのそれぞれに関する情報を区別することは、ノンスデータから判断されてよい。例えば、別々のノンスファクタがノンスデータから導出可能であることも、分離されることもない。

【００９３】

[0101] 様々なノンスファクタを個別に区別可能にできることは、都合のよいことに、リプレイアタックが発生しているかどうかについての判断に、より大きい粒度を入れることを可能にすることができる。例えば、様々なノンスファクタが様々に重みを加えられてよい。例えば、認証イベント間で異なる可能性が高いノンスファクタは、認証イベント間で異なる可能性が低いことがあるノンスファクタより多く重みを加えられてよい。１つの例において、バーコード領域の方向および座標のデータが認証イベント間で同一であり得る可能性は極めて低いことがある。しかし、画像デバイスの状態（例えば、露出時間、ＩＳＯ感度、等）にいくつかの変化があり得る可能性があるが、これは、繰返しの可能性が高くなり得るファクタであることがある。このようなイベントにおいて、バーコード領域の方向および座標のデータは、さらに重みを加えられてよい。重み付けは、リプレイアタックの評価中に考慮されてよい。

【００９４】

[0102] 個別のファクタに目を向けることは、記録および／またはリプレイされる可能性があるデータの一定の部分だけが存在し得るときに有効なこともある。例えば、いくつかの実施形態において、リプレイアタック中、物理トークンに関係があるすべてのデータが記録され、リプレイされることがある。このようなシナリオにおいて、ファクタのいずれかにおける何らかのずれが、リプレイアタックが発生したという見込みを減らすことがある。他の実施形態において、リプレイアタック中、物理トークンに関係がある選択データだけが記録され、リプレイされることがある。例えば、画像特性データだけが記録され、リプレイされることがあるが、画像デバイスの状態に関するデータはリプレイされない。１つのシナリオなどにおいて、ファクタのうちの１つ（例えば、バーコード領域の方向、ひずみ）の１００％マッチが、リプレイアタックの発生の見込みをもたらすのに十分なことがある。いくつかの実施形態において、本明細書で提供されるシステムおよび方法は、ノンスデータが収集および／または考慮される方法を考慮することができる。何らかのリプレイが自動的にノンスファクタすべてをまとめる方式でノンスデータが収集される場合

、ノンスデータにおける何らかのずれが、リプレイアタックの可能性が低いことを示すのに十分なことがある。別々のノンスファクタが分離され、および／または個別に提供され得る方式でノンスデータが収集される場合、特に、繰り返し現れる可能性の低いノンスファクタといったノンスファクタの１００％マッチが、リプレイアタックの高い見込みをもたらすのに十分なことがある。

【００９５】

[0103] リプレイアタックが発生したかどうかの判断において、（例えば、シナリオＢに示すような）様々な個別のノンスファクタが考慮されてよい。一方、（例えば、シナリオＡに示すような）全体的なノンスデータだけが考慮されてよく、何らかの程度の相違が、リプレイアタックの見込みを減らすことがある。いくつかの例において、相違の程度は、リプレイアタックの見込みを判断する際に考慮されてよい。例えば、すべてのノンスファクタが同一である場合、リプレイアタックの見込みが高い可能性がある。単一のノンスファクタが同一であり、繰返しの可能性があり得るものである場合、リプレイアタックの見込みがあまり高くないことがもたらされることがあり、ノンスファクタが同一でない場合、リプレイアタックの見込みが低いことがもたらされることがある。

【００９６】

[0104] 図５は、本発明の実施形態による、様々な取引に対して、どのようにしてデータが格納され得るかについての例を示す。データは、本発明の１つの実施形態による、ユーザおよび／または詐欺的取引を識別するために使用されてよい。取引は、本明細書の他の場所で前述されたように発生してよい。

【００９７】

[0105] データは、１つまたは複数の取引などの、１つまたは複数の認証イベントから収集された履歴データであってよい。履歴データは、単一のメモリユニットに一緒にすべて格納されてよく、または複数のメモリユニットにわたって分散されてもよい。複数のメモリユニットにわたって分散されたデータは同時にアクセス可能か、もしくはリンクされてよく、またはそうでなくてもよい。履歴データは単一のユーザのデータ、または複数のユーザからのデータを含むことができる。複数のユーザからのデータは一緒にすべて格納されてよく、または互いに別々に格納されてもよい。履歴データは、単一のユーザデバイスから収集されたデータ、または複数のユーザデバイスから収集データを含むことができる。複数のユーザデバイスからのデータは一緒にすべて格納されてよく、または互いに別々に格納されてもよい。いくつかの例において、ただ１つユーザデバイスが、ただ１人のユーザに提供されてよい。一方、認証イベントを行うときに、複数のユーザがただ１つのユーザデバイスを使用してよく、または１人のユーザが複数のユーザデバイスを使用してもよい。

【００９８】

[0106] 格納データは、取引ＩＤ５０１などの情報、および／または取引関連データを含むことができる。取引に言及する本明細書における任意の議論は、任意のタイプの認証イベントを指してよい。例えば、取引に関する本明細書における任意の議論は、ユーザの任意の認証、および／またはユーザアカウントへのアクセスに適用することもできる。

【００９９】

[0107] 取引ＩＤ５０１は、特定の取引、例えば、ＴＩＤ１、ＴＩＤ２、ＴＩＤ３、ＴＩＤ４、等を識別する一意の識別子であってよい。前述のように、ユーザまたはユーザデバイスが認証イベントを行うときはいつでも取引があってよい。履歴データの中で行われたような取引は、問題が伝えられるかどうか、および／または金銭、商品、もしくはサービスのいずれかの移送が完了に向けて前進するのを可能にされるかどうかに関わらず格納されてよい。

【０１００】

[0108] 例えば、ＩＤ１、ＩＤ２、等といった、任意のタイプの識別関連データ５０３が格納されてよい。識別関連データ５０３は、取引を行っているとされるユーザ、ユーザのデバイスに関する情報、または取引自体に固有の任意の情報に関係してよい。識別関連デ

ータは、認証データを含むことができる。例えば、ユーザ名、パスワードもしくはフレーズ、暗号化された鍵、バイオメトリクスデータ（例えば、指紋、光学式スキャン、手形、声紋）、またはユーザを認証するために使用される他の任意のタイプの情報が提供されてよい。

【０１０１】

[0109] 識別データ５０３は、ユーザの名前、ユーザに一意の識別子、またはユーザに関する任意の個人情報（例えば、ユーザの住所、ｅメール、電話番号、生年月日、出生地、ウェブサイト、社会保障番号、口座番号、性別、人種、宗教、教育情報、健康関連情報、雇用情報、家庭情報、配偶者の有無、扶養家族、またはユーザに関連した他の任意の情報）を含むことができる。ユーザに関する個人情報は、ユーザに関する財務情報を含むことができる。例えば、ユーザに関する財務情報は、ユーザのペイメントカード情報（例えば、クレジットカード、デビットカード、ギフトカード、割引カード、プリペイドカード、等）、ユーザの金融口座情報、銀行支店コード、残高、負債額、信用限度額、過去の金融取引、または他の任意のタイプの情報を含むことができる。

【０１０２】

[0110] 識別データ５０３は物理トークンに関係してよい。例えば、ＩＤカード上のバーコードなどの一意の物理トークンが提供されてよい。バーコードにエンコードされた識別情報が提供されてよい。

【０１０３】

[0111] 識別データ５０３はユーザのデバイスに関係してよい。例えば、一意のデバイス識別子が提供されてよい。デバイスの識別特徴データ（例えば、デバイスの１つまたは複数の特性に関する情報）が提供されてよい。デバイスの時計、デバイスのＩＰアドレス、デバイス上で動くアプリケーションに関して収集される情報、またはデバイスに関する他の任意の情報が収集されてよい。

【０１０４】

[0112] 取引固有の情報が組み込まれてよい。例えば、取引の性質、取引を伴うエンティティ、取引の時間、取引に対する商品もしくはサービスの任意の財務もしくはやりとりの量、取引に関わる口座番号、または取引に関係がある他の任意の情報が提供されてよい。

【０１０５】

[0113] いくつかの実施形態において、識別データ５０３は物理トークンによって提供されてよい。物理トークンは、図２で説明されたものと同じトークンであってよい。識別データは、ユーザデバイスを使用して物理トークンをスキャンすることによって取得されてよく、スキャン画像データは、識別データをデコードするために処理されてよい。デコードされた識別データは、以前に暗号化されたデータであってよく、またはそうでなくてもよい。いくつかの実施形態において、データベースに格納された識別データは、暗号化された暗号文である。任意選択により、データベースに格納された識別データは、平文データである。

【０１０６】

[0114] 識別データが取得されるときに、ノンスデータが自動的に収集されてよい。物理トークンの画像がキャプチャされるときに、ノンスデータが収集されてよい。物理トークンの画像が処理または分析されるときに、ノンスデータが収集されてよい。

【０１０７】

[0115] いくつかの実施形態において、ノンスデータ５０５は、追加センサまたは追加動作を要することなく収集されてよい。例えば、画像デバイスの状態の情報に関するノンスデータは、追加動作または何らかの動作がなくても、キャプチャされた静的トークンのメタデータから収集されてよい。別の例において、画像データの状態に関するノンスデータは、任意の追加の計算または分析がなくても、画像処理中に収集されてよい。

【０１０８】

[0116] 認証イベントが発生するときに、ノンスデータ５０５が収集されてよい。ノンスデータは、画像デバイスの状態、キャプチャされた静的トークンの状態、および／または

ユーザデバイスに関する情報を含むことができる。ノンスデータは、その後の認証イベントで繰り返し現れる可能性が極めて低いデータであってよい。ノンスデータは、ただ１つの時点に収集されたデータからの、または複数の時点で（例えば、様々な時間間隔で、もしくは時間範囲内で継続的に）収集されたデータからのデータを含んでよく、またはこれのデータから導出されてもよい。ノンスデータは、データの単一のセットまたは複数のセットとして格納されてよい。ノンスデータは、ＮＤ１、ＮＤ２、ＮＤ３、等と表されてよい。

【０１０９】

[0117] 履歴データは、デバイスおよび／もしくはユーザを識別するか、またはユーザを認証するために分析されてよい。図示のように、最初の２つの取引が何らかの注意を促すことはない。例えば、ＴＩＤ１、ＴＩＤ２に関して、識別データＩＤ１およびＩＤ２は、これらが異なる取引に対するものであるので異なってよく、ノンスデータＮＤ１およびＮＤ２も、データの両方のセットが変化しているので異なってもよい。

【０１１０】

[0118] 第３のシナリオＴＩＤ３において、注意が促される。別々の取引が発生しているが、同じ識別データＩＤ１は、これがＴＩＤ１と同じアイデンティティ（例えばユーザ）であると思われるということを示すことができる。ノンスデータＮＤ３は、ＴＩＤ１とＴＩＤ３の間でいくつかの情報が異なることを示すことができるので、これが同じ取引である可能性は低い。これは、同じユーザが異なる取引を行うことを示すことができる。ＴＩＤ１とＴＩＤ３の間で識別情報ＩＤ１が同一である事実は矛盾している可能性があり、詐欺行為の見込みを増大させる可能性がある。

【０１１１】

[0119] 第４のシナリオは、注意を促す可能性を示す。例えば、ＴＩＤ４は別々の取引として示されるが、同じ識別データＩＤ２および第２の取引ＴＩＤ２を有する。ノンスデータＮＤ２も、ＴＩＤ２とＴＩＤ４の間で同じとして示されてよい。ノンスデータは繰り返し現れる可能性が極めて低い可能性があり、または繰り返し現れることは決してない。ノンスデータの繰返しは、リプレイアタックを示すことができる。したがって、第４の取引ＴＩＤ４に関して、リプレイアタックの見込みが高いことが伝えられる。

【０１１２】

[0120] １つのイベントに類似の動作パラメータのセット（例えば同じ露出時間）を画像デバイスが有する可能性がある場合があるが、前述のように、特に、高レベルの正確さおよび／または精密さで判断される計測値をデータが含むときに、情報が正確にマッチする（例えば、非常に正確な方向および／もしくは空間的位置が正確にマッチするか、または画像フレームに関する静的トークンの非常に正確な座標、方向、ひずみ、大きさが正確にマッチする）可能性は非常に低い。したがって、第４のシナリオには、リプレイアタックの危険が多少ある可能性がある。

【０１１３】

[0121] いくつかのシナリオにおいて、ノンスデータ５０５は、認証イベント中の複数の時点で収集されたノンス情報を含むことができる。１つの例において、画像データをキャプチャした後、静的トークンがデコードされた後、または間のどこかで、ユーザが画像デバイスを始めるときに、ノンス情報が収集されてよい。

【０１１４】

[0122] このようなシナリオは、ほんの一例として提供される。認証イベントは、デバイスおよび／またはユーザを識別することを含むことができる。例えば、識別情報は、ユーザおよび／またはデバイスを識別するために使用されてよい。識別情報は、識別情報の１つまたは複数の以前に格納されたセットと比較されてよい。いくつかの実施形態において、識別情報が識別情報の以前に格納されたセットにマッチするときに、識別情報は、同じユーザおよび／またはデバイスに属すると判断されてよい。

【０１１５】

[0123] 任意選択により、ユーザおよび／またはデバイスを識別するときにノンスデータ

が考慮されてよい。ノンスデータはこれ自体に対して分析されてよく、および／またはノンスデータの１つまたは複数の以前に格納されたセットと比較されてよい。以前に格納されたノンスデータのセットにノンスデータが寸分たがわずマッチする場合、リプレイアタックの危険があることが判断されてよい。これは、ユーザが、自分が称しているユーザではないこと、またはユーザが改ざん情報を提供していることを示唆することができる。

【０１１６】

[0124] 図６は、本発明の実施形態による、どのようにしてノンスデータ６０１および識別データ６０３が、認証パラメータ６００を形成するために使用され得るかを示す。ノンスデータに関する本明細書におけるいずれかの説明は、本明細書で提供されるような認証パラメータに適用することもできる。認証パラメータはリプレイパラメータであってよく、これは、ノンスデータおよび識別データを含むことができる。いくつかの実施形態において、識別データは、ユーザ、物理トークン、デバイス、またはサービスに関係する静的データであってよい。ノンスデータは、取引によって変化する動的データであってよい。したがって本発明の認証パラメータは、取引によって自然に変化することができる。

【０１１７】

[0125] いくつかの実施形態において、認証パラメータ６００は、シナリオＡに示されるような、識別データ６０３およびノンスデータ６０１を含むことができる。識別データおよびノンスデータは、同じ画像のキャプチャ中および分析処理中に収集されてよい。識別データおよびノンスデータは、取引中に同じ静的トークンを使用して収集されてよい。

