(19)日本国特許庁(JP)

# (12)特許公報(B2)

(11)特許番号
特許第7092911号
(P7092911)

(45)発行日　令和4年6月28日(2022.6.28)

(24)登録日　令和4年6月20日(2022.6.20)

(51)国際特許分類

| | | | |
|---|---|---|---|
| *Ｇ０６Ｑ　20/40　(2012.01)* | Ｇ０６Ｑ | 20/40 | |
| *Ｇ０６Ｑ　20/32　(2012.01)* | Ｇ０６Ｑ | 20/32 | ３３０ |

FI

請求項の数　5　（全22頁）

(21)出願番号　特願2021-35533(P2021-35533)
(22)出願日　令和3年3月5日(2021.3.5)
(62)分割の表示　特願2019-529606(P2019-529606)の分割
原出願日　平成29年12月25日(2017.12.25)
(65)公開番号　特開2021-89774(P2021-89774A)
(43)公開日　令和3年6月10日(2021.6.10)
審査請求日　令和3年3月5日(2021.3.5)
(31)優先権主張番号　201710001426.2
(32)優先日　平成29年1月3日(2017.1.3)
(33)優先権主張国・地域又は機関
中国(CN)

(73)特許権者　520015461
アドバンスド ニュー テクノロジーズ カンパニー リミテッド
英国領ケイマン諸島 グランド ケイマン ケーワイ１－９００８ ジョージ タウン ホスピタル ロード ２７ ケイマン コーポレート センター
(74)代理人　100099759
弁理士　青木 篤
(74)代理人　100123582
弁理士　三橋 真二
(74)代理人　100092624
弁理士　鶴田 準一
(74)代理人　100114018
弁理士　南山 知広

最終頁に続く

(54)【発明の名称】　携帯装置において利用されるスキャンアンドペイ方法と装置

(57)【特許請求の範囲】

【請求項１】

携帯装置のためのスキャンアンドペイ方法であって、

前記携帯装置のオペレータの支払要求を受信することと、

前記支払要求に基づいて、下記の情報、

複数の数字の中から選択された冗長な値と、

支払口座と関連付けられている第１情報と、

前記オペレータの行動的生体認証特質と、前記携帯装置に記録されている履歴行動的生体認証特質と関連付けられている第２情報と、を少なくとも含んでいる支払コードを生成すること、を備え、

前記第２情報は、前記オペレータは前記携帯装置の所有者かどうかの判定結果を含んでおり、前記判定結果は、

前記オペレータの前記行動的生体認証特質と、前記携帯装置に記録されている前記履歴行動的生体認証特質との間の特質類似性を計算し、

前記特質類似性を予め設定された閾値と比較し、

前記特質類似性が予め設定された閾値よりも大きい場合、前記オペレータが前記携帯装置の所有者であると判定する、ことによって取得され、

前記支払要求に基づいて前記支払コードを生成することは、

前記冗長な値を変更することと、

前記第２情報と前記冗長な値とは異なる識別子の値との間の、予め設定された対応関係に

従って、前記支払要求に含まれている前記第２情報に対応する前記識別子の値を判定することと、
前記支払コードにおける少なくとも１桁が前記識別子の値に対応している前記支払コードを、前記識別子の値と前記冗長な値と前記第１情報を使用してバーコード画像として生成すること、を備えていることを特徴とする方法。
【請求項２】
前記行動的生体認証特質は、遠隔手続き呼出し（ＲＰＣ）要求記録、閲覧ログ、携帯装置を持つ姿勢、および指で押すときの特性の少なくとも１つを含んでいることを特徴とする請求項１に記載の方法。
【請求項３】
携帯装置のためのスキャンアンドペイ装置であって、
前記携帯装置のオペレータの支払要求を受信するための受信ユニットと、
前記支払要求に基づいて、下記の情報、
複数の数字の中から選択された冗長な値と、
支払口座と関連付けられている第１情報と、
前記オペレータの行動的生体認証特質と、前記携帯装置に記録されている履歴行動的生体認証特質と関連付けられている第２情報と、を少なくとも含んでいる支払コードを生成するための生成ユニットと、を備え、
前記第２情報は更に、前記オペレータは前記携帯装置の所有者かどうかの判定結果を含んでおり、前記判定結果は、
前記オペレータの前記行動的生体認証特質と、前記携帯装置に記録されている前記履歴行動的生体認証特質との間の特質類似性を計算し、
前記特質類似性を予め設定された閾値と比較し、
前記特質類似性が予め設定された閾値よりも大きい場合、前記オペレータが前記携帯装置の所有者であると判定する、ことによって取得され、
前記生成ユニットが、前記支払要求に基づいて前記支払コードを生成することは、
前記冗長な値を変更することと、
前記第２情報と前記冗長な値とは異なる識別子の値との間の、予め設定された対応関係に従って、前記支払要求に含まれている前記第２情報に対応する前記識別子の値を判定することと、
前記支払コードにおける少なくとも１桁が前記識別子の値に対応している前記支払コードを、前記識別子の値と前記冗長な値と前記第１情報を使用してバーコード画像として生成すること、を備えていることを特徴とする装置。
【請求項４】
携帯装置においてスキャンアンドペイを実行するために利用されるリスク制御装置であって、
前記携帯装置により提供される、下記の情報、
複数の数字の中から選択された冗長な値であって、支払コードが生成される前に値が変更される冗長な値と、
支払口座と関連付けられている第１情報と、
前記携帯装置のオペレータの行動的生体認証特質と、前記携帯装置に記録されている履歴行動的生体認証特質と関連付けられている第２情報と、を少なくとも含んでいる前記支払コードを取得するための取得ユニットと、
前記支払コードに含まれている前記第２情報に基づいて、サーバのリスク制御識別を起動するかどうかを判定するためのリスク制御処理ユニット、を備え、
前記第２情報は、前記オペレータは前記携帯装置の所有者かどうかの判定結果を含んでおり、前記判定結果は、
前記オペレータの前記行動的生体認証特質と、前記携帯装置に記録されている前記履歴行動的生体認証特質との間の特質類似性を計算し、
前記特質類似性を予め設定された閾値と比較し、

前記特質類似性が予め設定された閾値よりも大きい場合、前記オペレータが前記携帯装置の所有者であると判定する、ことによって取得され、
前記取得ユニットが、前記携帯装置により提供される前記支払コードを取得することは、前記携帯装置により提供されるバーコード画像をスキャンすることと、
前記支払コードに含まれている、前記支払口座と関連付けられている前記第１情報と、前記携帯装置の前記オペレータの前記行動的生体認証特質と、前記携帯装置に記録されている前記履歴行動的生体認証特質と関連付けられている前記第２情報を、前記支払コードとして生成された前記バーコード画像から抽出し、
前記第２情報と前記冗長な値とは異なる識別子の値との間の、予め設定された対応関係に従って、前記支払コードに含まれている前記第２情報に対応する前記識別子の値を判定すること、を備えていることを特徴とするリスク制御装置。
【請求項５】
前記第２情報は、前記オペレータの前記行動的生体認証特質と、前記携帯装置に記録されている前記履歴行動的生体認証特質との比較に基づく、前記オペレータは前記携帯装置の所有者かどうかの判定結果を含んでおり、
前記リスク制御処理ユニットが、前記支払コードに含まれている前記第２情報に基づいて、前記サーバにリスク制御要求を送るかどうかを判定することは、
前記支払コードに含まれている前記判定結果が、前記オペレータは前記携帯装置の前記所有者ではないということである場合、前記サーバの前記リスク制御識別を誘発することを備えていることを特徴とする請求項４に記載のリスク制御装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本願は、インターネット技術の分野に関し、特には、携帯装置において利用されるスキャンアンドペイ方法と装置に関する。
【背景技術】
【０００２】
オフラインスキャンアンドペイは徐々に、支払方法の主流になってきた。現在では、典型的なオフラインスキャンアンドペイのフローは、ユーザの支払要求に応答して、クライアント上の支払コードを生成することと、業者が、スキャン装置を使用してクライアント上の支払コードにおける情報を読み、業者のネットワークを介して、その情報をサーバにアップロードすることと、サーバが、リスクがないかどうかのリスク制御スキャンを実行して、ユーザに更なる検証のためにオンラインになるように要求し、スキャンの結果、リスクがなければ、業者とユーザに、取引は承認されたことを通知すること、を備えている。
【０００３】
そのような支払方法は、３つの特徴を有する必要がある。第１に、支払速度は、ユーザの体験を満足させることを確実にするような速さである必要があり、そして、典型的な目標は、支払時間を最小限にすることである。第２に、送信するデータは小さいこと。ユーザが支払のために携帯装置を使用するときは、携帯装置は、ネットワークのない環境にあることがよくあるので、携帯装置は少量のデータしか送信できない。例えば、携帯装置は、クライアントにより生成されたバーコードを、データ送信を達成するために業者のスキャン装置に送信する。しかし、限られた量のデータしか送信できないということは、後続するリスク制御に対する問題を提起する。第３に、各支払は、支払の安全性を向上するために、リアルタイムのリスク制御を必要とする。
【０００４】
従って、現在の技術に係るオフライン支払方法は、リスク制御により使用される時間が、ユーザの体験と相反し、サーバによるリスク制御の行使と計算は、毎回大量のサーバリソースを消費し、これは更に、オフライン支払に対するユーザの体験を悪くすることになる。
【発明の概要】
【０００５】