【０１１８】

[0126] 識別情報／データ６０３は、本明細書の他の場所で説明されるような任意のタイプの情報を含むことができる。例えば、識別情報は、ユーザ、ユーザデバイス、ユーザによって保有される物理トークンに関係してよく、および／または認証イベント（例えば取引）に関係してよい。識別は、ただ１つの情報（例えば一意の識別子）であってよく、または複数ファクタの情報（例えば、本明細書の他の場所で説明されるような他のタイプの情報の任意の組合せ）を含んでもよい。

【０１１９】

[0127] いくつかの実施形態において、識別データ６０３は静的トークンであってよい。静的トークンは、バーコードなどの物理トークンによって提供されてよい。静的トークンは、図２で説明されたものと同じであってよい。識別データは、ユーザデバイスを使用して物理トークンの画像をキャプチャすることによって取得されてよく、情報をデコードするために画像データを処理する。いくつかのケースにおいて、画像の処理およびデコードは、ユーザデバイスによって、搭載された１つまたは複数のプロセッサによって行われてよい。他のケースにおいて、画像の処理およびデコードは、ユーザデバイスの外部の１つまたは複数のプロセッサによって行われてよい。物理トークンを収めるキャプチャ画像データは、デコードおよび／または解読のために外部デバイスに伝送されてよく、本明細書の他の場所で説明されるような外部デバイスは、これ自体の認証または識別評価を行うために情報を分析することができる。この場合、キャプチャ画像データは、他のデバイスに伝送される前に処理（例えば圧縮）されても、されなくてもよい。

【０１２０】

[0128] ノンスデータ６０１によって封印された識別データ６０３は、物理トークンからデコードされたデータであってよい。例えば、識別データは、ユーザデバイスによってキャプチャされたグラフィカルコードの影像からデコードされてよい。キャプチャ画像は、ユーザデバイス上でデコードされても、されなくてもよい。いくつかのケースにおいて、キャプチャ画像は、ユーザデバイス内でデコードされてよい。例えば、運転免許証上のＰＤＦ４１７コードは、ユーザデバイスを使用してスキャンされてよく、ユーザアイデンティティ情報は、ユーザデバイス上で実行されたアプリケーションまたはソフトウェアによってデコードされてよい。

【０１２１】

[0129] デコードされた識別データは、前もって暗号化されてよく、または暗号化されな

くてもよい。ユーザデバイスは、データを解読するための暗号化鍵または方法にアクセスできても、できなくてもよい。いくつかの実施形態において、デコードされたデータは、認証のために使用されるパラメータとしてノンスデータによって直接的に封印されてよい。いくつかの実施形態において、データが前もって暗号化されるときに、このデータは、ユーザデバイスに搭載されたアプリケーションまたはソフトウェアによって解読され、その後ノンスデータによって封印されてよい。他の実施形態において、ユーザデバイスはデータを解読できないので、データは、評価および分析のための暗号化鍵またはパスワードを有する、取引に関わるエンティティなどの外部デバイスに伝送されてよい。ノンスデータで封印された識別データは、画像データ、バイナリ、英数字、ＡＳＣＩＩ、等などの任意のフォーマットおよび任意のデータタイプのものであってよい。

【０１２２】

[0130] いくつかの実施形態において、識別データは、ノンスデータを収集するために使用されるものと同じ画像データによって提供されても、されなくてもよい。例えば、ノンスデータは、画像デバイスが画像データをキャプチャしているときの画像デバイスの状態から収集されてよく、同じ画像データが識別情報を提供することはない。別の例において、ノンスデータは、グラフィカルコードなどの静的トークンを収めるキャプチャ画像データの状態から収集されてよく、静的トークンは識別情報を提供しても、しなくてもよい。異なる例において、ノンスデータは、静的トークンを収めるキャプチャ画像データの状態から収集されてよく、ここで静的トークンは識別情報の少なくとも一部を提供することができる。

【０１２３】

[0131] ノンスデータ６０１は、１つもしくは複数のノンスファクタから導出されたノンスデータ、または個別にアクセス可能なフォーマットの１つもしくは複数のノンスファクタを含むことができるノンスデータなどの任意のタイプのノンスデータであってよい。ノンスデータは、それ自体が封印されても、されなくてもよい。例えば、ノンスデータは、その元のノンスファクタに分裂もしくは分割されるか、または導出可能であっても、なくてもよい。封印されたノンスデータは、元のノンスファクタ、および／またはノンスデータを導出するために使用される未加工のデータにアクセスするのを許可することはない。封印されないノンスデータは、元のノンスファクタおよび／またはノンスデータを導出するために使用される未加工のデータにアクセスできるようにすることがある。

【０１２４】

[0132] ノンスデータ６０１および識別情報６０３は、互いに関連付けられてよい。ノンスデータおよび識別情報は、互いにリンクまたは接続されてよい。ノンスデータおよび識別情報は、認証パラメータを導出するために使用されてよい。ノンスデータが認証イベント間で同一の場合、認証パラメータは、認証イベント間で同一であってよい。いくつかの例において、ノンスデータが同一で、識別情報が同一の場合、認証パラメータは認証イベント間で同一であってよい。ノンスデータが同一で、識別情報が同一でない場合、認証パラメータは任意選択により同一でなくてよい。

【０１２５】

[0133] ノンスデータ６０１は認証イベントに結びつけられてよく、この場合、ユーザとされる人はこの認証イベントに参加した。その後の認証イベントに関して、ノンスデータが異なり、この認証イベントに関する識別情報が異なる場合、これが何らかの注意を促すことはなく、なぜならノンスデータは、異なる認証イベントに対して異なる可能性があるからである。ノンスデータが異なるが、識別情報が同じである場合、これは疑問を提起することがある。例えば、これが、同じ認証イベントを指す同一の情報を指している場合、ノンスデータは同じはずであり、異ならない。別の例において、ノンスデータが同じで、識別情報が異なる場合、これは、リプレイアタックの注意を促し、見込みを提起することがある。例えば、異なる認証イベントが発生している場合、ノンスデータがマッチする可能性は極めて低い。ノンスデータは、認証イベント間で変化するはずのデータを含むように選択される。別の例において、ノンスデータおよび識別情報が同じである場合、これは

、同じ認証イベントに対してデータが何度も記録される場合に発生することがある。一方、同一のノンスデータについての何らかの指示は、識別情報が同じであるとされていても、注意を促すことがあり、またはリプレイアタックの可能性を多少、提供することもある。

【０１２６】

[0134] いくつかの実施形態において、封印された認証パラメータ６００は、個別に区別でき、読み取れるフォーマットのノンスデータおよび識別情報を含むことができる。例えば、ノンスデータは評価され、読み取られてよく、識別情報は評価され、読み取られてよい。封印された認証パラメータは、分離できないフォーマットでノンスデータおよび識別情報を互いに永続的にリンクさせることができる。代替実施形態において、認証パラメータは、ノンスデータおよび識別情報を個別に区別し、または読み取れるようにすることはない。

【０１２７】

[0135] いくつかの実施形態において、ノンスデータ６０１および識別データ６０３は、封印された認証パラメータ６００として暗号化されてよい。ノンスデータおよび識別データは、認証パラメータを生み出すために実装された秘密暗号化アルゴリズムの入力パラメータとして使用されてよい。パラメータを暗号化するために様々な方法が使用されてよい。例えば、暗号化および解読のために対称鍵が使用されてよい。これらの鍵は、一文のまたは一連の意味のないキャラクタから構成されてよく、暗号化は、パラメータ（例えばノンスデータおよび識別データ）を構成するデータの塊（例えば、元のデータ、構造データ、およびリードソロモンデータ）に対してビット単位のＸＯＲ動作を行うことによって行われる。別の例において、ノンスデータおよび識別データは、１０２４ビット多形暗号法、またはエクスポート制御に応じてＡＥＳ２５６ビット暗号化方法を使用して暗号化されてよい。さらに、暗号化は、リモート鍵（シード）またはローカル鍵（シード）を使用して行われてよい。例えば、ＳＨＡ２５６、ＡＥＳ、Ｂｌｏｗｆｉｓｈ、ＲＳＡ、および同様のものといった、当業者によって理解されるような代替の暗号化方法が使用されてよい。いくつかのケースにおいて、ユーザデバイス、および取引に関わる他の認証システムまたはエンティティ上のソフトウェアおよび／アプリケーションは、暗号化鍵および暗号化方法を保有することができる。

【０１２８】

[0136] 識別データとノンスデータの組合せ（封印された認証パラメータ）が、認証のために使用されてよい。識別データは、静的トークンによって提供されてよい。識別データは、ユーザおよび／またはデバイスを識別するために使用されてよい。ノンスデータは、同じ静的トークンをキャプチャおよび分析する処理から収集されてよい。ノンスデータは、詐欺行為の検出のために使用されてよい。ノンスデータはこれ自体に対して分析されてよく、および／またはノンスデータの１つもしくは複数の以前に格納されたセットと比較されてよい。ノンスデータが、ノンスデータの以前に格納されたセットに寸分たがわずマッチする場合、リプレイアタックの危険があることが判断されてよい。これは、ユーザが、自分が称しているユーザではないということ、またはユーザが改ざん情報を提供しているということを示唆することができる。

【０１２９】

[0137] いくつかの実施形態において、認証パラメータ６１１は、図６のシナリオＢに示すような追加情報を含むことができる。追加の取引情報は、ノンスデータおよび識別データを収集するために使用される画像データ以外の様々なソースまたは手段によって提供されてよい。例えば、取引中に、ユーザは認証のために、カードまたは外部デバイス上のグラフィカルコード（例えばＩＤカード上のバーコード）をスキャンするように促されてよい。キャプチャ画像から収集された識別情報６１３およびノンスデータ６１１に加えて、ユーザは、ユーザアカウント名、パスワード、金融取引額、および同様のものなどの他の取引情報を入力することもできる。追加情報は、識別データおよびノンスデータ封印でされ、取引に関わる他のエンティティに伝送されてよい。

【０１３０】
[0138] 別の実施形態において、追加情報は、動的トークン６１５に応じてデータを含むことができる。動的トークンおよび結果データは、ユーザ、デバイス、または取引を認証するために使用されてよく、さらなるセキュリティを認証処理に追加することができる。動的トークンは、認証システム、または取引に関わるエンティティによって提供され、ユーザデバイスで受け取られてよい。様々な取引に対して様々な動的トークンが生成されてよい。動的トークンは、認証システムによって最初に生成され、ユーザデバイスに伝送されてよい。返された動的トークンまたは動的トークンと一意に関連付けられた情報が最初の動的トークンにマッチするときに、ユーザは認証されてよい。

【０１３１】
[0139] いくつかの実施形態において、動的トークンは、画像デバイスの動作パラメータのセットを含む命令であってよい。動作パラメータは、取引中に、画像デバイスのいくつかのパラメータを固定値に設定することができる。例えば、フォーカス長（focus length）、ＩＳＯ感度、フラッシュの使用、および同様のものが、グラフィカルトークンの画像データをキャプチャするためにカメラが使用されるときの固定値に設定されてよい。いくつかのケースにおいて、ユーザは、例えば、物理トークンにカメラのレンズをフォーカスさせるために、物理トークンと画像デバイスの間の距離を調節することによって、画像デバイスの設定を処理する必要があることがある。

【０１３２】
[0140] 動的トークンへの対応としての追加データ６１５が、封印された認証パラメータに含まれてよい。例えば、動的トークンによって影響を受けることがあるフォーカス長、ＩＳＯ感度、絞りの開口時間、シャッタースピード、および同様のものが収集され、確認または認証のために認証システムまたはエンティティに返されてよい。

【０１３３】
[0141] 一方、ノンスデータは、動的トークンを受け取った結果として分析されてよい。動的トークンは、ノンスデータの変化を生じることができる。前述のように、ノンスデータは、画像デバイスの動作パラメータを含むことができる。したがって、ノンスデータに含まれる対応データの評価は、封印された認証パラメータの有効性を確認することができる。

【０１３４】
[0142] 図７は、本発明の実施形態による、識別データおよびノンスデータを使用して、ユーザおよび／またはデバイスを識別する例を示す。ノンスデータと識別データのセットは、ユーザデバイスを使用して収集されてよい７０２。ノンスデータおよび識別データは、履歴上のノンスデータおよび識別データと共に格納されてよい７０４。ノンスデータおよび識別データは、ノンスデータと識別データの１つまたは複数の以前に収集されたセットとそれぞれ比較されてよい７０６。比較に基づいてユーザの識別が評価されてよい７０８。いくつかの実施形態において、取引は、比較に基づいて許可されても、されなくてもよい。任意選択により、リプレイアタックなどの詐欺行為の見込みの指示が提供されてよい。

【０１３５】
[0143] ノンスデータと識別データのセットは、認証イベント中に収集されてよい７０２。識別データは、本明細書の他の場所で説明されるような視覚グラフィカルコードなどの物理トークンによって提供されてよい。物理トークンに関する画像データは、ユーザデバイスによってキャプチャされてよい。１つまたは複数のプロセッサは、キャプチャされた視覚グラフィカルコードをデコードし、識別データを取得するように構成されてよい。いくつかの実施形態において、デコードされた識別データは、デコードされた識別データが、暗号化鍵なしで読み取れるように、または読み取れないように第三者によって前もって暗号化されてよい。識別データは、以前に説明されたような任意のフォーマットおよびデータタイプのものであってよい。識別データは視覚グラフィカルコードに関係してよい。識別データはユーザに関係してよい。識別データはサービスに関係してよい。

【０１３６】
[0144] 本明細書の他の場所で説明されたように、識別データは、取引イベントなどで使用される同じ物理トークン、同じユーザ、同じサービス、または同じ取引に関係した情報を収めることができる。識別データは、ユーザのアイデンティティを認証または確認するために使用される情報を収めることができる。識別データは、ユーザのアイデンティティを表す名前、生年月日、住所、国籍、および同様のものなどの個人情報を収めることができる。識別データは、製品またはサービスのアイデンティティを表す取扱説明、購入オプション、サービス提供者情報、および同様のものなどの製品情報を収めることができる。識別データは、ユーザ、サービス、取引、等を一意に識別できる任意のタイプの情報を収めることができる。

【０１３７】
[0145] 識別データは、ノンスデータを収集するために使用されるものと同じ画像データによって提供されても、されなくてもよい。例えば、ノンスデータは、画像デバイスが画像データをキャプチャしているときの画像デバイスの状態から収集されてよく、ここで、同じ画像データが識別情報を提供することはない。別の例において、ノンスデータは、グラフィカルコードなどの静的トークンを収めるキャプチャ画像データの状態から収集されてよく、静的トークンは識別情報を提供しても、しなくてもよい。異なる例において、ノンスデータは、静的トークンを収めるキャプチャ画像データの状態から収集されてよく、ここで、静的トークンは識別情報の一部を提供することができる。