上記のことに鑑み、本願の実施形態は、現在の技術に係るオフライン支払方法における、リスク制御に多くの時間がかかり、大量のサーバリソースを消費するという問題を解決するための、携帯装置において利用されるスキャンアンドペイ方法と装置を提供する。

【０００６】

本願の実施形態は、携帯装置において利用されるスキャンアンドペイ方法を提供し、方法は、

携帯装置のオペレータの支払要求を受信することと、

支払要求に基づいて、下記の情報、

支払口座と関連付けられている第１情報と、オペレータの行動的特徴を利用した生体認証特質（以降、行動的生体認証特質）と、携帯装置に記録されている履歴行動的生体認証特質と関連付けられている第２情報を少なくとも含んでいる支払コードを生成すること、を備えている。

【０００７】

本願は更に、携帯装置において利用されるスキャンアンドペイ装置を提供し、装置は、

携帯装置のオペレータの支払要求を受信するための受信ユニットと、

支払要求に基づいて、下記の情報、支払口座と関連付けられている第１情報と、オペレータの行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質と関連付けられている第２情報を少なくとも含んでいる支払コードを生成するための生成ユニットを備えている。

【０００８】

本願は更に、携帯装置においてスキャンアンドペイを実行するために利用されるリスク制御方法を提供し、方法は、

携帯装置により提供される、下記の情報、支払口座と関連付けられている第１情報と、携帯装置のオペレータの行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質と関連付けられている第２情報を少なくとも含んでいる支払コードを取得することと、

支払コードに含まれている第２情報に基づいて、サーバのリスク制御識別を起動するかどうかを判定すること、を備えている。

【０００９】

本願は更に、携帯装置においてスキャンアンドペイを実行するために利用されるリスク制御装置を提供し、装置は、

携帯装置により提供される、下記の情報、支払口座と関連付けられている第１情報と、携帯装置のオペレータの行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質と関連付けられている第２情報を少なくとも含んでいる支払コードを取得するための取得ユニットと、

支払コードに含まれている第２情報に基づいて、サーバのリスク制御識別を起動するかどうかを判定するためのリスク制御処理ユニットを備えている。

【００１０】

本願に係る上記の解決策は、下記の技術的効果を達成可能である。

【００１１】

第１は、リスク制御識別の高められた能力である。従来の支払リスク制御に対して、本願に係る技術的解決策は、リスク制御判定のために支払コードを介して、オペレータの行動的特徴を利用した生体認証情報（以降、行動的生体認証情報）に基づく識別結果をサーバに送信し、リスク制御システム全体が、より多い次元のデータを使用してリスクを精度よく判定することを可能にし、それにより、リスク制御の精度を向上する。

【００１２】

第２は、削減されたリスク制御解析コストである。サーバにおける従来のリスク制御に対して、本願に係る技術的解決策においては、オペレータの行動的生体認証情報に基づくリスク制御識別を端末装置が実行し、操作は同じ人間によるものであると判定されたときは、取引要求に対する、サーバにおけるリスク制御操作を不要にし、それにより、サーバリ

ソースの消費を大幅に削減する。
【００１３】
第３は、リスク制御に対する削減された時間である。オペレータの行動的生体認証情報に基づくリスク制御識別を端末装置が実行し、操作は同じ人間によるものであると判定されたときは、取引要求に対する、サーバにおけるリスク制御操作を不要にする。更に、このプロセスの間に行われる演算は、端末装置に任せる。従って、サーバにおける従来のリスク制御に対して、取引のこの部分に対するリスク制御に使用される時間は大幅に削減される。
【００１４】
第４は、向上されたリスク制御効率である。
【図面の簡単な説明】
【００１５】
本願の実施形態の技術的解決策または現在の技術を、より明確に記述するために、実施形態または現在の技術において使用される付随する図面を下記に簡単に記述する。下記の記述における付随する図面は、本願における単なる幾つかの実施形態に過ぎないということは明白である。これらの付随する図面に基づいて、通常の技量を有する当業者は、他の関連する図面を創造的努力なしに取得できる。
【００１６】
【図１】本願の幾つかの実施形態に係る、携帯装置のためのスキャンアンドペイ方法のフローチャートである。
【００１７】
【図２】本願の幾つかの実施形態に係る、携帯装置においてスキャンアンドペイを実行するためのリスク制御方法のフローチャートである。
【００１８】
【図３】本願の幾つかの実施形態に係る、携帯装置においてスキャンアンドペイを実行するためのリスク制御方法のフローチャートである。
【００１９】
【図４】本願の幾つかの実施形態に係る、携帯装置上のスキャンアンドペイ装置の模式的構造図である。
【００２０】
【図５】本願の幾つかの実施形態に係る、携帯装置においてスキャンアンドペイを実行するためのリスク制御装置の模式的構造図である。
【発明を実施するための形態】
【００２１】
支払分野における生体認証の適用は、ますます広範囲になっている。各生体学的個人は、測定可能な、または自動的に識別および検証可能な、固有の生理学的特性または行動的特性、つまり生体認証を有しており、それらの特性は、生理学的生体認証特質（例えば、目の特性、声紋、指紋、掌紋、心拍、脈拍、染色体、ＤＮＡ、咬口傷などであり、目の特性は、アイプリント（網膜上の血管パターン）、虹彩、目の強膜などの生体認証を含むことができる）と、行動的生体認証特質（例えば、歩き方、音声、筆跡、キーの打ち方、キーを押す力、電子装置を持つ姿勢、閲覧ログ特性、遠隔手続き呼出し（ＲＰＣ）プロトコル要求記録特性など）に分割できる。生体認証識別は、身元検証を完了するために、個人の固有な生体認証に基づいて個人を識別する。
【００２２】
生体認証の特徴は、身元検証において、簡単、迅速、安全で、信頼性があり、正確なため、支払の安全性の分野において、生体認証を適用する傾向がある。しかし、リスク制御効率を向上するために、どのように行動的生体認証特質を利用するかについては、対処されていない。
【００２３】
本願の目的を達成するために、本願の実施形態は、携帯装置のオペレータの支払要求を受

信するための携帯装置において利用されるスキャンアンドペイ方法と装置を提供し、支払要求に基づいて、支払口座と関連付けられている第１情報と、オペレータの行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質と関連付けられている第２情報を少なくとも含んでいる支払コードを生成する。このように、オペレータの行動的生体認証特質に関する情報と、携帯装置に記録されている履歴行動的生体認証特質に関する情報を、リスク制御判定のために支払コードを介してサーバに送信することが可能であり、それにより、リスク制御システム全体が、より多くの次元におけるデータを使用してリスクを精度よく判定し、リスク制御の精度を向上し、そのため、リスク制御識別の効率を向上することを可能にする。

【００２４】

本願の実施形態における行動的生体認証特質は、ＲＰＣ要求記録、閲覧ログ、携帯装置を持つ姿勢、および指で押すときの特性の少なくとも１つを含むことができるということに留意すべきである。

【００２５】

通常の技量を有する当業者が、本願の技術的解決策をより良好に理解することを可能にするために、本願の実施形態における技術的解決策を、本願の実施形態における付随する図面を参照して、下記に明確且つ完全に記述する。記述される実施形態は幾つかの例に過ぎず、本願のすべての実施形態ではないということは明白である。本願の実施形態に基づいて、通常の技量を有する当業者が、創造的努力なしに取得できるすべての他の実施形態は、本願の範囲に含まれるとする。

【００２６】

図１は、本願の幾つかの実施形態に係る、携帯装置において利用されるスキャンアンドペイ方法のフローチャートである。この方法を下記に記述する。

【００２７】

ステップ１０１：携帯装置のオペレータの支払要求を受信する。

【００２８】

例えば、オペレータが、支払要求を開始することが必要と判定すると、オペレータは、支払制御または、他の支払関連ページ要素を誘発することにより、支払要求を開始する。このとき、携帯装置におけるクライアントは、支払要求を受信する。