【０１３８】
[0146] ノンスデータは、識別データの収集と並行して収集されてよい。本明細書の他の場所で説明されたように、ノンスデータは、識別データを収める物理トークンが画像デバイスによってスキャンされ、１つまたは複数のプロセッサによって処理され、分析されるときに収集されてよい。ノンスデータは、認証イベントの検出に応答して収集されてよい。ノンスデータは、画像デバイスを使用してユーザデバイスによって静的トークン（例えば視覚グラフィカルコード）がキャプチャされることに応答して収集されてよい。ノンスデータは、ユーザデバイス上の１つまたは複数のプロセッサを用いて収集されてよい。ノンスデータは、ユーザデバイス上の１つまたは複数のセンサを用いて収集されてよい。ノンスデータは、ユーザデバイス上の１つまたは複数のセンサによって収集されたセンサデータに基づいて生成されてよい。ノンスデータは、画像デバイスの状態に関するデータを含むか、またはこれらのデータから導出されてよい。ノンスデータは、キャプチャ画像データの状態に関するデータを含むか、またはこれらのデータから導出されてよい。ノンスデータは、ユーザデバイスの状態に関するデータを含むか、またはこれらのデータから導出されてよい。ノンスデータは、画像デバイスの局所状態もしくは環境状態に関するデータを含むか、またはこれらのデータから導出されてよい。ノンスデータは、画像デバイスの動作パラメータ、画像データの特性、位置情報、時間に基づく情報、または本明細書の他の場所で説明されるような他の任意のタイプの情報を含むことができる。ノンスデータは、認証イベント間で繰り返し現れる可能性の低いデータを含むか、またはこれらのデータから導出されてよい。ノンスデータは、認証イベント間で繰り返し現れる可能性が２％、１％、０．５％、０．１％、０．０５％、０．０１％、０．００５％、または０．００１％より小さいデータを含むことができる。ノンスデータは、繰り返し用いられることのない特異値を表すことができる。いくつかの実施形態において、ノンスデータが１００％同一になる場合、これは、リプレイアタックを示すか、またはリプレイアタックである可能性が極めて高い。

【０１３９】
[0147] ノンスデータは、ただ１つの時点の、または複数の時点にわたる、画像デバイスの状態および／またはキャプチャ画像データの状態を反映することができる。ノンスデータは、この認証イベントに対して実質的に一意であってよい。ユーザデバイスから収集されたデータは任意選択により、ユーザデバイスの外部のデバイスに通信されてよい。収集データは、ノンスデータのセットを生成するためにユーザデバイス内で解釈されてよい。

一方、ユーザデバイスの外部のデバイスは、受け取られた収集データに基づいてノンスデータを生成することができる。外部デバイスがノンスデータを生成すると、ノンスデータは、ユーザデバイスに送り返されても、されなくてもよい。

【０１４０】

[0148] ノンスデータのセットが生成されると、これは、認証のために識別データで封印されてよい７０４。識別データおよびノンスデータを含む封印された認証パラメータは、図６で説明されたものと同じ認証パラメータ６００であってよい。封印された認証パラメータは、さらなるセキュリティを取引イベントにもたらすために、さらに暗号化されても、されなくてもよい。いくつかの実施形態において、封印された識別データおよびノンスデータは、サーバ、またはユーザの認証をリクエストする他のタイプのホストデバイスなどの取引エンティティに伝送されてよい。取引エンティティは、ノンスデータおよび識別データを取得するために、封印された認証パラメータを解読する必要があっても、なくてもよい。

【０１４１】

[0149] ノンスデータのセットが生成されると、これは、履歴上のノンスデータおよび履歴上の識別データ７０６として識別データと共に格納されてよい。ノンスデータおよび識別データが格納される方式は、図６で説明されたものと同じであってよい。履歴上のノンスデータおよび識別データは、１つまたは複数のメモリユニットに格納されてよい。履歴上のノンスデータおよび識別データは、ユーザデバイスに搭載されたメモリ、ユーザデバイスの外部のデバイス（例えば、ホストサーバ、上述のタイプのいずれかの別々のデバイス）に搭載されたメモリに格納されてよく、または複数のデバイス（例えば、ユーザデバイスと外部デバイスの間のピアツーピア、クラウドコンピューティングベースのインフラストラクチャ）にわたって分散されてもよい。いくつかの実施形態において、ノンスデータは、ユーザデバイス内で生成され、ユーザデバイス、外部デバイス内に格納されてよく、または複数のデバイスにわたって分散されてもよい。他の実施形態において、ノンスデータは、外部デバイス内で生成されてよく、外部デバイス、またはユーザデバイス内に格納されてよく、または複数のデバイスにわたって分散されてもよい。１つまたは複数のメモリユニットは、データベースを含むことができる。履歴上のノンスデータおよび識別データのただ１つの複製が格納されてよく、または複数の複製が格納されてもよい。複数の複製は、様々なメモリユニットに格納されてよい。例えば、複数の複製は、相違するデバイス上に格納されてよい（例えば、第１の複製はユーザデバイス内に格納されてよく、第２の複製は外部デバイス内に格納されてよい）。

【０１４２】

[0150] 履歴上のノンスデータは、ユーザデバイスの１つまたは複数のセンサおよび１つまたは複数のプロセッサを用いて収集されるデータを含むことができる。同じユーザ、同じ物理トークンに属するとされ、および／または同じデバイスと関連付けられたノンスデータを、履歴上のノンスデータは含むことができる。例えば、ノンスデータの現在のセットが、第１のユーザに対して収集される場合、履歴上の位置データは、同じユーザに対して収集されたノンスデータを含むことができる。これは、同じデバイスを使用して収集される同じユーザ（および／またはデバイス）のすべてのノンスデータを含むことができる。これは、「登録」ノンスデータを含んでも、含まなくてもよい。いくつかの実施形態において、ユーザは、初期認証を行うことによって、ユーザのアイデンティティおよび／またはユーザデバイスのアイデンティティを登録することができる。初期認証から生成されたノンス情報のセットは、登録ノンスデータとして格納されてよい。一方、特定の登録ノンスデータは作り出されない。ユーザ（および／または同じデバイス）の認証イベントすべてからの様々なノンスデータが格納されてよい。一方、登録ノンスデータだけが格納されてもよい。一方、特定のユーザ（および／またはユーザデバイス）のノンスデータの最も最近のセットだけが格納されてもよい。いくつかの例において、特定のユーザ（および／またはデバイス）のノンスデータの最も最近のＸ個のセットだけが格納されてよく、ここでＸは、例えば、Ｘ＝１、２、３、４、５、６、７、８、９、１０、またはそれ以上と

いった所定の数である。

【０１４３】

[0151] いくつかの実施形態において、履歴上のノンスデータは、ユーザデバイスと対話したいずれかのユーザに属するユーザデバイスによって収集されたノンスデータを含むことができる。例えば、複数のユーザが、ユーザデバイスを使用して取引または認証イベントを行ったことがあってよい。履歴上のノンスデータは、様々なユーザ（および／または同じユーザもしくは異なるユーザのデバイス）に属するノンスデータを含むことができ、これは、同じとされるユーザを含むことができる。例えば、ノンスデータの現在のセットが、第１のデバイスに対して収集される場合、履歴上のノンスデータは、同じユーザならびに他のユーザに対して収集されるノンスデータのセットを含むことができる。これは、同じデバイスを使用して収集される１つまたは複数のユーザのすべてのノンスデータを含むことができる。これは、「登録」ノンスデータを含んでも、含まなくてもよい。いくつかの実施形態において、ユーザは、初期認証イベントを行うことによって、ユーザまたはユーザのデバイスを登録することができる。初期認証イベントから生成されたノンスデータのセットは、このユーザの、またはユーザのこのデバイスの登録ノンスデータとして格納されてよい。このような登録は、複数のデバイスおよび／または複数のユーザに対して発生してよい。いくつかの例において、各デバイスは、デバイスが認証イベントのために使用される初回に登録される必要があることがある。一方、特定の登録ノンスデータは作り出されない。認証イベントすべてからのノンスデータの様々なセットが格納されてよい。一方、登録ノンスデータだけがデバイスごとまたはユーザごとに格納されてよい。一方、デバイスごとまたはユーザごとのノンスデータの最も最近のセットだけが格納されてよい。いくつかの例において、デバイスごとまたはユーザごとのノンスデータの最も最近のＸ個のセットだけが格納されてよく、ここでＸは、例えば、Ｘ＝１、２、３、４、５、６、７、８、９、１０、またはそれ以上といった所定の数である。

【０１４４】

[0152] 前述のように、履歴データは、特定のユーザデバイスを使用して収集されるデータに関係してよい。一方、ユーザデバイスからのデータが共有および／または集約されてよい。履歴データは複数のユーザデバイスからのデータを含むことができる。履歴データは、複数のユーザデバイスを通じて収集されたノンスデータを含むことができる。これは、ただ１つのユーザデバイスで、または複数のユーザデバイスにわたって認証イベントを行う同じユーザまたは複数のユーザを含むことができる。履歴データは、履歴上のノンスデータのデータベースに情報を提供し得る１つのユーザデバイスまたは複数のユーザデバイスと対話している可能性があるすべてのユーザに関係があるデータを含むことができる。例えば、サーバ、または本明細書の他の場所で説明された他の任意のデバイスなどの外部デバイスは、１つまたは複数のユーザデバイスからノンスデータを受け取り、履歴上のノンスデータを格納することができる

【０１４５】

[0153] ノンスデータおよび識別情報のセットが収集された後、このセットは、ノンスデータと識別データの１つまたは複数の以前に収集されたセットと比較されてよい７０８。これは、認証または識別のために識別データを履歴上の識別データと比較し、その後、詐欺行為の検出のために、ノンスデータのセットをアイデンティティと関連付けられた履歴上のノンスデータと比較することを含むことができる。ノンスデータのセットは、同じ識別データ（例えば、認証イベントのために使用されているものと同じユーザの物理トークン、同じユーザ、または同じユーザデバイス、等）からのものであるとされるノンスデータのセットと比較されてよい。例えば、識別データは、ユーザの名前または他の識別子などの識別情報を含んでよく、またはユーザの名前または他の識別子がアクセスされ得るアカウントにアクセスするために使用されてもよい。識別情報は、同じとされるユーザを識別するために使用されてよい。例えば、ユーザがＪｏｈｎ　Ｄｏｅであることを識別情報が示す場合、ノンスデータのセットは、Ｊｏｈｎ　Ｄｏｅに属するノンスデータの他のセットと比較されてよい。これは、Ｊｏｈｎ　Ｄｏｅのすべてのカードのノンスデータ、ま

たは認証イベントのために使用されているものと同じＪｏｈｎ　Ｄｏｅの物理トークンだけと比較されてよい。収集されたノンスデータが、以前に格納されたノンスデータに寸分たがわずマッチする場合、ユーザが、Ｊｏｈｎ　Ｄｏｅとして以前に識別された同じユーザである可能性があるかどうかについて、いくらかの疑いが提起されることがある。同一のマッチが自然に発生する可能性は非常に低い可能性があり、リプレイアタックを示す可能性がある。

【０１４６】

[0154] ノンスデータのセットは、同じユーザに属すると思われるノンスデータの以前に収集されたセットのいずれかまたはすべてと比較されてよい。これは、さらに具体的には、同じユーザの物理トークンに狭められてよく、または同じユーザのいずれかまたはすべての物理トークンに適用してもよい。例えば、ノンスデータの登録セットが提供される場合、ノンスデータの収集されたセットは、ノンスデータの登録セットと比較されてよい。収集されたノンスデータは、他の任意のノンスデータと比較されずに登録ノンスデータと比較されてよく、登録ノンスデータおよび他のノンスデータと比較されてもよく、または登録ノンスデータと比較されずに他のノンスデータと比較されてもよい。いくつかの例において、ノンスデータは、最も最近に収集されたノンスデータと比較されてよい。ノンスデータは、任意の数の最も最近に収集されたノンスデータに対して、例えば、ノンスデータの最も最近に収集された２つのセット、ノンスデータの最も最近に収集された３つのセット、ノンスデータの最も最近に収集された４つのセット、ノンスデータの最も最近に収集された５つのセット、などといった、所定の数の最も最近に収集されたノンスデータと比較されてよい。

【０１４７】

[0155] いくつかの実施形態において、ノンスデータは、これらが所定の範囲内にあるかどうかを確かめるためにチェックされてよい。ノンスデータが所定の範囲を超えているのが検出されると、詐欺師によって悪意をもってデータが変更される可能性がある。例えば、画像フレームに対するバーコード領域の配向角から導出されたノンスデータは、（４桁のフォーマットで）０００００から３６００までの範囲にあってよく、３８００など、数字が範囲外にあることが検出される場合、これは詐欺行為を示すことができる。

【０１４８】

[0156] ノンスデータは、履歴上のノンスデータに識別情報を格納したいずれかのユーザからのものであるとされるノンスデータと比較されてよい。ノンスデータのセットが収集されるとき、識別情報は認証イベント中に収集されてよく、この情報は、ユーザおよび／またはユーザデバイスに関するデータを含むことができる。以前に論じられたように、識別情報はユーザを識別するために使用されてよい。識別情報は、同じとされるユーザを識別するために使用されてよい。例えば、識別情報が、ユーザがＪｏｈｎ　Ｄｏｅであることを示すか、またはこのことを見つけるために使用される場合、カードのノンスデータは、Ｊｏｈｎ　Ｄｏｅ、ならびに履歴データを格納した可能性がある他のいずれかのユーザに属する他のノンスデータと比較されてよい。収集されたノンスデータが、以前に格納されたノンスデータに寸分たがわずマッチする場合、これは、リプレイアタックの疑いを提起することができる。

【０１４９】

[0157] ノンスデータのセットは、認証イベントに参加したユーザのいずれかに属すると思われるノンスデータの以前に収集されたセットのいずれかまたはすべてと比較されてよい。例えば、様々なユーザのノンスデータが提供される場合、ノンスデータは様々なユーザの登録ノンスデータと比較されてよい。ノンスデータは、他の任意のノンスデータと比較されずに登録ノンスデータと比較されてよく、登録ノンスデータおよび他のノンスデータと比較されてもよく、または登録ノンスデータと比較されずに他のノンスデータと比較されてもよい。いくつかの例において、ノンスデータは、ユーザ、またはユーザのデバイスのそれぞれの最も最近に収集されたノンスデータと比較されてよい。ノンスデータは、ノンスデータの任意の数の最も最近に収集されたセットに対して、例えば、ノンスデータ

の最も最近に収集された２つのセット、ノンスデータの最も最近に収集された３つのセット、ノンスデータの最も最近に収集された４つのセット、ノンスデータの最も最近に収集された５つのセット、などといった、所定の数の最も最近に収集されたノンスデータと比較されてよい。

【０１５０】

[0158] 比較に基づくユーザの識別が評価されてよい７１０。識別は、識別データに基づく実際のユーザとしてユーザを認証すること含むことができる。同じ識別データに対して、ノンスデータの以前に格納されたセットと比較されるときにノンスデータの収集されたセットが注意を促す場合（例えば、マッチがあまりにも同一すぎるとき）、現在、現在の認証イベントが同じユーザによって行われていないことを示すことができる。例えば、ノンスデータが寸分たがわずマッチし、Ｊｏｈｎ Ｄｏｅのノンスデータの以前のセットが存在する場合、認証を試みる現在のユーザは、Ｊｏｈｎ Ｄｏｅではない可能性がある。同じ識別および／または認証がユーザデバイスに対して行われてよい。例えば、ユーザデバイスが、このデバイス自体を特定のデバイスとして識別しており、以前の認証イベントのデータと同じノンスデータが収集される場合、注意を促されてよい。現在の認証イベントが同じデバイスによって行われておらず、別のデバイスがリプレイアタックに参加している可能性があるということを示すことができる。

【０１５１】

[0159] 任意選択により、見込みの詐欺行為の指示が提供されてよい。例えば、識別データが特定のユーザ（例えばＪｏｈｎ Ｄｏｅ）として識別し、同じユーザ（例えばＪｏｈｎ Ｄｏｅ）の以前の認証イベントからのノンスデータにノンスデータが寸分たがわずマッチする場合、詐欺行為の可能性がもたらされてよい。詐欺行為の可能性は、バイナリの指標（例えば、詐欺行為の注意喚起、詐欺行為なし）であってよく、またはリスク値（例えば、割合などの数値、またはレターグレードなどのグレード値）として提供されてもよい。例えば、詐欺行為グレード９は、詐欺行為グレード２より高い詐欺行為の見込みを提供することができる。

【０１５２】

[0160] 収集されたノンスデータは、寸分たがわずマッチする（例えば１００％マッチする）とみなされることになるノンスデータの以前に格納されたセットに対して完全に同一であってよい。完全な１００％マッチは疑わしい可能性がある。例えば、ユーザが認証イベントを行うたびに、いくつかの小さな変化がある可能性がある。物理的に、正確に同じ位置（例えば、方向および／または空間的位置）で個人が認証イベントを行う可能性は極めて低い。別の例において、物理トークンの全く同じ画像をキャプチャする可能性も極めて低い。全く同じ特性を有することは、一種のリプレイアタックの指標であってよい。

【０１５３】

[0161] いくつかの実施形態において、詐欺行為のリスクが検出されると、１人または複数の個人が注意喚起されてよい。例えば、認証イベントを行っているユーザは、認証についての彼らの試みが、詐欺行為の多少のリスクによって注意を向けられたことを通知されても、されなくてもよい。ユーザが取引を行うおうとしているエンティティは、詐欺行為のリスクを通知されても、されなくてもよい。例えば、ユーザがｅコマースサイトから品物を購入しようとしている場合、ｅコマースサイトは、取引が、詐欺行為の多少のリスクによって注意を向けられたことを通告されてよい。取引自体は継続することを許可されても、されなくてもよい。いくつかの例において、詐欺行為の何らかのリスクがある場合、取引は停止されてよい。一方、詐欺行為の多少のリスクがあるが、リスクは低いと判断される場合、取引は、１つもしくは複数の当事者が多少の詐欺行為リスクを通知される間に継続することができ、および／またはさらなるチェックが発生してもよい。詐欺行為のリスクが閾値レベルを超える場合（例えば、詐欺行為の適度のまたは高いリスクに到達する場合）、取引は停止されてよい。

【０１５４】

[0162] 任意のタイプの詐欺行為が検出されてよい。いくつかの実施形態において、検出

される詐欺行為は、リプレイアタックを含むことができる。リプレイアタック中、同じユーザ、ユーザデバイスとしてごまかすか、または認証イベントを完了させる（例えば、取引を完了させる）ために、認証イベント中にデータが記録されることがあり、その後、その後の認証イベントでリプレイされる。リプレイアタックは、初期認証イベントとは異なるユーザによって、または初期認証イベントと同じユーザによって行われることがある。リプレイアタックは、初期認証イベントと同じデバイスを使用して、または初期認証イベントとは異なるデバイスを使用して行われることがある。

【０１５５】

[0163] いくつかの例において、取引を停止するための閾値は、取引の価格、または取引の他の特性に依存してよい。例えば、高額取引に関して、取引を停止するための閾値は、少額取引の閾値よりも低くてよい。例えば、取引が大きい金額のものである場合、低いリスクの詐欺行為でも取引を停止させることができるが、比較的小さな金額に対しては、取引を停止させるために比較的高いリスクの詐欺行為が要求されてよい。一方、取引を停止するための閾値は、すべての取引に対して同じであってよい。

【０１５６】

[0164] 封印されたノンスデータおよび識別データが、認証イベント中に、および／または認証イベントに応答して、収集されてよい。例えば、ノンスデータおよび識別データは、ユーザが、自分を自己識別および／または認証しようとしているときに収集されてよい。ユーザは、ユーザアカウントにアクセスし、および／または取引を行うために、自己識別しようとするか、および／または認証されてよい。封印されたノンスデータおよび識別データは、デバイスおよび／またはユーザの認証のために、個別に、または組み合わせて使用されてよい。封印されたノンスデータおよび識別データは、取引を認可する際に個別に、または財務情報などの他の情報と組み合わせて使用されてよい。封印されたノンスデータおよび識別データは、詐欺行為の検出のために単独で使用されてよい。

【０１５７】

[0165] いくつかの実施形態において、ノンスデータおよび識別データが分析されるとき、すべてに対するデータが、ただ１つのイベントから収集されてよい。ノンスデータおよび識別データのすべてが同時に評価されてよい。他のいくつかの実施形態において、ノンスデータおよび識別データは、順番に、または様々な順序で評価されてよい。

【０１５８】

[0166] 認証処理の様々な工程がユーザデバイス上で行われてよい。ユーザデバイスは、本明細書の他の場所で説明されたように、例えば、開示の実施形態と一致する１つまたは複数の動作を行うように構成される１つまたは複数のコンピューティングデバイスであってよい。例えば、ユーザデバイスは、ソフトウェアまたはアプリケーションを実行できるコンピューティングデバイスであってよい。いくつかの実施形態において、ソフトウェアおよび／またはアプリケーションは、ユーザデバイスを使用してグラフィカルコード／トークンをユーザがスキャンできるようにすることによって識別データおよびノンスデータを収集すること７０２、識別情報をデコードし、ノンスデータを収集するためにキャプチャ画像を処理すること、取引中にユーザデバイスと、他の外部デバイスまたはシステムとの間で封印された認証データを伝送すること７０４を行うように構成されてよい。ソフトウェアおよび／またはアプリケーションは、封印された認証データを暗号化しても、しなくてもよい。いくつかの実施形態において、ソフトウェアおよび／またはアプリケーションは、取引に関わる他のデバイスもしくはエンティティから受け取られた命令、または所定の命令に基づいて、物理トークンのタイプをキャプチャすることをユーザに促すように構成されてよい。

【０１５９】

[0167] いくつかの実施形態において、ソフトウェアおよび／またはアプリケーションは、取引中に、識別データおよびノンスデータをユーザデバイス上の履歴データと比較すること７０８、次にさらなる識別または認証のために別のデバイスまたはシステムに評価結果を提供すること７１０を行うように構成されてよい。他の実施形態において、ソフトウ

ェアおよび／またはアプリケーションは、取引を完了させるためにユーザデバイス上で比較７０８および識別／認証７１０を行うように構成されてよい。

【０１６０】

[0168] ソフトウェアおよび／またはアプリケーションは、追加の取引情報と共に識別データおよびノンスデータを封印するように構成されても、されなくてもよい。いくつかの実施形態において、ノンスデータを収集するために使用される画像データ以外の様々なソースまたは手段によって追加の取引情報が提供されてよい。例えば、取引中にユーザは、認証のためにカードまたは外部デバイス上のグラフィカルコード（例えばＩＤカード上のバーコード）をスキャンするように促されてよい。キャプチャ画像から収集された識別情報およびノンスデータに加えて、ユーザは、ユーザアカウント名、パスワード、金融取引額、および同様のものなどの他の取引情報を入力することもできる。追加情報は、識別データおよびノンスデータと共に封印され、取引に関わる他のエンティティに伝送されてよい。

【０１６１】

[0169] ソフトウェアおよび／またはアプリケーションは、画像デバイスを制御するようにさらに構成されてよい。いくつかの実施形態において、画像デバイスの動作パラメータのセットを収める動的トークンが、ソフトウェアおよび／またはアプリケーションによって受け取られてよい。動的トークンは、図６で説明されたものと同じ動的トークンであってよい。したがって、ソフトウェアは、動的トークンに基づくパラメータを使用して画像データをキャプチャするように画像デバイスに命令することができる。

【０１６２】

[0170] 他の実施形態において、ノンスデータは、詐欺行為の検出のために単独で使用されてよい。ノンスデータはこれ自体に対して分析されてよく、および／またはノンスデータの１つまたは複数の以前に格納されたセットと比較されてよい。ノンスデータが、ノンスデータの以前に格納されたセットに寸分たがわずマッチする場合、リプレイアタックの危険があることが判断されてよい。これは、ユーザが、自分が称しているユーザではないということ、またはユーザが改ざん情報を提供しているということを示唆することができる。

【０１６３】

[0171] 図８は、本発明の実施形態による、ノンスデータを使用して、ユーザおよび／またはデバイスを識別する例を示す。ノンスデータのセットは、ユーザデバイスを使用して収集されてよい８０２。ノンスデータは、履歴上のノンスデータと共に格納されてよい８０４。ノンスデータは、ノンスデータの１つまたは複数の以前に収集されたセットと比較されてよい８０６。比較に基づくユーザの識別が評価されてよい８０８。いくつかの実施形態において、取引は、比較に基づいて許可されても、されなくてもよい。任意選択により、リプレイアタックなどの詐欺行為の見込みの指示が提供されてよい。本明細書の他の場所における封印された認証データのいずれかの説明は、本明細書で提供されるようなノンスデータに適用することもできる。

【０１６４】

[0172] ノンスデータのセットは、認証イベント中に収集されてよい８０２。ノンスデータは継続的に、またはスケジュールに応じて収集されてよい。ノンスデータは、認証イベントの検出に応答して収集されてよい。ノンスデータは、画像ベースのトークンがユーザデバイスによってキャプチャされることに応答して収集されてよい。ノンスデータは、ユーザデバイス上の１つまたは複数のプロセッサのを用いて収集されてよい。ノンスデータは、ユーザデバイス上の１つまたは複数のセンサを用いて収集されてよい。ノンスデータは、ユーザデバイス上の１つまたは複数のセンサによって収集されたセンサデータに基づいて生成されてよい。ノンスデータは、画像デバイスの状態に関するデータを含むか、またはこれらのデータから導出されてよい。ノンスデータは、キャプチャ画像データの状態に関するデータを含むか、またはこれらのデータから導出されてよい。ノンスデータは、ユーザデバイスの状態に関するデータを含むか、またはこれらのデータから導出されてよ

い。ノンスデータは、画像デバイスの局所状態もしくは環境状態に関するデータを含むか、またはこれらのデータから導出されてよい。ノンスデータは、画像デバイスの動作パラメータ、画像データの特性、位置情報、時間に基づく情報、または本明細書の他の場所で説明されるような他の任意のタイプの情報を含むことができる。ノンスデータは、認証イベント間で繰り返し現れる可能性の低いデータを含むか、またはこれらから導出されてよい。ノンスデータは、認証イベント間で繰り返し現れる可能性が、２％、１％、０．５％、０．１％、０．０５％、０．０１％、０．００５％、または０．００１％より小さいデータを含むことができる。ノンスデータは、繰り返し用いられることのない特異値を表すことができる。いくつかの実施形態において、ノンスデータが１００％同一だった場合、これは、リプレイアタックを示すか、またはリプレイアタックである可能性が極めて高い。

【０１６５】

[0173] ノンスデータは、ただ１つの時点でまたは複数の時点にわたって画像デバイスの状態および／またはキャプチャ画像データの状態を反映することができる。ノンスデータは、この認証イベントに対して実質的に一意であってよい。ユーザデバイスから収集されたデータは任意選択により、ユーザデバイスの外部のデバイスに通信されてよい。収集データは、ノンスデータのセットを生成するために、ユーザデバイス内で解釈されてよい。一方、ユーザデバイスの外部のデバイスは、受け取られた収集データに基づいてノンスデータを生成することができる。外部デバイスがノンスデータを生成する場合、ノンスデータは、ユーザデバイスに送り返されても、されなくてもよい。

【０１６６】

[0174] ノンスデータのセットが生成されると、これは、履歴上のノンスデータと共に格納されてよい８０４。履歴上のノンスデータは、１つまたは複数のメモリユニットに格納されてよい。履歴上のノンスデータは、ユーザデバイスに搭載されたメモリ、ユーザデバイスの外部のデバイス（例えば上述のタイプのいずれかの別々のデバイス）に搭載されたメモリに格納されてよく、または複数のデバイス（例えば、ユーザデバイスと外部デバイスの間にある、ピアツーピアの、クラウドコンピューティングベースのインフラストラクチャ）にわたって分散されてもよい。いくつかの実施形態において、ノンスデータは、ユーザデバイス内で生成され、ユーザデバイス、外部デバイス内に格納されてよく、または複数のデバイスにわたって分散されてもよい。他の実施形態において、ノンスデータは、外部デバイス内で生成され、外部デバイス、またはユーザデバイス内に格納されてよく、または複数のデバイスにわたって分散されてもよい。１つまたは複数のメモリユニットは、データベースを含むことができる。履歴上のノンスデータのただ１つの複製が格納されてよく、または複数の複製が格納されてもよい。複数の複製は様々なメモリユニットに格納されてよい。例えば、複数のコピーは、相違するデバイスに格納されてよい（例えば、第１の複製はユーザデバイス内に格納されてよく、第２の複製は外部デバイス内に格納されてよい）。

【０１６７】

[0175] 履歴上のノンスデータは、ユーザデバイスの１つまたは複数のセンサおよび１つまたは複数のプロセッサを用いて収集されるデータを含むことができる。履歴上のノンスデータは、同じユーザに属するとされ、および／または同じデバイスと関連付けられたノンスデータを含むことができる。例えば、ノンスデータの現在のセットが、第１のユーザに対して収集される場合、履歴上の位置データは、同じユーザに対して収集されたノンスデータを含むことができる。これは、同じデバイスを使用して収集される同じユーザ（および／またはデバイス）に対するすべてのノンスデータを含むことができる。これは、「登録」ノンスデータを含んでも、含まなくてもよい。いくつかの実施形態において、ユーザは、初期認証を行うことによって、ユーザのアイデンティティおよび／またはユーザデバイスのアイデンティティを登録することができる。初期認証から生成されたノンス情報のセットは、登録ノンスデータとして格納されてよい。一方、特定の登録ノンスデータは作り出されない。ユーザ（および／または同じデバイス）の認証イベントすべてからの様