【００２９】

支払要求を受信したときに、支払要求を開始する前に、オペレータの一連の行動的生体認証特質を判定する必要があるということに留意すべきである。本願の実施形態においては、オペレータの行動的生体認証特質は、携帯装置に設置されている、携帯装置のオペレータの行動的生体認証特質を識別できるシステムまたは装置により収集でき、または、他の方法で取得でき、それは、明細書では制限されない。

【００３０】

携帯装置に設置されている、携帯装置のオペレータの行動的生体認証特質を識別できるシステムまたは装置は、明細書においては例として使用される。

【００３１】

行動的生体認証特質は、オペレータの行動的習慣をある程度反映し、一方、幾つかの行動的習慣は、ほとんどの状況において変化しない。システムまたは装置は、携帯装置を操作することで生成される、オペレータの行動的生体認証特質（ＢＢＳ）をリアルタイムで記録および監視できる。つまり、オペレータの身元は、オペレータの行動的生体認証特質を通して認識できる。

【００３２】

ユーザの閲覧ログを例に取ると、ある連続した期間においてユーザにより閲覧されたウェブサイトまたはウェブページの内容は、ユーザの個人的または職業的な好みを反映し、それは、ほとんどの状況において変化しない。ユーザの閲覧ログ挙動を監視することで、携帯装置上の行動的生体認証特質監視システムまたは装置が、最近のある期間においてユーザにより閲覧されたウェブサイトまたはウェブページの内容が大きく変化したことを見出

した場合、それは、ユーザが異常な閲覧ログ挙動を有することを示している。この時点で、携帯装置を使用するユーザが変わったと、つまり、携帯装置を現在使用しているユーザは、その携帯装置を以前使用していたユーザではないと結論可能である。

【００３３】

詳細な識別プロセスは、本願の注目する点ではない。本願の実施形態においては、行動的生体認証特質監視システムまたは装置は、オペレータの行動的生体認証特質を収集するために使用され、携帯装置に基づくリスク識別システムは、オペレータは携帯装置の所有者であるかどうかを判定し、サーバのリスク制御効率の目的のために、相反する特質を提供するために使用される。相反する特質は、最近の行動的生体認証特質と、履歴記録における行動的生体認証特質との差を反映しており、つまり、オペレータは携帯装置の所有者であるかどうかを、総合的な方法で評価可能である。

【００３４】

携帯装置のオペレータは、支払要求を開始する前に、典型的には、他のページを閲覧したり、スワイプ操作のような他の操作を携帯装置上で行い、これらの操作はすべて、オペレータの行動的生体認証特質と称することができる。従って、携帯装置上の行動的生体認証特質監視システムまたは装置は、オペレータが携帯装置上で他の操作を行うときに、リアルタイムでこれらの行動的生体認証特質を収集する。

【００３５】

行動的生体認証特質監視システムまたは装置がこれらの行動的生体認証特質を収集した後、収集された行動的生体認証特質は、指定された格納スペースに格納できるということに留意すべきである。行動的生体認証特質のライブラリは、指定された格納スペースにおいて維持でき、さまざまの時点において収集された、携帯装置を操作するオペレータの行動的生体認証特質は、行動的生体認証特質のライブラリに格納される。通常は、端末装置の指定された格納スペースに格納されている行動的生体認証特質は、ほとんどが、携帯装置の所有者の行動的生体認証特質であるべきである。または、指定された格納スペースのサイズによっては、最近監視された行動的生体認証特質（ここで「最近」とは、ある設定された期間を指すことができ、例えば、過去の週内に監視された行動的生体認証特質を指すことができる）を格納し、以前に収集された履歴行動的生体認証特質（過去の週以前に監視された行動的生体認証特質を指すことができる）はサーバに送り、または端末装置のハードディスクに格納できるが、これは、明細書では制限されない。

【００３６】

収集時間と、収集された行動的生体認証特質との間の対応関係は、行動的生体認証特質の上記のライブラリに格納されるということに留意すべきである。

【００３７】

ステップ１０２：支払要求に基づいて支払コードを生成する。

【００３８】

ここで、支払コードは、下記の情報、支払口座と関連付けられている第１情報と、オペレータの行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質と関連付けられている第２情報を少なくとも含んでいる。

【００３９】

本願の実施形態においては、支払要求を受信すると、クライアントは、支払要求に基づいて支払コードを生成する。

【００４０】

１つの例においてはまず、支払要求に基づいて、下記の情報、支払口座と関連付けられている第１情報と、オペレータの行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質と関連付けられている第２情報が判定される。

【００４１】

第１情報はここでは、支払口座と関連付けられている情報のことであり、つまり、口座識別子、口座名、口座番号、支払口座識別子、携帯装置の装置識別子、などであり、明細書においては詳述しない。

【００４２】
第２情報をここで更に記述する。本願の実施形態における第２情報は、オペレータの行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質と関連付けられている情報のことである。第２情報が判定される前に、支払要求を受信する前の、ある設定された期間において収集された行動的生体認証特質を判定する必要がある。
【００４３】
本願の実施形態においては、クライアントは、支払要求を受信したときの時間に従って、設定時間範囲を決めることができる。設定時間範囲に基づいてクライアントは、携帯装置の指定された格納スペースにおける設定時間範囲で収集された行動的生体認証特質を検索し、つまり、支払要求が開始される前に生成された、オペレータの行動的生体認証特質を取得する。
【００４４】
行動的生体認証特質を取得した後、第２情報を、行動的生体認証特質に基づいて取得できる。本願の実施形態における第２情報に含まれている情報は、相反する特質情報と称することができ、相反する特質情報は、端末装置におけるリスク識別モジュールによる計算で取得できるということに留意すべきである。そして、サーバが支払コードを取得すると、サーバは、支払コードに含まれている第２情報に従って、リスク識別を直接実行でき、それにより、リスク識別の間の、サーバリソースの消費が効果的に削減され、リスク識別全体の効率が向上される。
【００４５】
本願の実施形態における第２情報は、下記の幾つかの方法で判定できる。
【００４６】
第１の方法
支払要求が開始される前に生成されたオペレータの行動的生体認証特質を取得した後、オペレータの、取得された行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質に基づいて、オペレータは携帯装置の所有者かどうかを判定するために、比較操作を実行できる。
【００４７】
１つの例においては、取得したオペレータの行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質との間の特質類似性が計算され、この特質類似性に従って、オペレータは携帯装置の所有者かどうかが判定される。
【００４８】
特質類似性が、設定された閾値よりも大きい場合は、オペレータは携帯装置の所有者であることを示し、特質類似性が、設定された閾値よりも大きくない場合は、オペレータは携帯装置の所有者ではないことを示している。
【００４９】
第２情報は、オペレータは携帯装置の所有者がどうかの判定結果に基づいて取得でき、つまり、第２情報は、オペレータは携帯装置の所有者かどうかの判定結果を含み、判定結果は、オペレータは携帯装置の所有者であるか、またはオペレータは携帯装置の所有者ではないかの何れかである。
第２の方法
【００５０】
本願の実施形態における第２情報は、異なる情報の組み合わせの方法でも取得でき、つまり、一方では、オペレータは携帯装置の所有者であるかどうかの判定結果を含み、他方では、収集された行動的生体認証特質は、収集された行動的生体認証特質と履歴行動的生体認証特質に基づいて、異常であるかどうかの判定結果を含んでいる。そのような情報の組み合わせで、オペレータは携帯装置の所有者であるかどうかを精度良く識別可能である。
【００５１】
例えば、オペレータは携帯装置の所有者かどうかの判定結果に加えて、第２情報は更に、ＲＰＣ要求記録は異常かどうかの判定結果や、閲覧ログは異常かどうかの判定結果のよう

な、収集された行動的生体認証特質が異常かどうかの判定結果を含んでいる。

【００５２】

オペレータは携帯装置の所有者かどうかの判定結果が、単に「はい」または「いいえ」により表現される場合、携帯装置は、判定の精度の良い結果を取得するために、膨大な演算をする必要があり、それは、携帯装置が大量のリソースを消費する必要があることを意味する。携帯装置により出力される判定の結果を、相対的に精度の良いものにするために、本願の実施形態においては、異なる情報の組み合わせの方法を使用でき、つまり、オペレータは携帯装置の所有者である確率が計算され、そして、その確率は他の判定結果と組み合わされて、判定の結果の精度を確実にすることが可能で、更に、携帯装置により消費されるリソースを削減可能である。