々なノンスデータが格納されてよい。一方、登録ノンスデータだけが格納されてもよい。一方、特定のユーザ（および／またはユーザデバイス）のノンスデータの最も最近のセットだけが格納されてもよい。いくつかの例において、特定のユーザ（および／またはデバイス）のノンスデータの最も最近のＸ個のセットだけが格納されてよく、ここでＸは、例えば、Ｘ＝１、２、３、４、５、６、７、８、９、１０、またはそれ以上といった所定の数である。

【０１６８】

[0176] いくつかの実施形態において、履歴上のノンスデータは、ユーザデバイスと対話したいずれかのユーザに属するユーザデバイスによって収集されたノンスデータを含むことができる。履歴上のノンスデータは、様々なユーザ（および／または同じユーザのデバイスもしくは異なるユーザ）に属するノンスデータを含むことができ、これは、同じとされるユーザを含むことができる。これは、同じデバイスを使用して収集される１つまたは複数のユーザに対するすべてのノンスデータを含むことができる。これは、「登録」ノンスデータを含んでも、含まなくてもよい。いくつかの実施形態において、ユーザは、初期認証イベントを行うことによって、ユーザまたはユーザのデバイスを登録することができる。初期認証イベントから生成されたノンスデータのセットは、このユーザに対する、またはユーザのこのデバイスに対する登録ノンスデータとして格納されてよい。このような登録は、複数のデバイスおよび／または複数のユーザに対して発生してよい。いくつかの例において、各デバイスは、認証イベントのためにデバイスが使用される初回に登録される必要があることがある。一方、特定の登録ノンスデータは作り出されない。認証イベントすべてからのノンスデータの様々なセットが格納されてよい。一方、登録ノンスデータだけが、デバイスごとまたはユーザごとに格納されてもよい。一方、デバイスごとまたはユーザごとのノンスデータの最も最近のセットだけが格納されてもよい。いくつかの例において、デバイスごとまたはユーザごとのノンスデータの最も最近のＸ個のセットだけが格納されてよく、ここでＸは、例えば、Ｘ＝１、２、３、４、５、６、７、８、９、１０、またはそれ以上といった所定の数である。

【０１６９】

[0177] ノンスデータのセットが収集された後、このデータは、ノンスデータの１つまたは複数の以前に収集されたセットと比較されてよい８０６。これは、ノンスデータのセットを履歴上のノンスデータと比較することを含むことができる。ノンスデータのセットは、同じユーザ（または同じユーザデバイス）からのものであるとされるノンスデータのセットと比較されてよい。例えば、ノンスデータのセットが収集されるとき、追加情報は、認証イベント中に収集されてよく、これは、認証／識別情報を含むことができる。追加情報は、ユーザの名前または他の識別子などの識別情報を含んでよく、またはユーザの名前または他の識別子がアクセスされ得るアカウントにアクセスするために使用されてもよい。追加情報は、同じとされるユーザを識別するために使用されてよい。例えば、ユーザがＪｏｈｎ　Ｄｏｅであることを追加情報が示す場合、ノンスデータのセットは、Ｊｏｈｎ　Ｄｏｅに属するノンスデータの他のセットと比較されてよい。これは、Ｊｏｈｎ　Ｄｏｅのすべてのカード、または認証イベントのために使用されているものと同じＪｏｈｎ　Ｄｏｅのユーザデバイスだけに対するノンスデータと比較されてよい。収集されたノンスデータが、以前に格納されたノンスデータに寸分たがわずマッチする場合、ユーザが、Ｊｏｈｎ　Ｄｏｅとして以前に識別された同じユーザである可能性があるかどうかについて、いくらかの疑いが提起される。同一のマッチが自然に発生する可能性は非常に低い可能性があり、リプレイアタックを示す可能性がある。

【０１７０】

[0178] 追加情報は、本明細書の他の場所で説明されるような識別データを含むことができる。識別情報は、図７で説明されたものと同じ識別情報であってよい。

【０１７１】

[0179] ノンスデータのセットは、同じユーザに属すると思われるノンスデータの以前に収集されたセットのいずれかまたはすべてと比較されてよい。これは、より具体的には、

ユーザの同じデバイスに狭められてよく、または同じユーザのいずれかまたはすべてのデバイスに適用してよい。例えば、ノンスデータの登録セットが提供される場合、ノンスデータの収集されたセットは、ノンスデータの登録セットと比較されてよい。収集されたノンスデータは、他のいずれかのノンスデータと比較されずに登録ノンスデータと比較されてよく、登録ノンスデータおよび他のノンスデータと比較されてもよく、または登録ノンスデータと比較されずに他のノンスデータと比較されてもよい。いくつかの例において、ノンスデータは、最も最近に収集されたノンスデータと比較されてよい。ノンスデータは、任意の数の最も最近に収集されたノンスデータに対する、例えば、ノンスデータの最も最近に収集された２つのセット、ノンスデータの最も最近に収集された３つのセット、ノンスデータの最も最近に収集された４つのセット、ノンスデータの最も最近に収集された５つのセット、などといった、所定の数の最も最近に収集されたノンスデータと比較されてよい。

【０１７２】

[0180] いくつかの実施形態において、ノンスデータは、これらが所定の範囲内にあるかどうかを確かめるためにチェックされてよい。ノンスデータが所定の範囲を超えているのが検出されると、詐欺師によって悪意をもってデータが変更される可能性がある。例えば、画像フレームに対するバーコード領域の配向角から導出されたノンスデータは、（４桁のフォーマットで）０００００から３６００までの範囲にあってよく、３８００など、数字が範囲外にあることが検出される場合、これは詐欺行為を示すことができる。

【０１７３】

[0181] ノンスデータは、履歴上のノンスデータに情報を格納したいずれかのユーザからのものであるとされるノンスデータと比較されてよい。ノンスデータのセットが収集されるとき、追加情報は認証イベント中に収集されてよく、この情報は、ユーザおよび／またはユーザデバイスに関するデータを含むことができる。以前に論じられたように、追加情報は、ユーザを識別するために使用され得る情報を識別することを含むことができる。追加情報は、同じとされるユーザを識別するために使用されてよい。例えば、追加情報が、ユーザがＪｏｈｎ　Ｄｏｅであることを示すか、またはこのことを見つけるために使用される場合、カードのノンスデータは、Ｊｏｈｎ　Ｄｏｅ、ならびに履歴データを格納した可能性がある他のいずれかのユーザに属する他のノンスデータと比較されてよい。収集されたノンスデータが、以前に格納されたノンスデータに寸分たがわずマッチする場合、これは、リプレイアタックの疑いを提起することができる。

【０１７４】

[0182] ノンスデータのセットは、認証イベントに参加したユーザのいずれかに属すると思われるノンスデータの以前に収集されたセットのいずれかまたはすべてと比較されてよい。例えば、様々なユーザのノンスデータが提供される場合、ノンスデータは、様々なユーザの登録ノンスデータと比較されてよい。ノンスデータは、他の任意のノンスデータと比較されずに登録ノンスデータと比較されてよく、登録ノンスデータおよび他のノンスデータと比較されてもよく、または登録ノンスデータと比較されずに他のノンスデータと比較されてもよい。いくつかの例において、ノンスデータは、ユーザ、またはユーザのデバイスのそれぞれの最も最近に収集されたノンスデータと比較されてよい。ノンスデータは、ノンスデータの任意の数の最も最近に収集されたセットに対して、例えば、ノンスデータの最も最近に収集された２つのセット、ノンスデータの最も最近に収集された３つのセット、ノンスデータの最も最近に収集された４つのセット、ノンスデータの最も最近に収集された５つのセット、などといった、所定の数の最も最近に収集されたノンスデータと比較されてよい。

【０１７５】

[0183] 比較に基づくユーザの識別が評価されてよい８０８。識別は、認証および／または識別情報に基づく実際のユーザとしてユーザを認証することを含むことができる。同じ追加情報に対して、ノンスデータの以前に格納されたセットと比較されるときにノンスデータの収集されたセットが注意を促す場合（例えば、マッチがあまりにも同一すぎるとき

）、現在、現在の認証イベントが同じユーザによって行われていないことを示すことができる。例えば、ノンスデータが寸分たがわずマッチし、Ｊｏｈｎ　Ｄｏｅのノンスデータの以前のセットが存在する場合、認証を試みる現在のユーザは、Ｊｏｈｎ　Ｄｏｅではない可能性がある。同じ識別および／または認証がユーザデバイスに対して行われてよい。例えば、ユーザデバイスが、このデバイス自体を特定のデバイスとして識別しており、以前の認証イベントのデータと同じノンスデータが収集される場合、注意を促されてよい。現在の認証イベントが同じデバイスによって行われておらず、別のデバイスがリプレイアタックに参加している可能性があるということを示すことができる。

【０１７６】

[0184] 任意選択により、見込みの詐欺行為の指示が提供されてよい。例えば、様々な認証および／または識別情報が特定のユーザ（例えばJohn Doe）として識別し、同じユーザ（例えばJohn Doe）の以前の認証イベントからのノンスデータにノンスデータが寸分たがわずマッチする場合、詐欺行為の可能性がもたらされてよい。詐欺行為の可能性は、バイナリの指標（例えば、詐欺行為の注意喚起、詐欺行為なし）であってよく、またはリスク値（例えば、割合などの数値、またはレターグレードなどのグレード値）として提供されてもよい。例えば、詐欺行為グレード９は、詐欺行為グレード２より高い詐欺行為の見込みを提供することができる。

【０１７７】

[0185] 収集されたノンスデータは、寸分たがわずマッチする（例えば１００％マッチする）とみなされることになるノンスデータの以前に格納されたセットに完全に同一であってよい。完全な１００％マッチは疑わしい可能性がある。例えば、ユーザが認証イベントを行うたびに、いくつかの小さな変化がある可能性がある。物理的に、全く同じ物理トークンの画像データが認証イベントを行う個人によってキャプチャされる可能性は極めて低い。全く同じ特性を有することは、一種のリプレイアタックの指標であってよい。

【０１７８】

[0186] いくつかの実施形態において、詐欺行為のリスクが検出されると、１人または複数の個人が注意喚起されてよい。例えば、認証イベントを行っているユーザは、認証についての彼らの試みが、詐欺行為の多少のリスクによって注意を向けられたことを通知されても、されなくてもよい。ユーザが取引を行うおうとしているエンティティは、詐欺行為のリスクを通知されても、されなくてもよい。例えば、ユーザがｅコマースサイトから品物を購入しようとしている場合、ｅコマースサイトは、取引が、詐欺行為の多少のリスクによって注意を向けられたことを通告されてよい。取引自体は、継続することを許可されても、されなくてもよい。いくつかの例において、詐欺行為の何らかのリスクがある場合、取引は停止されてよい。一方、詐欺行為の多少のリスクがあるが、リスクは低いと判断される場合、取引は、１つもしくは複数の当事者が多少の詐欺行為リスクを通知される間に継続することができ、および／またはさらなるチェックが発生してもよい。詐欺行為のリスクが閾値レベルを超える場合（例えば、詐欺行為の適度のまたは高いリスクに到達する場合）、取引は停止されてよい。

【０１７９】

[0187] 任意のタイプの詐欺行為が検出されてよい。いくつかの実施形態において、検出された詐欺行為は、リプレイアタックを含むことができる。リプレイアタック中、同じユーザ、ユーザデバイスとしてごまかすか、または認証イベントを完了させる（例えば、取引を完了させる）ために、認証イベント中にデータが記録されることがあり、その後、その後の認証イベントでリプレイされる。リプレイアタックは、初期認証イベントとは異なるユーザによって、または初期認証イベントと同じユーザによって行われることがある。リプレイアタックは、初期認証イベントと同じデバイスを使用して、または初期認証イベントとは異なるデバイスを使用して行われることがある。

【０１８０】

[0188] いくつかの例において、取引を停止するための閾値は、取引の価格または取引の他の特性に依存してよい。例えば、高額取引に関して、取引を停止するための閾値は少額

取引の閾値よりも低くてよい。例えば、取引が大きい金額のものである場合、低いリスクの詐欺行為でも取引を停止させることができるが、比較的小さな合計金額に対しては、取引を停止させるために比較的高いリスクの詐欺行為が要求されてよい。一方、取引を停止するための閾値は、すべての取引に対して同じであってよい。

【０１８１】

[0189] ノンスデータは、認証イベント中に、および／または認証イベントに応答して収集されてよい。例えば、ノンスデータは、ユーザが、自分を自己識別および／または認証しようとしているときに収集されてよい。ユーザは、ユーザアカウントにアクセスし、および／または取引を行うために、自己識別しようとするか、および／または認証されてよい。ノンスデータは、個別に、または他の情報と組み合わせて識別するために使用されてよい。ノンスデータは、個別に、または組み合わせてデバイスおよび／またはユーザを認証する際に使用されてよい。ノンスデータは、取引を認可する際に個別に、または財務情報などの他の情報と組み合わせて使用されてよい。ノンスデータは、詐欺行為の検出のために単独で、または他の情報と組み合わせて使用されてよい。

【０１８２】

[0190] いくつかの実施形態において、ノンスデータ、および／または他の任意の情報が分析されるとき、すべてに対するデータが、ただ１つのイベントから収集されてよい。ノンスデータおよび／または他の任意の情報のすべてが同時に評価されてよい。他のいくつかの実施形態において、ノンスデータおよび／または他の情報は、順番に、または様々な順序で評価されてよい。

【０１８３】

[0191] いくつかの実施形態において、認証パラメータデータは、ユーザの識別および／または認証を行う際に使用されてよい。これは、取引処理に使用されてよい。詐欺行為の見込みは、認証パラメータを使用して評価されても、されなくてもよい。認証パラメータデータは任意選択により、図７に類似の処理で使用されてよく、ここで、認証パラメータは履歴データベースに格納され、比較されてよい。以前に説明されたような認証パラメータデータは、ノンスデータおよび識別データを含むことができる。いくつかの実施形態において、識別データは静的トークンであってよい。

【０１８４】

[0192] 図９は、本発明の実施形態による、認証イベントに関わるエンティティの例を提供する。前述のように、様々な取引などの任意のタイプの認証イベントは、本明細書の他の場所で説明されたように発生してよく、使用されてよい。認証は、様々な取引に対して行われてよく、これらは、金銭および／または商品もしくはサービスのやりとりを含んでも、含まなくてもよい。取引は、情報の交換を含んでも、含まなくてもよい。認証は、ユーザまたはユーザデバイスのアイデンティティをユーザが確認できるいずれかの局面を含むことができる。

【０１８５】

[0193] 認証システムは、１つまたは複数の外部デバイス９１０、９２０と通信できる１つまたは複数のユーザデバイス９００ａ、９００ｂ、９００ｃ、９００ｄを含むことができる。１つまたは複数のユーザデバイスは、１人または複数の個々のユーザと関連付けられてよい。通信は、ネットワーク９３０上で発生してよく、または直接的に発生してもよい。グラフィカルコード９６０ａ、９６０ｂ、９６０ｃ、９７０ｄなどの物理トークンは、１つまたは複数のユーザデバイスによってキャプチャされ、分析されてよく、データ（例えば、識別データおよびノンスデータ）は収集されてよい。１つまたは複数のユーザデバイスからのデータ９４０ａ、９４０ｂ、９４０ｃ、９４０ｄは、１つまたは複数の外部デバイスに伝えられてよい。いくつかの実施形態において、第１の外部デバイス９５０ａによって受け取られたデータは、第２の外部デバイス９５０ｂによって受け取られたデータと同じであってよく、またはデータは異なってもよい。１つの例において、第１の外部デバイスは、認証サーバシステム（例えば、セキュア認証を行うように構成されるサーバシステム）であるか、もしくはこれらに属してもよく、および／あるいは第２の外部デバ

イスは、１つもしくは複数の第三者（例えば、商人のシステム、仲介者のシステム、もしくはアイデンティティ認証を要する他のエンティティなどの、本明細書の他の場所で説明されるような任意の取引エンティティ）であるか、またはこれらに属してもよい。

【０１８６】

[0194] ネットワーク９３０は通信ネットワークであってよい。通信ネットワークは、ローカルエリアネットワーク（LAN）、またはインターネットなどの広域ネットワーク（WAN）を含むことができる。通信ネットワークは、送信機、受信機、およびその間でメッセージをルーティングするための様々な通信チャネル（例えばルータ）を含むテレコミュニケーションネットワークを含むことができる。通信ネットワークは、イーサネット、ユニバーサルシリアルバス（USB: Universal Serial Bus）、ＦＩＲＥＷＩＲＥ、グローバルシステムフォーモバイルコミュニケーションズ（GSM: Global System for Mobile Communications）、拡張データＧＳＭ環境（EDGE: Enhanced Data GSM Environment）、符号分割多元接続（CDMA: code division multiple access）、時分割多重アクセス（TDMA: time division multiple access）、Ｂｌｕｅｔｏｏｔｈ、Ｗｉ－Ｆｉ、ボイスオーバーインターネットプロトコル（VoIP: Voice over Internet Protocol）、Ｗｉ－ＭＡＸ、または他の任意の適切な通信プロトコルなどの、様々な有線もしくはワイヤレスプロトコルを含む任意の既知のネットワークプロトコルを使用して実装されてよい。

【０１８７】

[0195] ユーザデバイス９００ａ、９００ｂ、９００ｃ、９００ｄは、本明細書の他の場所で説明された、ユーザデバイスの様々な実施形態の１つまたは複数の特性を含むことができる。例えば、ユーザデバイスは、図１のユーザデバイスの１つまたは複数の特性、構成要素、または機能を有することができる。ユーザデバイスは、静的トークンをキャプチャするように構成される画像デバイスを備えることができる。いくつかの実施形態において、ユーザデバイスは、ユーザ、第１の外部デバイス９１０、および／または第２の外部デバイス９２０からの様々なリクエストを処理するように構成される１つまたは複数のプロセッサを含むことができる。ユーザデバイスは、取引情報、取引データ、認証情報、識別情報、財務情報、ユーザデバイスと関連付けられたユーザのアカウント情報、ユーザデバイスのデバイス情報、ユーザデバイスと対話できるカードリーダのデバイス識別子、ノンスデータ、履歴上の認証データ、および／またはユーザデバイスのユーザと関連付けられた使用データ（例えば、ユーザと関連付けられた他の活動データ）を含むがこれらに限定されない様々な情報を格納するための１つもしくは複数のデータベースを含むか、またはこれらにアクセスできてもよい。認証を容易にするために様々なタイプのユーザデバイスが使用されてよい。認証システムは、同時に使用され得る複数のタイプのユーザデバイスを含むことができる。

【０１８８】

[0196] 様々なタイプのユーザデバイスは、ハンドヘルドデバイス、ウェアラブルデバイス、モバイルデバイス、タブレットデバイス、ラップトップデバイス、デスクトップデバイス、コンピューティングデバイス、テレコミュニケーションデバイス、メディアプレーヤ、ナビゲーションデバイス、家庭用ゲーム機、テレビ、リモート制御、またはこれらのデータ処理デバイスもしくは他の処理デバイスのうちの任意の２つ以上の組合せを含むことができるがこれらに限定されない。任意選択により、ユーザデバイスは、任意のタイプのペイメントカードをなどの磁気カードを読み取ることができてよい。ユーザデバイスは、ペイメントカードの認証の読取りを行うことができてよい。ユーザデバイスは、ペイメントカードのスパイプを受け入れることができ、ペイメントカードから磁気情報を読み取ることができてよい。使用デバイスは、スワイプ速度、方向、角度、変動、および／またはペイメントカードの本来の磁気プロパティなどの、ペイメントカードの１つまたは複数のスワイプ特性を読み取ることができてよい。一方、ユーザデバイスは、本明細書で説明される機能のいずれかを有するカードリーダに接続することができる。

【０１８９】

[0197] 第１の外部デバイス９１０は、１つまたは複数のプロセッサを含むことができる

。第１の外部デバイスは認証サーバシステムであってよい。第１の外部デバイスは、１つもしくは複数のデータベースを含むか、またはこれらにアクセスできてよい。第１の外部デバイスは、１つまたは複数のユーザデバイス９００ａ、９００ｂ、９００ｃ、９００ｄと通信状態にあってよい。第１の外部デバイスは、通信ユニット（例えばI/0インターフェース）を用いて様々なユーザデバイスと通信状態にあってよい。第１の外部デバイスは、様々な取引エンティティシステム（例えば、商人のシステム、仲介者のシステム、クレジットカード会社、ソーシャルネットワークプラットフォーム、および／または他のエンティティ）と通信状態にあってよい。第１の外部デバイスは、１つまたは複数のＩ／Ｏインターフェースを用いて様々な外部サーバシステムと通信状態にあってよい。ユーザデバイスおよび／またはカードリーダへのＩ／Ｏインターフェースは、ユーザデバイスおよび／またはカードリーダそれぞれと関連付けられた入力および出力の処理を容易にすることができる。例えば、Ｉ／Ｏインターフェースは、セキュア認証のリクエストと関連付けられたユーザ入力の処理を容易にすることができる。外部サーバシステムへのＩ／Ｏインターフェースは、１つまたは複数の第三者エンティティ（例えば、商人のシステム、仲介者のシステム、クレジットカード会社、ソーシャルネットワークプラットフォーム、および／または他のエンティティ）との通信を容易にすることができる。

【０１９０】

[0198] 第１の外部デバイスは、１つまたは複数の工程を行うためのコード、ロジック、または命令を含む非一時的コンピュータ可読媒体を備えることができるメモリストレージユニット備えることができる。第１の外部デバイスの１つまたは複数のプロセッサは、例えば、非一時的コンピュータ可読媒体に従って、１つまたは複数の工程を実行することができてよい。いくつかの実施形態において、１つまたは複数のプロセッサは、セキュア認証を行い、リクエストを処理し、ノンスデータと識別データを比較し、認証に必要とされる情報を識別し、認証を行い、リクエストに応じて認証結果を返すリクエストを、生成するかまたは受け取ることができる。１つまたは複数のデータベースは、対応するノンスデータ、対応する識別データ、各ユーザと関連付けられたアカウント情報、ユーザデバイスのデバイス情報（例えばユーザデバイス識別子）、履歴上の認証データ、および／または各ユーザと関連付けられた使用データ（例えば、各ユーザと関連付けられた活動データ）を含むがこれらに限定されない様々な情報を格納することができる。

【０１９１】

[0199] ユーザに関する格納されたデータは、ユーザに関する識別情報を含むことができる。識別情報は、名前、出生のデータ、住所、電話番号、性別、社会保障番号、またはユーザに関する他の任意の個人情報を含むことができる。

【０１９２】

[0200] ユーザに関する格納されたデータは、ユーザに関する財務情報を含むことができる。財務情報は、ユーザについてのカードリーダおよび／またはユーザに関するアカウント情報を含むことができる。ユーザのカード情報は、カードの種類（例えば、クレジットカード、メンバシップカード、アイデンティティカード、等）、カード発行人（例えば、クレジットキャリア、会社、政府、等）、クレジットキャリアの種類（例えば、Visa、Mastercard、American Express、Discover、等）、カード番号、カードの有効期限、および／またはカードのセキュリティコードを含むことができる。アカウント情報は、ユーザの名前、ユーザのメールアドレス、ユーザの電話番号、ユーザの電子メールアドレス、ユーザの生年月日、ユーザの性別、ユーザの社会保障番号、ユーザアカウントＩＤと関連パスワード、またはユーザに関する他の任意の個人情報を含むことができる。

【０１９３】

[0201] ノンスデータなどの取引関連データが格納されてよい。ノンスデータは、特定の認証イベント（例えば取引）のために、ユーザまたはユーザデバイスと関連付けられてよい。ノンスデータは、（例えば、繰返しの危険が、１％、０．５％、０．１％、０．０５％、０．０１％、０．００５％、０．００１％、０．０００５％、０．０００１％、０．００００５％、０．００００１％、０．０００００５％、または０．０００００１％以下

といった）繰り返し現れる可能性が極めて低いデバイスの条件またはパラメータに関する情報から個別にまたは組み合わせて導出されてよく、またはこれらの情報を含んでもよい。ノンスデータは、この特定の時点または時間間隔におけるデバイスの特異値を表すことができる。

【０１９４】

[0202] 識別データおよびノンスデータを含む封印された認証パラメータは、図５に説明されたような１つまたは複数のデータベースに格納されてよい。

【０１９５】

[0203] ユーザの様々な認証活動中に、様々なタイプの情報（例えば、財務情報、ユーザ情報、デバイス情報、および／またはノンスデータ）が取得され、第１の外部デバイス９５０ａのデータベースに格納されてよい。第１の外部デバイスは、様々なタイプの情報を格納するためのデータベースまたはデータベースのサブセットにアクセスできてよい。様々なタイプの情報は、ユーザの初期登録中に、第１の外部デバイス（例えば認証サーバシステム）で取得され、格納されても、されなくてもよい。いくつかの実施形態において、様々なタイプの情報は、第１の外部デバイスによってアクセス可能であってよい。例えば、第２の外部デバイス（例えば、第三者エンティティ）９２０は、様々なタイプの情報を格納するための同じデータベースまたは同じデータベースのサブセットにアクセスできても、できなくてもよい。

【０１９６】

[0204] 第２の外部デバイス９２０は第三者エンティティであってよく、またこのエンティティに属してもよい。第三者エンティティは、１つもしくは複数のスタンドアロンのデータ処理装置、またはコンピュータの分散ネットワーク上に実装されてよい。いくつかの実施形態において、エンティティは、根本的なコンピューティングリソース、および／またはインフラストラクチャリソースを提供する、第三者のサービス提供者（例えば、第三者のクラウドサービス提供者）の様々な仮想デバイスおよび／またはサービスを用いることもできる。いくつかの実施形態において、ユーザの承認時に、および関連するプライバシポリシに従って、第三者の取引エンティティは、ユーザと関連付けられたカード情報、アカウント情報、使用データ、ノンスデータ、および／またはデバイス情報を格納しても、しなくてもよい。１つまたは複数の第三者の取引エンティティは、ｅコマースシステム、小売システム、金融機関（例えば、銀行、仲介者、およびクレジットカード会社）、商人のシステム、ソーシャルネットワーキングプラットフォーム、ならびに／またはユーザが認証を行う他のエンティティを含むことができる。いくつかの例において、第三者エンティティはオンラインｅコマースであってよく、ユーザのデバイスに関するユーザのノンスデータは、オンラインで製品の購入を完了するか、または拒否するために分析されてよい。いくつかの例において、第三者エンティティは仲介者システムであってよく、ノンスデータは、ユーザの金融口座と仲介者システムとの間の資金の移送を確認するために分析されてよい。いくつかの例において、第三者エンティティは、複数のユーザアカウントを管理するソーシャルネットワーキングプラットフォームであってよい。ユーザは、ソーシャルネットワーキングプラットフォームへのユーザのログインを確認するためにノンスデータを使用することができる。

【０１９７】

[0205] 前述のように、第１の外部デバイス９５０ａおよび第２の外部デバイス９５０ｂによってアクセスできるデータは同じであってよく、または相違してもよい。いくつかの実施形態において、第１の外部デバイスは、比較的大量のデータにアクセスでき得る認証システムであってよく、および／または第２の外部デバイスは、比較的少量のデータにアクセスでき得る第三者エンティティであってよい。第１の外部デバイスおよび第２の外部デバイスは両方、ノンスデータ、および／または任意の認証イベント関連データ（例えば取引データ）にアクセスできてよい。一方、第１の外部デバイスはノンスデータを取得できてよいが、第２の外部デバイスはノンスデータにアクセスできなくてよく、または逆もまた同様である。任意選択により、認証イベント関連データまたはそのサブセットは、第

１の外部デバイスおよび／もしくは第２の外部デバイスの両方によって、または第１の外部デバイスもしくは第２の外部デバイスのうちのただ１つによって取得されてよい。

【０１９８】

[0206] 外部デバイス９５０ａおよび９５０ｂは、１つまたは複数の物理トークン９６０ａ、９６０ｂ、９６０ｃ、９６０ｄをユーザに提供するエンティティであっても、なくてもよい。外部デバイスは、ユーザを確認または認証するために識別データを解読する必要があっても、なくてもよい。いくつかの実施形態において、外部デバイス９５０ａおよび９５０ｂは、ユーザがスキャンするためにディスプレイデバイス上にグラフィカルコード９７０ｄを提供するエンティティであってよい。グラフィカルコード（例えばQRコード）は、ユーザデバイス上で動く認証システムによって提供される認証済アプリケーションによってのみ読み取られ得るように独自のものであってよい。いくつかの例において、認証システムまたは認証アプリケーションだけが、グラフィカルコードを暗号化／解読することができる。グラフィカルコードは、ユーザを認証するための静的トークンとして使用され得る識別情報をエンコードすることができる。コードがユーザデバイス９００ｄによってスキャンされると、ノンスデータは自動的に生成され、詐欺行為の検出のために使用されてよい。