【００５３】

例えば、オペレータは携帯装置の所有者である確率が、設定された閾値よりも低いと、第１の方法によれば、それは、オペレータは携帯装置の所有者でないことを示す。他の情報からの判定結果を考慮することにより、この結果を補正でき、そして、サーバによる後続する操作にも影響を与えることができる。

【００５４】

このように、サーバが支払コードを受信すると、サーバはもはや、オペレータは携帯装置の所有者かどうかを、第１の方法における判定の結果のみに基づいて識別することはせず、種々の情報間の相互の確証を通して行い、それは、リスク識別の効率と精度を向上することを支援可能である。

【００５５】

第１の方法において携帯装置により判定されるような、オペレータは携帯装置の所有者である確率が、オペレータは携帯装置の所有者かどうかを精度良く判定することが可能でない場合、支払コードが生成されるとき第２の方法において、第２情報を判定でき、これにより、オペレータは携帯装置の所有者かどうかの判定の精度を確実にすることが可能であるということに留意すべきである。

【００５６】

第２に、支払コードは、判定された第１情報と第２方法に基づいて生成される。

【００５７】

１つの例においては、取得された第１情報と第２情報は、支払コードを取得するために符号化される。

【００５８】

上記の第１の方法に対しては、第２情報は判定結果を含むので、オペレータは携帯装置の所有者であるという判定結果に対応する識別子の値は１であり、オペレータは携帯装置の所有者でないという判定結果に対応する識別子の値は０と仮定することが可能である。支払コードは、第１情報と、判定された識別子の値を使用する符号化を通して取得可能である。

【００５９】

このように、取得された支払コードに含まれる識別子の値が０の場合は、サーバは、オペレータは携帯装置の所有者でないと判定し、取得された支払コードに含まれる識別子の値が１の場合は、サーバは、オペレータは携帯装置の所有者であると判定する。結果として、サーバは大量の演算を行う必要がなく、オペレータの身元認識を、取得された支払コードに含まれる第２情報に基づくだけで完了可能であり、それにより、支払要求についてのリスク識別を達成する。

【００６０】

上記の第２の方法に対しては、第２情報は異なる情報の組み合わせを含むので、第２情報はまず、第２情報に対応する識別子の値を取得するための符号化の間に変換される必要がある。

【００６１】

第２情報をどのように変換するかを、第２情報が３つのタイプの情報、つまり、オペレー

タは携帯装置の所有者かどうかの判定結果と、ＲＰＣ要求記録は異常かどうかの判定結果と、閲覧ログは異常かどうかの判定結果を含んでいる例を使用して下記に記述する。

【００６２】

これら３つのタイプの情報は、３桁の２進数［Ｘ］［Ｙ］［Ｚ］に対応すると仮定し、ここにおいて、Ｘは、オペレータは携帯装置の所有者かどうかの判定結果に対応し、つまり、判定結果は、オペレータは携帯装置の所有者であるということである場合は、Ｘの値はｘ１であり、判定結果は、オペレータは携帯装置の所有者でないということである場合は、Ｘの値はｘ２である。

【００６３】

Ｙは、閲覧ログは異常かどうかの判定結果に対応し、つまり、判定結果は正常であるということである場合は、Ｙの値はｙ１であり、判定結果は異常であるということである場合は、Ｙの値はｙ２である。

【００６４】

Ｚは、ＲＰＣ要求記録は異常かどうかの判定結果に対応し、つまり、判定結果が正常であるということである場合は、Ｚの値はｚ１であり、判定結果が異常であるということである場合は、Ｚの値はｚ２である。

【００６５】

携帯装置は、異なる情報の判定結果に従う２進コードを取得可能である。２進コードは、第２情報に対応する識別子の値と称することができる。更に、２進コードはまた、１０進数に変換することもでき、そして、この１０進数は、第２情報に対応する識別子の値である。

【００６６】

支払コードが固有で安全であることを確実にするために、第２情報に対応する識別子の値は、ランダムな方法で判定できる。例えば、０から９の１０個の数字の中から１個の数字をランダムに選択して、この数字と［Ｘ］［Ｙ］［Ｚ］の間の対応関係に基づいて、ｘ１、ｘ２、ｙ１、ｙ２、ｚ１、およびｚ２の値を判定できる。１つの例においては、数字の選択の間、１～２個の数字を、０から９の１０個の数字からランダムに選択でき、つまり、選択された１～２個の数字は、符号化ノイズの増大を制御するための冗長な値として使用され、符号化の解決策が容易に破られないようにする。言い換えれば、冗長な値としての数字は、［Ｘ］［Ｙ］［Ｚ］との対応関係を確立するための数字としては選択不可である。

【００６７】

［Ｘ］［Ｙ］［Ｚ］は典型的には２進数であり、そしてこの２進数の値域は、０から７である。３つの次元を有する情報は、合計で８つの組み合わせ方法で組み合わせることができ、８個の数字は、０から９の１０個の数字から選択され、各組み合せ方法に割り当てられる。

【００６８】

例えば、上記の２値の符号化方法においては、操作は所有者によるものであり、ＲＰＣ記録は正常であり、閲覧ログは正常でると判定され、２値化の結果は［１］［０］［０］であり、１０進数への変換の結果は４である。これに対応して、符号化の間の、行動的生体認証特質を格納するための数字が４であれば、それは、「操作は所有者によるものであり、ＲＰＣ記録は正常であり、閲覧ログは正常であることが判定される」ことを表わしている。

【００６９】

符号化の間に各数字により表わされる組み合せの意味は、変更できるということを理解すべきである。例えば、上記の実現方法においては、数字の４は、「操作は所有者によるものであり、ＲＰＣ記録は正常であり、閲覧ログは正常であることが判定される」ということを表わし、０から９の任意の他の数字を、上記の意味を表わすために数字４と置き換えることができる。言い換えれば、対応関係は、上記の３つの判定の種々の可能な組み合わせと、すべての可能な値の間で確立する必要があるだけである。加えて、符号化ノイズと

しての冗長な値もまた変更できる。同時に、符号化の解決策における数字の意味と、冗長な値の構成への規則的または不規則的な変更は共に、コードを破ることにおける困難さを更に高めることができる。通常の技量を有する当業者は、本実現方法において列挙した行動的生体認証特質は、単に好適な例であり、携帯装置上で収集可能なすべての行動的生体認証特質はすべて、操作は所有者によるものかどうかの判定のための基準として使用できるということも理解すべきである。例示されていない幾つかの実現方法は更に、行動的生体認証特質に関する情報に基づいて、サーバにおいてリスク制御を開始するかどうかを判定するステップを備えている。

【００７０】

支払コードは固有で安全であることを確実にするために、識別子の値と第２情報との間の対応関係は、少なくとも部分的には、規則的または定期的に変更できる。または、支払コードが支払要求に基づいて生成される前に、識別子の値と第２情報との間の対応関係は、冗長な値の少なくとも１つを変更することにより調整される。このようにして、支払コードの安全性は確実にされる。

【００７１】

本願の幾つかの他の実施形態においては、方法は更に、

判定結果は、オペレータは携帯装置の所有者である確率は、設定された閾値よりも低いということであり、携帯装置がオフライン支払状態であると判定された場合、携帯装置のオペレータについてのオンライン身元確認を誘発することを備えている。

【００７２】

１つの例においては、携帯装置が、オペレータは携帯装置の所有者かどうかを判定するときに、携帯装置は、オペレータは携帯装置の所有者である確率を計算できる。確率が、設定された閾値より低い場合、それは、オペレータは携帯装置の所有者でない可能性が高いことを示し、また、高いリスクの存在も意味する。更に、この時点で携帯装置が、オフライン支払状態である場合、オペレータが、携帯装置のオペレータについてのオンライン身元確認を起動するように、催促メッセージで促すことができる。つまり、オペレータはオンライン支払要求を開始し、オンライン身元検証を行うことが要求される。

【００７３】

本願におけるスキャンアンドペイは、例えば、支払コードが携帯装置上で生成され、業者は、支払コードにおける情報をスキャン装置を使用して読み取り、その情報をサーバに送って支払を完了するというプロセスを意味している。

【００７４】

上記の内容によれば、支払コードは、業者がスキャンして、それにより更なる支払手順を完了するために携帯装置上で生成される。本願に係る支払方法では、ユーザの行動的生体認証特質に基づく判定結果は支払コードに符号化され、それは本質的には、補助的オフラインリスク制御方法である。このタイプのオフライン補助的リスク制御は、サーバに対するリスク制御スキャンの負担を大幅に削減可能であり、サーバにおけるリソースを節約可能であり、リスク制御に対する総時間を削減可能である。

【００７５】

本願におけるスキャンアンドペイ方法によれば、携帯装置のオペレータの支払要求が受信され、支払要求に基づいて、支払口座と関連付けられている第１情報と、オペレータの行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質と関連付けられている第２情報を少なくとも含んでいる支払コードが生成される。このようにして、オペレータの行動的生体認証特質に基づく識別結果が、リスク制御判定のために支払コードを介してサーバに送信され、それにより、リスク制御システム全体が、より多い次元でのデータを使用して精度よくリスクを判定し、リスク制御の精度を向上し、そのためリスク制御識別の効率を向上することを可能にする。

【００７６】

本願の実施形態に係るスキャンアンドペイ方法のオフライン支払における適用は、行動的生体認証特質に基づく端末装置による識別を実行し、それにより、オフライン支払の安全

性を確実にするだけでなく、サーバにおけるリスク制御のコストを削減し、オフライン支払リスク制御の効率を向上可能であるということに留意すべきである。

【００７７】

図２は、本願の幾つかの実施形態に係る、携帯装置においてスキャンアンドペイを実行するために利用されるリスク制御方法のフローチャートである。本願の実施形態における実行実体は、スキャナまたはサーバであってよい。実行実体がサーバの場合、そのサーバは、リスク識別を実行するためのサーバとは異なる。この方法を下記に記述する。

【００７８】

ステップ２０１：携帯装置により提供される支払コードを取得する。

【００７９】

ここで、支払コードは、少なくとも下記の情報を含んでいる。支払口座と関連付けられている第１情報と、携帯装置のオペレータの行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質と関連付けられている第２情報。

【００８０】

本願の実施形態においては、携帯装置により提供される支払コードを取得する方法は、携帯装置により提供される支払コードをスキャンするために、業者のスキャンガンを使用すること、または、携帯装置により提供される支払コードを受信するために、支払コード識別装置を使用することであってよく、それは明細書においては制限されない。

【００８１】

例えば、携帯装置により提供される二次元バーコード画像がスキャンされ、
支払コードに含まれている、支払口座と関連付けられている第１情報と、携帯装置のオペレータの行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質と関連付けられている第２情報が、二次元バーコード画像から抽出される。

【００８２】

つまり、携帯装置により提供される支払コードがスキャンされると、支払コードに含まれている情報を抽出可能である。

【００８３】

ステップ２０２：支払コードに含まれている第２情報に基づいて、リスク制御要求をサーバに送るかどうかを判定する。

【００８４】

本願の実施形態においては、支払コードに含まれている第２情報を取得するために、支払コードに対して、復号化操作が実行される。

【００８５】

第２情報が、オペレータは携帯装置の所有者かどうかの判定結果のみを含んでいる場合、第２情報に含まれている判定結果が、オペレータは携帯装置の所有者でないということであれば、リスク制御要求が誘発されてサーバに送られる。

【００８６】

第２情報に含まれている判定結果が、オペレータは携帯装置の所有者であるということであれば、支払要求に対する応答が誘発される。

【００８７】

第２情報が、異なる情報に関する判定結果の組み合わせを含んでいる場合は、オペレータは携帯装置の所有者である確率は、異なる情報に関する判定結果の組み合わせを通して判定される。

【００８８】

例えば、オペレータは携帯装置の所有者である確率は、オペレータは携帯装置の所有者かどうかを判定する確率と、閲覧ログは異常かどうかの判定結果と、ＲＰＣ要求記録は異常かどうかの判定記録を通して判定される。この場合、オペレータは携帯装置の所有者である確率が、設定された閾値よりも低いと、閲覧ログは異常と判定され、および／または、ＲＰＣ要求記録は異常と判定されたときは、オペレータは携帯装置の所有者である確率は、第２閾値よりも低いと判定可能であり、閲覧ログは正常と判定され、ＲＰＣ要求記録は

正常と判定されたときは、オペレータは携帯装置の所有者である確率は、第２閾値よりも低いが、第１閾値よりも高いと判定可能である。
オペレータは携帯装置の所有者である確率が、設定された閾値よりも高い場合、閲覧ログは異常と判定され、および／または、ＲＰＣ要求記録は異常と判定されたときは、オペレータは携帯装置の所有者である確率は、第１閾値よりも高くなく、第２閾値よりも高いと判定可能である。
閲覧ログは正常と判定され、ＲＰＣ要求記録は正常と判定されたときは、オペレータは携帯装置の所有者である確率は、第１閾値よりも高いと判定可能である。
【００８９】
下記の操作が、判定結果に対して実行される。
確率が第１閾値よりも高い場合、支払要求に対する応答を誘発する。
確率が第２閾値よりも低い場合、オペレータは携帯装置の所有者でないことを示し、サーバのリスク制御識別システムにリスク識別要求を送り、サーバのリスク制御識別操作を起動する。
確率が第１閾値よりも高くなく、第２閾値よりも高い場合、オペレータは携帯装置の所有者であるリスクがあることを示し、スキャン装置に身元検証情報を送り、取引の安全性を確実にするなどする、つまり、ユーザに、スキャン装置を使用して、オペレータの身元についてのオフライン検証を実行するように要求する（例えば、ＩＤを提示する、オペレータは携帯装置の所有者であることを証明できる証明情報を提供するなど）。または、オンライン取引要求をスキャナ装置に送る、つまり、ユーザに、スキャン装置を使用して、オペレータに、ユーザについてのオンライン身元検証を実行するように、オフライン支払フローを起動することを通知するように要求する。
【００９０】
本願に係る技術的解決策では、携帯装置により提供された支払コードを受信すると、サーバによるリスク制御操作を再び開始する必要があるかどうかは、端末装置により、支払コードに含まれているオペレータの行動的生体認証特質に対して実行されるリスク制御識別の結果に基づいて判定できる。端末装置の局所リスク識別システムにより実行されるリスク制御識別を完了することは、端末装置に対する演算リソースを７０％節約可能であり、それは、サーバのリスク制御リソースの消費を大幅に削減し、サーバ全体のリスク制御効率を向上するということが実験を通して証明された。
【００９１】
図３は、本願の幾つかの実施形態に係る、携帯装置においてスキャンアンドペイを実行するために利用されるリスク制御方法のフローチャートである。本願の実施形態を、オフラインリスク制御を達成することを目標として、詳細に記述する。
【００９２】
ステップ３０１：携帯装置は、ユーザから支払要求を受信する。
【００９３】
支払要求は、ユーザがオフライン状態のときは、ユーザのために携帯装置に送られる。
【００９４】
携帯装置が支払要求を受信すると、携帯装置は、設定された時間範囲内で収集された、ユーザの行動的生体認証特質を判定する。
ステップ３０２：携帯装置は、支払要求に基づいて支払コードを生成する。
【００９５】
ここで、支払コードは、ユーザにより使用されている支払口座と、ユーザの行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質と、ユーザは携帯装置の所有者であるかどうかの判定結果の情報を含んでいる。
【００９６】
ステップ３０３：携帯装置により提供される支払コードをスキャンし、支払コードから、ユーザは携帯装置の所有者であるかどうかの判定結果を取得する。
【００９７】