【０１９９】

[0207] １つまたは複数のユーザデバイスからのデータ９４０ａ、９４０ｂ、９４０ｃ、９４０ｄは、前述のように、第１の外部デバイスおよび／または第２の外部デバイスによってアクセスできてよい。１つまたは複数のユーザデバイスからのデータは、ノンスデータおよび識別データ、ならびに／またはノンスデータを導出もしくは生成するために使用され得るデバイスの条件もしくはパラメータに関するデータを含むことができる。例えば、認証イベントに関して、ユーザデバイスは、対応するノンスデータおよび／または認証イベント関連情報を送ることができる。データは、認証イベントに応じて送られてよい。データは、ユーザデバイスによって送りつけられてよく、または第１の外部デバイスまたは第２の外部デバイスによって取り出されてもよい。データはリアルタイムに送られてよい。一方、データは定期的に、またはスケジュールに応じて送られてよい。いくつかの実施形態において、ユーザデバイスは、画像デバイスの状態、または他の場所で（例えば、第１の外部デバイスおよび／もしくは第２の外部デバイスで）ノンスデータを生成するために使用され得る静的トークンのキャプチャ画像データの状態に関するデータを送ることができる。画像デバイスおよびキャプチャ画像データの状態に関するデータは本明細書の他の場所で説明されるようなものである。画像デバイスおよびキャプチャ画像データの状態に関するデータは、デバイスに搭載されていない１つまたは複数のプロセッサを用いて収集されたデータを含むことができる。いくつかの実施形態において、画像デバイスおよび画像データの状態に関するデータは、デバイスに搭載されている、または搭載されていない、１つまたは複数のセンサおよびプロセッサからの未加工のデータまたは事前処理されたデータを含むことができる。

【０２００】

[0208] 様々な実施形態による、セキュア認証を行う工程が実装されてよい。認証のリクエストは、ユーザ側で始められてよい。いくつかの実施形態において、ユーザは、取引を完了させるためにセキュア認証のリクエストを始めることができる。例えば、取引またはログイン処理中に、ユーザは、取引またはログイン処理のセキュア認証を始めるというユーザの意図を示すために、（例えば、ボタンを押すこと、またはユーザデバイスのタッチスクリーンに触れることによって）ユーザ入力を送ることができる。いくつかの実施形態において、セキュア認証イベントのリクエストは、ユーザデバイスから始められてよい。いくつかの例において、セキュア認証のリクエストは、認証サーバシステムなどの外部デバイスから始められてよい。いくつかの例において、セキュア認証のリクエストは、第三者エンティティから始められてよい。

【０２０１】

[0209] 認証サーバシステムによるユーザアカウントの初期登録中に、ユーザは、このユ

ーザアカウントと関連付けられた活動のセキュア認証を要求するための関連アカウント設定の登録をすることができる。後続の活動中、認証サーバシステムは、ユーザアカウントと関連付けられた取引またはログイン処理のリクエストを認識することができる。取引のリクエストに応答して、認証サーバシステムは、取引またはログイン処理を完了させるために、セキュア認証のリクエストを送ることができる。登録中および／または後続のアカウント活動中に、ユーザは、すべての活動または一定の条件を伴ういくつかの活動の認証を要求できるように登録することができる。

【０２０２】

[0210] 第三者エンティティによるユーザアカウントの初期登録中に、ユーザは、このユーザアカウントと関連付けられた活動のセキュア認証を要求するための関連アカウント設定の登録をすることができる。例えば、銀行のウェブサイトで、または銀行のアプリケーションの中で、カードを有効化または管理するためのユーザアカウントの初期セットアップ中に、ユーザは、１つまたは複数の取引のセキュア認証を行うことを選択することができる。後続の取引中に、第三者の取引エンティティが、ユーザアカウントと関連付けられた取引がリクエストされたと認識すると、カードを使用してこの取引を完了させるためにセキュア認証が要求される。登録中、および／または後続のアカウント活動中、ユーザは、すべての活動または一定の条件を伴ういくつかの活動の認証を要求できるように登録することができる。

【０２０３】

[0211] セキュア認証は、本明細書の他の場所で説明されるような、ノンスデータおよび識別データの分析を要求することができる。セキュア認証は、１つまたは複数の活動に対する、認証サーバシステムによるオプションとして要求されるか、または行われてよい。いくつかの実施形態において、セキュア認証は第三者エンティティによって要求されてよい。例えば、銀行システムまたは仲介者システムは、すべてまたは一定の取引（例えば、注意を向けられた取引、所定の限度額を上回る取引、またはランダムに選択された取引）を完了させるために、セキュア認証が行われることを要求することができる。いくつかの例において、セキュア認証は任意選択でよいが、取引を完了させるためにユーザがセキュア認証を行うことを選ぶ場合、第三者エンティティは報酬金（例えば、キャッシュバック、またはボーナスの報酬金ポイント）をユーザに提供することができる。

【０２０４】

[0212] セキュア認証は、ユーザアカウントと関連付けられたすべての活動、またはいくつかの活動に対して要求されてよい。例えば、セキュア認証は、取引が所定の閾値の金額以上の金額を伴うときに要求されてよい。例えば、所定の閾値の金額は、＄１００、＄２００、＄５００、＄１０００、＄５０００、＄８０００、＄１０，０００、＄１５，０００、＄２０，０００であってよい。閾値の金額は、ユーザ、認証サーバシステム、または第三者エンティティによって判断されてよい。いくつかの実施形態において、セキュア認証は、活動が高リスク活動として識別されるときに要求されてよい。例えば、高リスク活動は、ユーザアカウントと関連付けられた疑わしい／ミスマッチのユーザアイデンティティ、疑わしい取引場所、間違ったユーザ情報の繰返し入力、および／または以前に関連付けられた詐欺的な有効化に対する注意を向けられたユーザアカウントを伴うことがある。いくつかの実施形態において、高リスク活動は、短時間に資金が移送されることを要求することなどの、高速取引を伴うことがある。高速取引が識別されると、ノンスデータ分析などのさらなるセキュリティチェックがユーザから要求されてよい。いくつかの例において、さらなる認証の使用は、以前に直接会う活動が必要とされた局面でオンライン活動が発生できるようにすることができる。ユーザのアイデンティティのさらなる保証は、さらに大きいスケールの取引を許可する際に、エンティティに安心を与えることに役立つことがある。

【０２０５】

[0213] 識別データと組み合わされたノンスデータは、第三者エンティティと金銭、商品、および／またはサービスをやりとりする取引の認証を行うために使用されてよい。例え

ば、ユーザは、ユーザデバイス（例えば、タブレットまたは携帯電話）を使用して、第三者エンティティ（例えばｅコマース）からオンラインで品物を購入することができる。ユーザは、第三者エンティティと関連付けられたウェブサイト上で、またはアプリケーションの中で認証を行うことができる。

【０２０６】

[0214] １つの例において、購入するために所望の品物を選択し、取引に要求される情報（例えば、品物の所望の量および関連ユーザ情報）を入力した後、ユーザは、セキュア認証を行うように促されてよい。例えば、ユーザが＄１０００の価格の品物を購入したいと思うとき、ユーザは、セキュア認証を要するユーザデバイスのディスプレイ上で通知を受け取ることができる。通知は、取引のためにノンスデータを生成させるユーザのＩＤカード上のＰＤＦ４１７コードなどの物理トークンを、ユーザがスキャンすることを要求することができる。ＰＤＦ４１７コードからの識別データは、ユーザを確認または認証するために使用されてよい。ノンスデータは、ノンスデータが繰り返し現れていないことを確かめるために、同じ物理トークンと関連付けられた履歴上のノンスデータと比較されてよい。ノンスデータが繰り返し現れている場合、さらなる認証チェックが要求されてよく、または詐欺的イベント（例えばリプレイアタック）のさらに高い見込みがあるという注意が促されてもよい。これは、取引を拒否させるか、または遅らせても、そうでなくてもよい。

【０２０７】

[0215] 他のいくつかの例において、ユーザは、公共サービス、オンライン投票システム、ソーシャルネットワーキングサービス、等など、ウェブサイト上、またはアプリケーションの中で、登録されたユーザアカウントにログインすることができる。ユーザは、ログイン処理中に、本人確認など、セキュア認証を行うように通知を受け取ることができる。通知は、取引のためにノンスデータを生成させるユーザの文書上のグラフィカルコードなどの物理トークンをユーザがスキャンすることを要求することができる。グラフィカルコードからの識別データは、ユーザを確認または認証するために使用されてよい。ノンスデータは、ノンスデータが繰り返し現れていないことを確かめるために、同じ物理トークンと関連付けられた履歴上のノンスデータと比較されてよい。物理トークンが確認され、詐欺行為の指示がないことをノンスデータが示す場合、本人確認は完了されてよい。

【０２０８】

[0216] いくつかの実施形態において、第三者エンティティは、第三者エンティティの要求ごとに、または第三者エンティティによって登録されたユーザアカウント設定ごとにセキュア認証を行うリクエストを生成することができる。第三者の取引エンティティは、表示のためにユーザデバイスにリクエストを送ることができる。リクエストは、グラフィカルユーザインターフェース上に表示されるＱＲコードなどのグラフィカルコードを、ユーザがスキャンするように促すことができる。ノンスデータは、ＱＲコードのスキャンと共に生成され、認証のために使用されることになるコードで封印されてよい。

【０２０９】

[0217] ログイン処理または他の任意のタイプの認証イベント中に、認証サーバシステム、第三者エンティティ、またはユーザによってセキュア認証が要求されてよい。リクエストに応答して、静的トークンに対するノンスデータが収集され、および／または分析されてよい。静的トークンと組み合わされたノンスデータはユーザデバイスから取得され、認証サーバシステムおよび／または第三者エンティティに直接的または間接的に伝送されてよい。ユーザデバイス情報（例えばユーザデバイス識別子）は、認証サーバシステムおよび／または第三者エンティティに確認のために伝送されてもよい。

【０２１０】

[0218] 認証サーバシステムは、認証のために使用され得る様々な履歴上の認証情報または登録情報を格納してよく、またはこれらの情報にアクセスできてもよい。情報は、履歴上のノンスデータ、取引データ、ユーザアカウント情報、ユーザデバイス識別子、または本明細書の他の場所で説明されるような他の任意のタイプの情報を含むことができるが、

これらに限定されない。第三者エンティティは、履歴上のノンスデータ、取引データ、ユーザアカウント情報、ユーザデバイス識別子、または本明細書の他の場所で説明されるような他の任意のタイプの情報など、認証のために使用され得る履歴上の認証情報または登録情報の様々なセットを格納してよく、またはこれらのセットにアクセスできてもよい。

【０２１１】

[0219] 認証は、認証サーバシステム単独で、または第三者エンティティ単独で行われてよい。いくつかの例において、認証は、組み合わされた手法で両方のシステムによって行われてよい。例えば、ユーザアカウント情報またはユーザデバイス識別子などのいくつかの情報が、第三者の取引エンティティにおいて確認されてよい。一方で、ノンスデータなどの他の情報は、認証サーバシステムで確認されてよい。

【０２１２】

[0220] いくつかの例において、第三者エンティティは、ノンスデータなどのユーザの他の秘密情報および／または財務情報にアクセスできないが、ユーザアカウント情報だけを格納してよく、またはこれらの情報だけにアクセスできてもよい。したがって、第三者エンティティによる認証が認証を要するとき、第三者エンティティは、認証を行うために認証サーバシステムを指定することができる。認証サーバシステムは次に認証を行い、認証が承認されるか否かを示すメッセージを第三者の取引エンティティに返すことができる。認証サーバは、特定の認証イベントに対するノンスデータの分析に基づいてメッセージを返すことができる。取引は次に、第三者エンティティによって適宜承認されるか、または拒絶されてよい。

【０２１３】

[0221] いくつかの実施形態において、認証システムの中で、認証サーバシステムは任意選択であってよい。別々の第三者エンティティは、認証のいずれかの工程またはすべての工程を行うことができる。

【０２１４】

[0222] いくつかの実施形態において、認証サーバシステムは、異なる活動に対する複数の認証に対する認証を同時に行うことができる。認証サーバシステムは、複数の別々の第三者エンティティに対して認証を同時に行うことができる。認証サーバシステムに格納された、またはアクセス可能な情報は、様々な第三者エンティティと関連付けられた複数の取引にわたって収集されてよい。例えば、様々な第三者エンティティと関連付けられたノンスデータは、認証サーバシステムによってアクセス可能であってよい。これは、認証を行う際に、複数の取引から集められたインテリジェンスを使用できるようにする。認証サーバシステムは、第三者エンティティが個別にアクセスできることのないデータリポジトリにアクセスできてよい。

【０２１５】

[0223] 認証サーバシステムおよび／または第三者エンティティは、受け取られた情報を分析し、履歴上の認証および／または登録から取得された対応情報と受け取られた情報を比較することができる。比較は、ノンスデータの比較を含むことができる。ユーザログインまたは取引は、比較結果に基づいて、承認されるか、拒絶されるか、またはリスク認証／ログインとして注意を向けられてよい。ログインまたは認証が、承認されるか、拒絶されるか、または注意を向けられると、ユーザは、認証サーバシステムまたは第三者エンティティによって通知されてよい。

【０２１６】

[0224] 収集データと履歴上の認証データまたは登録データとの間のマッチを評価するために、様々な実施形態が存在してよい。いくつかの例において、カードリーダから収集されたデータが、対応する履歴上の認証データまたは登録データにマッチするとき、認証を承認する第三者の取引エンティティにメッセージが送られてよい。いくつかの例において、ノンスデータ（および／またはノンスデータの１つまたは複数のノンスファクタ）がマッチしない場合、認証は承認されてよい。

【０２１７】

[0225] 例えば、収集されたノンスデータは、ユーザおよび／または物理トークンと関連付けられたノンスデータの以前に格納されたセットとは少なくともわずかに異なる必要があることがある。いくつかの例において、完全な１００％マッチは疑わしいことがある。例えば、認証を行うために物理トークンが影像をつくられるたびに、いくつかの小さな変化がある可能性がある。物理的に、画像デバイスおよび画像データが正確に同じ条件および特性を有する可能性は極めて低い。全く同じ条件および特性を有することは、一種のリプレイアタックの指標であることがある。

【０２１８】

[0226] ノンスデータの分析（および任意選択により、他のファクタの追加分析）を含み得る認証分析に応じて、詐欺行為の指示が提供されてよい。詐欺行為の指示はリプレイアタックの指示に関連してよい。前述のように、詐欺行為の指示は、詐欺行為のリスクのレベルを示すことができる。詐欺行為のリスクのレベルは任意選択により、ノンスデータの分析に依存してよい。詐欺行為のリスクのレベルは、収集されたノンスデータが履歴上のノンスデータにマッチするかどうかに依存してよい。詐欺行為のリスクのレベルは、どれだけ密接にノンスデータが履歴上のノンスデータにマッチするか、および／またはどのノンスファクタがマッチするかに依存してよい。例えば、ノンスデータがすべてのファクタに対して１００％完全にマッチする場合、詐欺行為のリスクのレベルは非常に高くなり得る。ノンスデータが大部分マッチするが、ノンスファクタのうちの１つが異なる場合、詐欺行為のリスクのレベルは適度になり得、ノンスファクタのほとんどがマッチするか、またはどれもマッチしない場合、詐欺行為のリスクのレベルは低くなり得る。詐欺行為のリスクのレベルは、ノンスデータがどれだけ高くマッチするかに比例してよい。比較的高いマッチ（例えば、比較的多くのファクタがマッチする）は、詐欺行為の比較的高いリスクに相関してよく、比較的低いマッチは、詐欺行為の比較的低いリスクに相関してよい。