判定結果が、百分率の形式で表現されている場合、
【００９８】
ステップ３０４：判定結果に対応する値を、第１閾値および第２閾値と比較する。
【００９９】
本願の実施形態における第２閾値と第１閾値は異なる値を有し、第２閾値は第１閾値よりも小さい。
【０１００】
ステップ３０５：判定結果に対応する値が第２閾値よりも小さい場合、オペレータは携帯装置の所有者ではないことを示し、サーバのリスク制御識別システムにリスク識別要求を送り、サーバのリスク制御識別操作を起動する。
【０１０１】
ステップ３０６：判定結果に対応する値が第１閾値よりも高くなく、第２閾値よりも高い場合、オペレータは携帯装置の所有者であるリスクがあることを示し、スキャン装置に身元検証情報を送り、つまり、ユーザに、スキャン装置を使用して、オペレータの身元についてのオフライン検証を実行するように要求する。
【０１０２】
ステップ３０７：判定結果に対応する値が第１閾値よりも高い場合、オペレータは携帯装置の所有者でないリスクは低いと判定し、または、オペレータは携帯装置の所有者であると判定して、支払要求に対する応答を誘発する。
【０１０３】
従って、ユーザの行動的生体認証特質と関連付けられている情報をオフラインで支払コードに符号化し、サーバにおいてリスク制御スキャンを開始するかどうかを、この情報に基づいて実行する、本願の係る方法においては、サーバのリスク制御リソースの消費量を大幅に削減可能であり、リスク制御に対する総時間を削減可能であり、ユーザの体験を向上可能である。
【０１０４】
図４は、本願の幾つかの実施形態に係る、携帯装置において利用されるスキャンアンドペイ装置の概略構造図である。装置は、受信ユニット４１と生成ユニット４２を備え、
受信ユニット４１は、携帯装置のオペレータの支払要求を受信するためであり、
生成ユニット４２は、支払要求に基づいて、下記の情報、
支払口座と関連付けられている第１情報と、オペレータの行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質と関連付けられている第２情報を少なくとも含んでいる支払コードを生成するためである。
【０１０５】
本願の幾つかの他の実施形態においては、第２情報は更に、
オペレータの行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質の比較に基づく、オペレータは携帯装置の所有者であるかどうかの判定結果を含んでいる。
【０１０６】
本願の幾つかの他の実施形態においては、装置は更に処理ユニット４３を備えており、
判定結果は、オペレータは携帯装置の所有者であるという確率は、設定された閾値よりも低いということであり、携帯装置はオフライン支払状態であると判定された場合、処理ユニット４３は、携帯装置のオペレータについてのオンライン身元確認を誘発する。
【０１０７】
本願の幾つかの他の実施形態においては、生成ユニット４２が、支払要求に基づいて支払コードを生成することは、
支払要求に基づいて、支払口座と関連付けられている第１情報と、オペレータの行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質と関連付けられている第２情報を判定することと、
第２情報と識別子の値との間の、予め設定された対応関係に従って、支払要求に含まれている第２情報に対応する識別子の値を判定することと、

支払コードにおける少なくとも１桁が識別子の値に対応するために使用される支払コードを、識別子の値と第１情報を使用して生成すること、を備えている。

【０１０８】

本願の幾つかの他の実施形態においては、行動的生体認証特質は、ＲＰＣ要求記録、閲覧ログ、携帯装置を持つ姿勢、および指で押すときの特性の少なくとも１つを含んでいる。

【０１０９】

本願の実施形態における装置は、ソフトウェアの方法またはハードウェアの方法で実現でき、それは明細書においては制限されないということに留意すべきである。装置は、携帯装置のオペレータの支払要求を受信して、支払要求に基づいて、支払口座と関連付けられている第１情報と、オペレータの行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質と関連付けられている第２情報を少なくとも含んでいる支払コードを生成する。このようにして、オペレータの行動的生体認証情報に基づく識別結果は、リスク制御判定のために支払コードを介してサーバに送信され、それにより、リスク制御システム全体が、より多くの次元におけるデータを使用して精度よくリスクを判定し、リスク制御の精度を向上し、そのため、リスク制御識別の効率を向上することを可能にする。

【０１１０】

図５は、本願の幾つかの実施形態に係る、携帯装置においてスキャンアンドペイを実行するために利用されるリスク制御装置の概略構造図である。リスク制御装置は、取得ユニット５１とリスク制御処理ユニット５２を備えており、

取得ユニット５１は、携帯装置により提供される、下記の情報、支払口座と関連付けられている第１情報と、携帯装置のオペレータの行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質と関連付けられている第２情報を少なくとも含んでいる支払コードを取得するためであり、

リスク制御処理ユニット５２は、支払コードに含まれている第２情報に基づいて、サーバのリスク制御識別を起動するかどうかを判定するためである。

【０１１１】

本願の幾つかの他の実施形態においては、取得ユニット５１が、携帯装置により提供される支払コードを取得することは、

携帯装置により提供される二次元バーコード画像をスキャンすることと、

支払コードに含まれている、支払口座と関連付けられている第１情報と、携帯装置のオペレータの行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質と関連付けられている第２情報を、二次元バーコード画像から抽出すること、を備えている。

【０１１２】

本願の幾つかの他の実施形態においては、第２情報は、オペレータの行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質との比較に基づく、オペレータは携帯装置の所有者であるかどうかの判定結果を含んでおり、

支払コードに含まれている第２情報に基づいて、リスク制御処理ユニット５２が、サーバにリスク制御要求を送るかどうかを判定することは、

支払コードに含まれている判定結果は、オペレータは携帯装置の所有者ではないということである場合、サーバのリスク制御識別を誘発することを備えている。

【０１１３】

本願の幾つかの他の実施形態においては、第２情報は、オペレータの行動的生体認証特質と、携帯装置に記録されている履歴行動的生体認証特質との比較に基づいて、閲覧ログは異常かどうかを判定し、遠隔手続き呼出し（ＲＰＣ）プロトコルは異常かどうかを判定することによる、オペレータは携帯装置の所有者かどうかの判定結果を含んでおり、

支払コードに含まれている第２情報に基づいて、リスク制御処理ユニット５２が、サーバにリスク制御要求を送るかどうかを判定することは、

支払コードに含まれている判定結果が、オペレータは携帯装置の所有者であるという確率は設定された閾値よりも低いということである場合、閲覧ログが異常と判定され、および／または、ＲＰＣ要求記録が異常と判定されると、サーバのリスク制御識別を誘発するこ

とを備えている。
【０１１４】
本願の実施形態におけるリスク制御装置は、ソフトウェアの方法またはハードウェアの方法で実現でき、明細書においては制限されないということに留意すべきである。リスク制御装置が、携帯装置により提供される支払コードを受信すると、リスク制御装置は、支払コードに含まれているオペレータの行動的生体認証特質について、端末装置により実行されるリスク制御識別の結果に基づいて、サーバによるリスク制御操作を、再び開始する必要があるかどうかを判定できる。端末装置の局所リスク識別システムにより実行されるリスク制御識別を完了することは、端末装置に対する演算リソースを７０％節約可能であり、それは、サーバのリスク制御リソースの消費を大幅に削減し、サーバ全体のリスク制御効率を向上するということが実験を通して証明された。
【０１１５】
１９９０年代において、技術の向上は、ハードウェアの向上（例えば、ダイオード、トランジスタ、スイッチなどの回路構造の向上）またはソフトウェアの向上（方法のフローの向上）に明白に区別可能である。しかし、技術的な発展に伴って、方法のフローの多くの現在の向上は、ハードウェア回路構造の直接の向上と考えることができる。設計者は、ほとんどいつも、向上された方法のフローを、ハードウェア回路にプログラムすることにより、対応するハードウェア回路構造を取得する。従って、方法のフローの向上は、ハードウェアモジュールで実現することは可能ではないと結論することは不可能である。例えば、プログラマブルロジックデバイス（ＰＬＤ）（例えば、フィールドプログラマブルゲートアレイ（ＦＰＧＡ））は、デバイスをプログラムすることにより、ユーザにより集積回路論理機能が決められるような集積回路である。設計者は、自分自身でプログラムして、デジタルシステムを、１つのＰＬＤ上に「集積」し、チップメーカーに、専用のＩＣチップの設計と製造を依頼する必要がない。現在では更に、このタイプのプログラミングは、手動でＩＣチップを製造するのではなく、「ロジックコンパイラ」を通してほとんど実現されてきている。ロジックコンパイラソフトウェアは、プログラムの開発および記述に使用されるソフトウェアコンパイラに類似しているが、コンパイルの前に、ソースコードを記述するために特別なプログラミング言語を使用しなければならず、それは、ハードウェア記述言語（ＨＤＬ）と称される。ＨＤＬは１つではなく、ＡＢＥＬ（Ａｄｖａｎｃｅｄ Ｂｏｏｌｅａｎ Ｅｘｐｒｅｓｓｉｏｎ Ｌａｎｇｕａｇｅ（高度なブール式言語））、ＡＨＤＬ（Ａｌｔｅｒａ Ｈａｒｄｗａｒｅ Ｄｅｓｃｒｉｐｔｉｏｎ Ｌａｎｇｕａｇｅ（アルテラハードウェア記述言語））、Ｃｏｎｆｌｕｅｎｃｅ（コンフルエンス）、ＣＵＰＬ（Ｃｏｒｎｅｌｌ Ｕｎｉｖｅｒｓｉｔｙ Ｐｒｏｇｒａｍｍｉｎｇ Ｌａｎｇｕａｇｅ（コーネル大学プログラミング言語））、ＨＤＣａｌ、ＪＨＤＬ（Ｊａｖａ（登録商標） Ｈａｒｄｗａｒｅ Ｄｅｓｃｒｉｐｔｉｏｎ Ｌａｎｇｕａｇｅ（ジャバハードウェア記述言語））、Ｌａｖａ、Ｌｏｌａ、ＭｙＨＤＬ、ＰＡＬＡＳＭ、ＲＨＤＬ（Ｒｕｂｙ Ｈａｒｄｗａｒｅ Ｄｅｓｃｒｉｐｔｉｏｎ Ｌａｎｇｕａｇｅ（ルビーハードウェア記述言語））などの多くのタイプのＨＤＬがある。現在、最も一般的に使用されているのは、ＶＨＤＬ（Ｖｅｒｙ－Ｈｉｇｈ－Ｓｐｅｅｄ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ Ｈａｒｄｗａｒｅ Ｄｅｓｃｒｉｐｔｉｏｎ Ｌａｎｇｕａｇｅ）とＶｅｒｉｌｏｇ（ヴェリログ）である。通常の技量を有する当業者は、方法のフローに対する少しのロジックプログラミングを実行し、方法のフローをＩＣにプログラムするために、上記のＨＤＬを使用することで、論理方法を実現するためのハードウェア回路を取得することは非常に容易であるということも認識すべきである。
【０１１６】
コントローラは、任意の適切な方法で実現できる。例えば、コントローラは、例えば、マイクロプロセッサまたはプロセッサの形式であってよく、同時に、（マイクロ）プロセッサにより実行可能なコンピュータ読取り可能プログラムコード（例えば、ソフトウェアまたはファームウェア）を格納するコンピュータ読取り可能媒体、ロジックゲート、スイッチ、特殊用途向け集積回路（ＡＳＩＣ）、プログラマブルロジックコントローラ、および

埋込みマイクロコントローラであってよい。コントローラの例としては、下記のマイクロコントローラに制限されるわけではないが、ＡＲＣ ６２５Ｄ、Ａｔｍｅｌ ＡＴ９１ＳＡＭ、Ｍｉｃｒｏｃｈｉｐ ＰＩＣ１８Ｆ２６Ｋ２０、およびＳｉｌｉｃｏｎｅ Ｌａｂｓ Ｃ８０５１Ｆ３２０がある。メモリコントローラは更に、メモリの制御ロジックの一部として実現できる。通常の技量を有する当業者は、コントローラは、純粋にコンピュータ読取り可能プログラムコードの方法で実現されるということに加えて、ロジックゲート、スイッチ、ＡＳＩＣ、プログラマブルロジックコントローラ、および埋込みマイクロコントローラの形式で、同じ機能をコントローラが実現することを可能にする方法のステップに対して、ロジックプログラミングを実行することは完全に実現可能であるということも認識すべきである。従って、そのようなコントローラは、ハードウェア部品と考えることが可能であるが、コントローラに含まれ、種々の機能を達成するように構成されているデバイスもまた、ハードウェア部品の内部の構造と考えることができる。または、種々の機能を達成するように構成されているデバイスは、方法を実現するためのソフトウェアと、ハードウェア部品の内部の構造の両者とさえ考えることができる。

【０１１７】

上記の実施形態において記述されたシステム、装置、モジュール、またはユニットは、コンピュータチップまたは実体により実現でき、または、機能を有する製品により実現できる。典型的な実現デバイスはコンピュータである。１つの例においては、コンピュータは、例えば、パーソナルコンピュータ、ラップトップコンピュータ、セルラーフォン、カメラフォン、スマートフォン、携帯情報端末、メディアプレーヤ、ナビゲーションデバイス、イーメールデバイス、ゲームコンソール、タブレットコンピュータ、ウェアラブルデバイス、または、これらのデバイスにおける任意のデバイスの組み合わせであってよい。

【０１１８】

記述の便宜上、上記のデバイスは、記述のために、機能によって種々のユニットに分割される。ユニットの機能は、本願が実現されるときに、１つの、または複数のソフトウェアおよび／またはハードウェアにおいて実現できる。

【０１１９】

通常の技量を有する当業者は、本発明の実施形態は、方法、システム、またはコンピュータプログラム製品として提供できるということを理解すべきである。従って、本発明は、完全なハードウェア実施形態、完全なソフトウェア実施形態、または、ソフトウェアとハードウェアを組み合わせた実施形態として実現できる。更に、本発明は、コンピュータ使用可能プログラムコードを備えている、１つ以上のコンピュータ使用可能格納媒体（下記のものに制限されるわけではないが、磁気ディスクメモリ、ＣＤ－ＲＯＭ、光メモリなどを含む）上で実現されるコンピュータプログラム製品の形式であってよい。

【０１２０】

本発明は、本発明の実施形態に係る、方法、デバイス（システム）、およびコンピュータプログラム製品のフローチャートおよび／またはブロック図を参照して記述されている。コンピュータプログラム命令は、フローチャートおよび／またはブロック図における各プロセスおよび／またはブロック、およびフローチャートおよび／またはブロック図における複数のプロセスおよび／またはブロックの組み合わせを実現するために使用できるということは理解されるべきである。これらのコンピュータプログラム命令は、汎用コンピュータ、特殊用途向けコンピュータ、埋込みプロセッサ、または、マシンを生成するための、他のプログラマブルデータ処理装置のプロセッサに対して提供でき、コンピュータ、または他のプログラマブルデータ処理装置のプロセッサにより実行される命令に、フローチャートにおける１つ以上のプロセス、および／または、ブロック図における１つ以上のブロックにおいて指定される機能を実現するための装置を生成させる。

【０１２１】

これらのコンピュータプログラム命令はまた、コンピュータまたは他のプログラマブルデータ処理装置に、特別な方法で作動することを指示可能なコンピュータ読取り可能メモリにも格納でき、コンピュータ読取り可能メモリに格納された命令に、指示装置を含む、製

造された製品を生成させる。指示装置は、フローチャートにおける１つ以上のプロセス、および／または、ブロック図における１つ以上のブロックにおいて指定される機能を実現する。

【０１２２】

これらのコンピュータプログラム命令はまた、コンピュータまたは他のプログラマブルデータ処理装置にもロードでき、一連の操作ステップを、コンピュータまたは他のプログラマブル装置上で実行させ、それにより、コンピュータにより実現される処理を生成する。従って、コンピュータまたは他のプログラマブル装置上で実行される命令は、フローチャートにおける１つ以上のプロセス、および／または、ブロック図における１つ以上のブロックにおいて指定される機能を実現するためのステップを提供する。

【０１２３】

典型的な構成においては、演算装置は、１つ以上のプロセッサ（ＣＰＵ）、入／出力インタフェース、ネットワークインタフェース、およびメモリを含んでいる。

【０１２４】

メモリには、揮発性メモリ、ランダムアクセスメモリ（ＲＡＭ）および／または、例えばリードオンリメモリ（ＲＯＭ）またはフラッシュＲＡＭである不揮発性メモリのようなコンピュータ読取り可能媒体を含むことができる。メモリは、コンピュータ読取り可能媒体の例である。

【０１２５】

コンピュータ読取り可能媒体としては、永久的、揮発性、可動、非可動媒体があり、これらの媒体は、任意の方法または技術で、情報の格納を実現可能である。情報は、コンピュータ読取り可能命令、データ構造、プログラムモジュール、または他のデータであってよい。コンピュータの格納媒体の例としては、下記のものに制限されるわけではないが、相変化ランダムアクセスメモリ（ＰＲＡＭ）、スタティックランダムアクセスメモリ（ＳＲＡＭ）、ダイナミックランダムアクセスメモリ（ＤＲＡＭ）、他のタイプのランダムアクセスメモリ（ＲＡＭ）、リードオンリメモリ（ＲＯＭ）、電気的消去可能型プログラマブルリードオンリメモリ（ＥＥＰＲＯＭ）、フラッシュメモリ、または他のメモリ技術、コンパクトディスクリードオンリメモリ（ＣＤ－ＲＯＭ）、デジタル多目的ディスク（ＤＶＤ）、または他の光メモリ、カセット、カセットおよびディスクメモリ、または他の磁気メモリ装置、または、任意の他の非伝送媒体があり、それらは、演算装置がアクセス可能な情報を格納するために使用可能である。明細書における定義によれば、コンピュータ読取り可能媒体は、変調データ信号およびキャリアのような一時的媒体は含まない。

【０１２６】

「含む」、「備える」、またはそれらの用語の任意の他の変形である用語は、非排他的な包含を含むことが意図されており、一連の要素を備えているプロセス、方法、商品、または装置に、これらの要素を備えさせるだけではなく、明確には列挙されてない他の要素も備えさせ、または、プロセス、方法、商品、または装置に本来的に備わっている要素を更に備えさせるということに更に留意すべきである。更なる制限がないときは、「１つの～を備えている」という記述により定義される要素は、上記の要素を備えているプロセス、方法、商品、または装置が更に、追加的な同一要素を更に備えるということを排除するものではない。