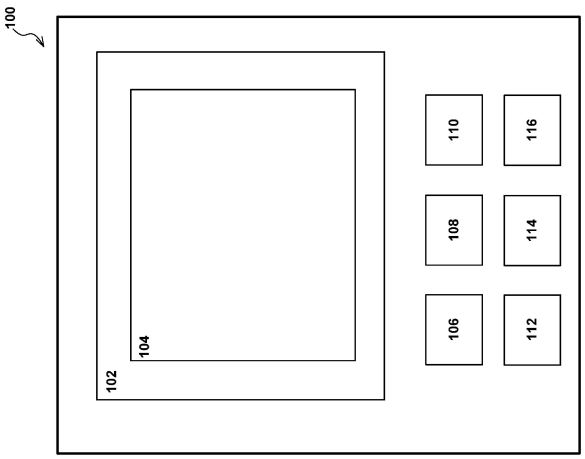
【０２１９】

[0227] いくつかの実施形態において、ノンスデータの分析は、リプレイアタックの見込みに関連してよい。他のタイプの詐欺行為分析は、取引に対して発生してよい。例えば、詐欺行為分析は、リプレイアタック、ならびに他のタイプの詐欺的攻撃（例えば、フィッシング、介入者攻撃、等）の見込みの評価を含むことができる。ユーザデバイス、ユーザアカウント、取引データ、または本明細書の他の場所で説明される他の任意のタイプのデータに関するデータなどの他のデータが、様々なタイプの詐欺行為を検出するために分析されてよい。詐欺行為分析に応じて、認証は、ユーザおよび／またはユーザデバイスに対して確かめられても、確かめられなくてもよい。これは任意選択により、取引を完了させることを許可するか、または取引を遅らせるか、もしくは拒否することができる。

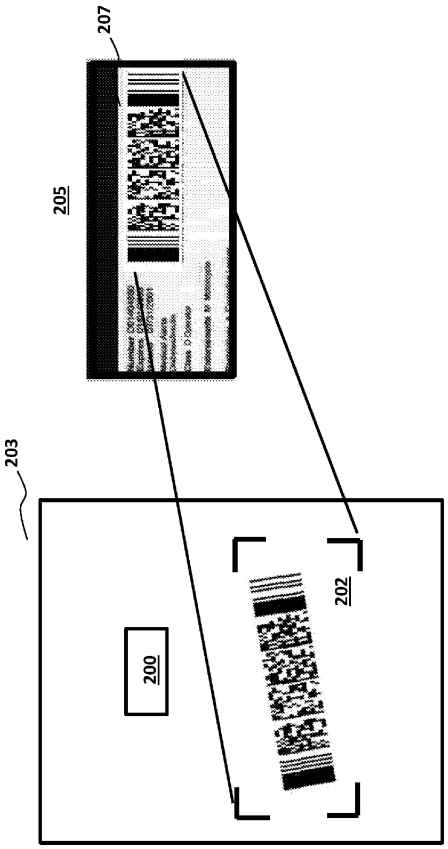
【０２２０】

[0228] 特定の実装形態が示され、説明されたが、様々な修正がこれらの実装形態に行われてよく、本明細書で想定されるということを前述から理解されたい。本明細書の中で提供された具体例によって本発明が限定されることを意図するものでもない。本発明は、前述の明細書を参照しながら説明されたが、本明細書における好ましい実施形態の説明および例証は、限定的な意味で解釈されることを意味するものではない。さらに、本発明のすべての態様は、様々な条件および変動要素に依存する、本明細書で示された特定の描写、構成、または相対的な比率に限定されないということが理解されよう。本発明の実施形態の形式および詳細の様々な修正は、当業者には明らかであろう。したがって、本発明は、このような任意の修正、変形、および均等物もカバーするということが想定される。

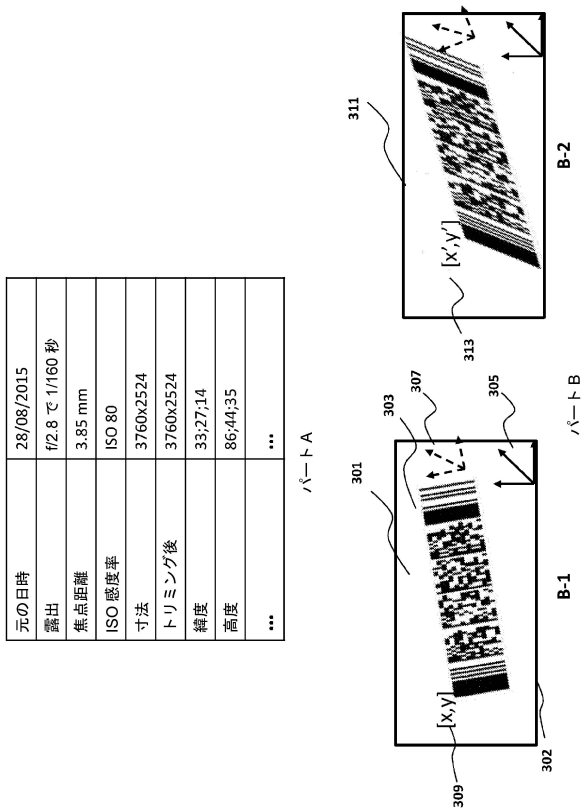
【図１】


100
102
104
106
108
110
112
114
116

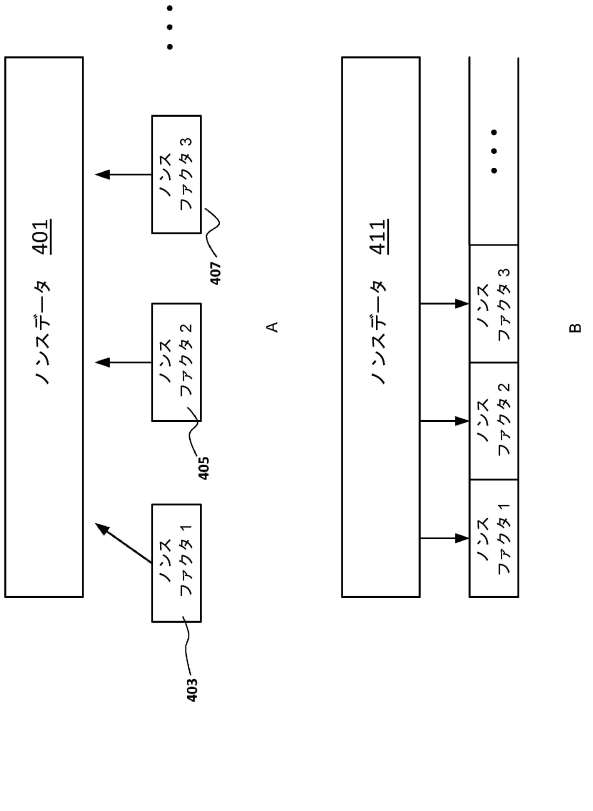
【図２】


207
205
203
200
202

【図３】


元の日時 28/08/2015
露出 f/2.8 で 1/160 秒
焦点距離 3.85 mm
ISO 感度率 ISO 80
寸法 3760x2524
トリミング後 3760x2524
緯度 33;27;14
高度 86;44;35
... ...
パート A
311
[x',y']
313
B-2
303
307
305
301
[x,y]
309
302
B-1
パート B

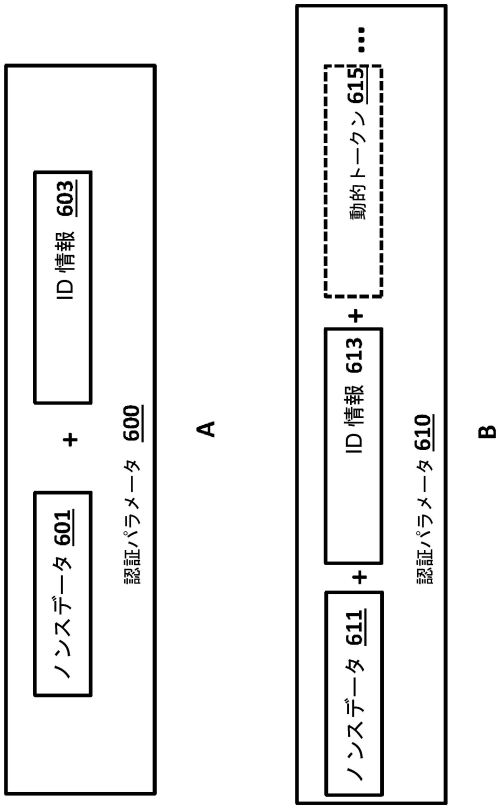
【図４】


ノンスデータ 401
ノンス ファクタ 1
ノンス ファクタ 2
ノンス ファクタ 3
403
405
407
A
ノンスデータ 411
ノンス ファクタ 1
ノンス ファクタ 2
ノンス ファクタ 3
B

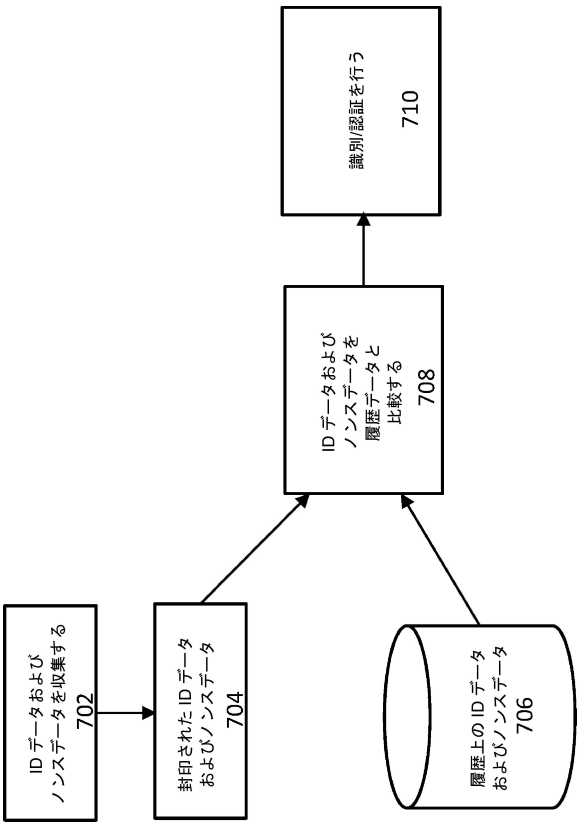
【図５】

取引ID 501	識別データ 503	ノンスデータ 505
TID 1	ID 1	ND 1
TID 2	ID 2	ND 2
TID 3	ID 1	ND 3
TID 4	ID 2	ND 2
…	…	…

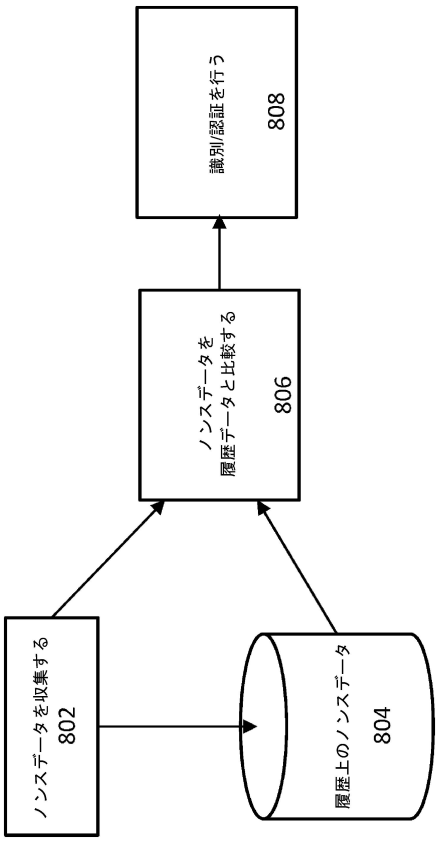
【図６】



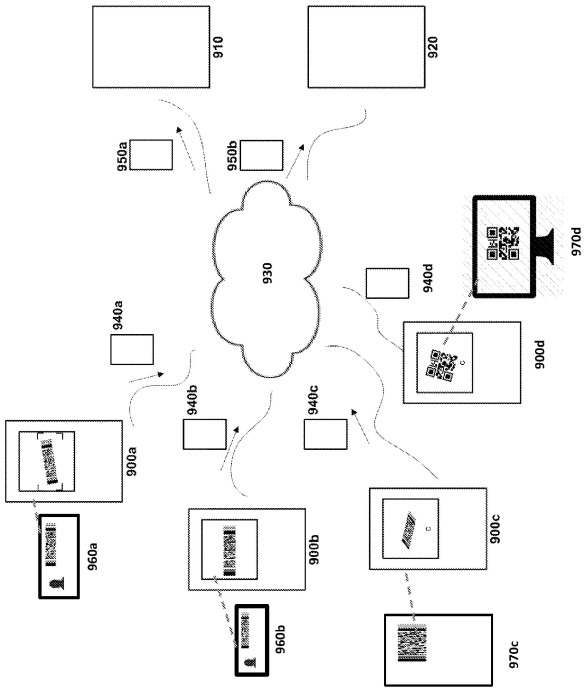
【図７】



【図８】



【図９】


910
920
950a
950b
930
940d
970d
940a
900d
940b
940c
900a
960a
900b
900c
960b
970c

フロントページの続き

(72)発明者　アイゼン，オリ
アメリカ合衆国，アリゾナ州　８５２５８，スコッツデール，ノース　ヴィア　デ　ラ　エスクエラ　７５０１
(72)発明者　レンゼルージギック，クレイトン
アメリカ合衆国，アリゾナ州　８５２５５，スコッツデール，イースト　サンダーホーク　ロード　７６９５
(72)発明者　マングーティツ，ニコラス
アメリカ合衆国，ケンタッキー州　４０５０５，レキシントン，コール　ドライブ　２１５６

審査官　平井　誠

(56)参考文献　特開２０１６－１３６３５２（ＪＰ，Ａ）
特開２００５－１４８９８２（ＪＰ，Ａ）
米国特許出願公開第２０１１／０２１９４２７（ＵＳ，Ａ１）
特開２００２－２５９３４５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／００－８８