【０１２７】

通常の技量を有する当業者は、本願の実施形態が、方法、システム、またはコンピュータプログラム製品として提供され得るということを理解すべきである。従って、本願は、完全なハードウェア実施形態、完全なソフトウェア実施形態、またはソフトウェアとハードウェアを組み合わせた実施形態として実現できる。更に、本願は、コンピュータ使用可能プログラムコードを備えている１つ以上のコンピュータ使用可能格納媒体（下記のものに制限されるわけではないが、磁気ディスクメモリ、ＣＤ－ＲＯＭ、光メモリなどを含む）上で実現されるコンピュータプログラム製品の形式であってよい。

【０１２８】

本願は、プログラムモジュールのような、コンピュータにより実行されるコンピュータ実行可能命令の通常の状況において記述できる。一般的に、プログラムモジュールは、特別な作業を実行するために、または、特別な抽象データタイプを実現するために、ルーチン、プログラム、オブジェクト、構成要素、データ構造などを備えている。本願はまた、分散型演算環境においても実践できる。これらの分散型演算環境においては、通信ネットワークを介して接続されている遠隔処理装置が作業を遂行する。分散型演算環境においては、プログラムモジュールを、格納装置を含む、局所および遠隔コンピュータ格納媒体に置くことができる。

【０１２９】

この明細書における実施形態は、それぞれの実施形態の、他の実施形態との差に注目して徐々に前進する方法で記述されており、実施形態は、同一または類似の部分を相互に参照され得る。特に、システムの実施形態は、システムの実施形態が、方法の実施形態と略類似しているので、相対的に簡単な方法で記述されている。方法の実施形態の記述は、関連する部分に対して参照され得る。

【０１３０】

上記の実施形態は、本願の実施形態に過ぎず、本願を制限するためには使用されない。通常の技量を有する当業者には、本願が、種々の修正および変更を有することができることが分かる。本願の精神および原理内で行われる如何なる修正、等価な置換、または改良も、本願の請求項により含まれるものとする。

【図面】

【図１】

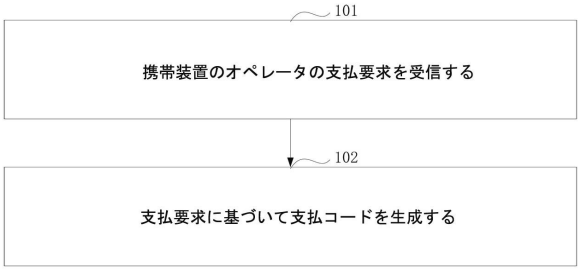


FIG. 1

【図２】

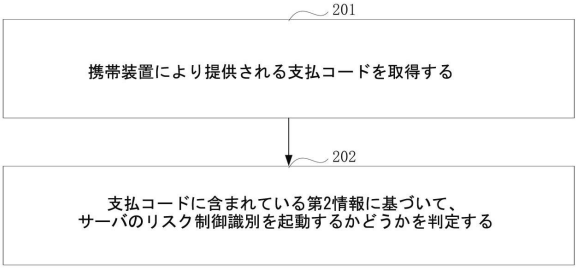


FIG. 2

【図３】

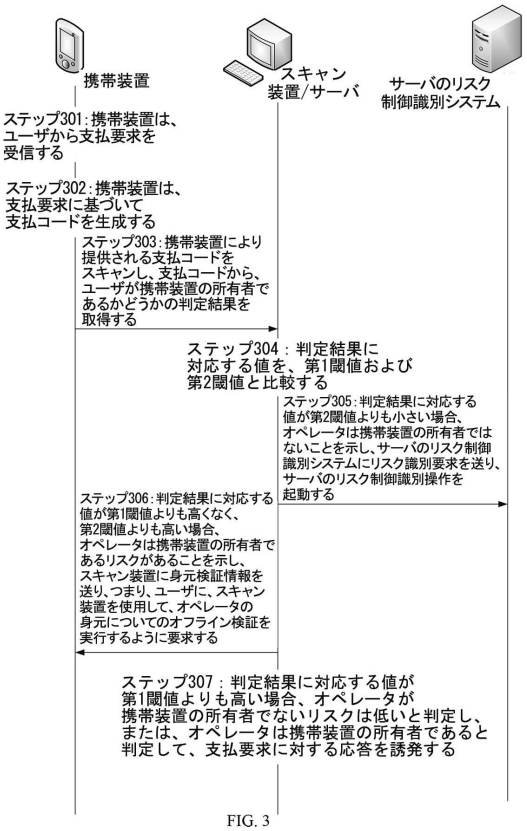


FIG. 3

【図４】

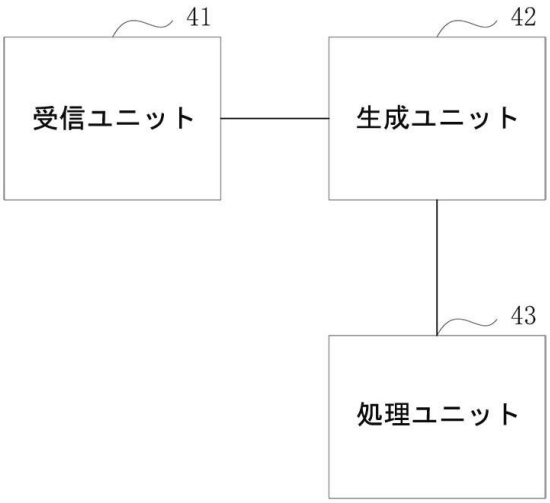


FIG. 4

【図５】

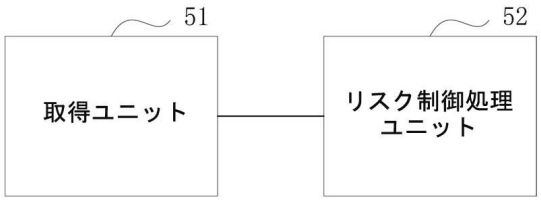


FIG. 5

フロントページの続き

(74)代理人 100117019
弁理士 渡辺 陽一
(74)代理人 100173107
弁理士 胡田 尚則
(72)発明者 ルー イーチョン
中華人民共和国，ジョージアーン ３１１１２１，ハーンジョウ，ユイ ハーン ディストリクト，ウエスト ウエン イー ロード ナンバー９６９，ビルディング ３，５／フロア，アリババ グループ リーガル ディパートメント
(72)発明者 チェン ショアイ
中華人民共和国，ジョージアーン ３１１１２１，ハーンジョウ，ユイ ハーン ディストリクト，ウエスト ウエン イー ロード ナンバー９６９，ビルディング ３，５／フロア，アリババ グループ リーガル ディパートメント
(72)発明者 チェン タオ
中華人民共和国，ジョージアーン ３１１１２１，ハーンジョウ，ユイ ハーン ディストリクト，ウエスト ウエン イー ロード ナンバー９６９，ビルディング ３，５／フロア，アリババ グループ リーガル ディパートメント
(72)発明者 シア チュイポン
中華人民共和国，ジョージアーン ３１１１２１，ハーンジョウ，ユイ ハーン ディストリクト，ウエスト ウエン イー ロード ナンバー９６９，ビルディング ３，５／フロア，アリババ グループ リーガル ディパートメント
(72)発明者 ワン ニン
中華人民共和国，ジョージアーン ３１１１２１，ハーンジョウ，ユイ ハーン ディストリクト，ウエスト ウエン イー ロード ナンバー９６９，ビルディング ３，５／フロア，アリババ グループ リーガル ディパートメント

審査官 池田 聡史

(56)参考文献 特開２００５－２０８８２２（ＪＰ，Ａ）
特開２００４－２５８８４５（ＪＰ，Ａ）
特開２００９－３０１４４０（ＪＰ，Ａ）
特開２０１０－９７４６７（ＪＰ，Ａ）
特開２０１５－１７６２３３（ＪＰ，Ａ）
中国特許出願公開第１０６１２７４６１（ＣＮ，Ａ）
中国特許出願公開第１０４８３５０４０（ＣＮ，Ａ）
中国実用新案第２０５６０８７６４（ＣＮ，Ｕ）
Haifeng Liu, et al.，“ A new user similarity model to improve the accuracy of collaborative filtering ”，Knowledge-Based Systems 56 (2014)，2014年，pp.156～166
Hyung Jun Ahn，“ A new similarity measure for collaborative filtering to alleviate the new user cold-starting problem ”，Information Sciences，Volume 178, Issue 1，2008年，pp.37～51

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｑ １０／００－９９／００