(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6732806号
(P6732806)
(45)発行日　令和2年7月29日(2020.7.29)　(24)登録日　令和2年7月10日(2020.7.10)

(51)Int.Cl.　F I
G06F 21/55 (2013.01)　G06F 21/55 320

請求項の数 18 (全 25 頁)

(21)出願番号　特願2017-562009(P2017-562009)
(86)(22)出願日　平成28年4月28日(2016.4.28)
(65)公表番号　特表2018-519586(P2018-519586A)
(43)公表日　平成30年7月19日(2018.7.19)
(86)国際出願番号　PCT/CN2016/080446
(87)国際公開番号　WO2016/192495
(87)国際公開日　平成28年12月8日(2016.12.8)
審査請求日　令和1年5月7日(2019.5.7)
(31)優先権主張番号　201510289825.4
(32)優先日　平成27年5月29日(2015.5.29)
(33)優先権主張国・地域又は機関
中国(CN)

早期審査対象出願

(73)特許権者　510330264
アリババ・グループ・ホールディング・リミテッド
ＡＬＩＢＡＢＡ　ＧＲＯＵＰ　ＨＯＬＤＩＮＧ　ＬＩＭＩＴＥＤ
英国領，ケイマン諸島，グランド・ケイマン，ジョージ・タウン，ワン・キャピタル・プレイス，フォース・フロア，ピー．オー．ボックス　８４７
(74)代理人　100188558
弁理士　飯田　雅人
(74)代理人　100205785
弁理士　▲高▼橋　史生
(74)代理人　100097320
弁理士　宮川　貞二

最終頁に続く

(54)【発明の名称】アカウント盗難リスクの識別方法、識別装置、及び防止・制御システム

(57)【特許請求の範囲】
【請求項１】
現在の操作挙動に関する情報に応じて、操作挙動を受けるデバイスのデバイス情報を収集するステップ（Ｓ２１０）と；
前記現在の操作挙動に先立つ所定の期間内における前記デバイス上の過去の操作挙動に関するすべてのユーザアイデンティティ情報を取得するステップ（Ｓ２２０）と；
前記ユーザアイデンティティ情報の各々において示されるユーザアイデンティティ解析位置を解析し、前記期間における前記デバイス上のユーザアイデンティティ解析位置の数を算定するステップ（Ｓ２３０）と；
前記期間における前記デバイス上のユーザアイデンティティ解析位置の数に応じて、前記現在の操作挙動がアカウント盗難リスクを有するか否かを判定するステップ（Ｓ２４０）と；を備える、
アカウント盗難リスクの識別方法。
【請求項２】
前記ユーザアイデンティティ情報は、ユーザ登録情報におけるクレデンシャル情報を含み；
前記ユーザアイデンティティ情報の各々において示されるユーザアイデンティティ解析位置を解析し、前記期間における前記デバイス上のユーザアイデンティティ解析位置の数を算定する前記ステップは、具体的に：
各ユーザ登録情報におけるクレデンシャルタイプ及びクレデンシャル番号に応じて、前

記ユーザアイデンティティ解析位置を取得し、前記デバイス上のユーザアイデンティティ解析位置の数を算定するステップを備える、
請求項１に記載のリスクの識別方法。
【請求項３】
各ユーザ登録情報におけるクレデンシャルタイプ及びクレデンシャル番号に応じて、前記ユーザアイデンティティ解析位置を取得し、前記デバイス上のユーザアイデンティティ解析位置の数を算定する前記ステップは：
前記クレデンシャルタイプのクラスに応じて、前記ユーザアイデンティティ解析位置の解析モードを決定するステップと；
前記クレデンシャルタイプが中国の国内居住者のＩＤカードである場合、各クレデンシャル番号の先頭６桁を解析して、前記ユーザアイデンティティ解析位置を取得し、それに応じて、前記デバイス上のユーザアイデンティティ解析位置の数を算定するステップ；又は、前記クレデンシャルタイプが中国の国内非居住者のＩＤカードであるか国外のクレデンシャルである場合、各クレデンシャルタイプ又は各クレデンシャル番号が１つのユーザアイデンティティ解析位置に対応すると推定し、それに応じて、前記デバイス上のユーザアイデンティティ解析位置の数を算定するステップと；を備える、
請求項２に記載のリスクの識別方法。
【請求項４】
現在の操作挙動に関する情報に応じて、操作挙動を受けるデバイスのデバイス情報を収集する前記ステップは：
前記デバイスのデバイス識別コードを収集することによって前記デバイスの対応するデバイス情報を取得するステップを備える、
請求項１に記載のリスクの識別方法。
【請求項５】
前記デバイスのデバイス識別コードを収集することによって前記デバイスの対応するデバイス情報を取得する前記ステップは：
前記デバイスのタイプに応じて、前記収集したデバイス情報のコンテンツを決定するステップを備え、
前記デバイスがＰＣである場合、前記収集したデバイス情報はＭＡＣ、ＩＰ、及び／又はＵＭＩＤを含み、
前記デバイスが携帯端末である場合、前記収集したデバイス情報はＭＡＣ、ＩＭＥＩ、ＴＩＤ、及び／又は携帯電話番号を含む、
請求項４に記載のリスクの識別方法。
【請求項６】
前記デバイスのデバイス識別コードを収集することによって前記デバイスの対応するデバイス情報を取得する前記ステップは：
前記デバイス識別コードから識別されるデバイスの数量に応じて、前記デバイス上のユーザアイデンティティ解析位置の数を算定するモードを決定するステップと；
一意のデバイスが識別された場合、前記デバイス上のユーザアイデンティティ解析位置の数を解析及び算定するステップ；又は、複数のデバイスが識別された場合、各デバイス上のユーザアイデンティティ解析位置の数を解析及び算定するステップ；又は、デバイスが識別されない場合、前記デバイス上のユーザアイデンティティ解析位置の数を０に設定するステップと；
得られた前記デバイス上のユーザアイデンティティ解析位置の数を、所定のスコアリングモデルの入力変数として用いて、前記デバイスのアカウント盗難リスクレベルを評価するステップと；を備える、
請求項４に記載のリスクの識別方法。
【請求項７】
前記期間における前記デバイス上のユーザアイデンティティ解析位置の数に応じて、前記現在の操作挙動がアカウント盗難リスクを有するか否かを判定する前記ステップは：

前記デバイス上のユーザの総数、前記現在の操作挙動のユーザにバインドされた携帯電話番号の数、前記現在のユーザの過去の操作挙動に対するデバイスの数、前記現在のユーザの前記過去の操作挙動のＩＰアドレスの数、前記現在のユーザの前記現在の操作挙動に関する前記情報と前記過去の操作挙動に関する情報との差分、及び／又は前記現在の操作挙動のルーティング特徴情報が前記過去の操作挙動のルーティング特徴情報と同一であるか否か、と組み合わせて、前記現在の操作挙動のユーザのアカウント盗難リスクレベルを評価するステップを備える、

請求項１乃至請求項６のいずれか一項に記載のリスクの識別方法。

【請求項８】

前記期間における前記デバイス上のユーザアイデンティティ解析位置の数に応じて、前記現在の操作挙動がアカウント盗難リスクを有するか否かを判定する前記ステップは：

前記デバイスの前記アカウント盗難リスクレベル及び前記現在の操作挙動のユーザの前記アカウント盗難リスクレベルと組み合わせてアカウント盗難リスク値を算定し、前記リスク値が所定の閾値を超える場合にアカウント盗難を識別するステップを更に備える、

請求項７に記載のリスク識別方法。

【請求項９】

現在の操作挙動に関する情報に応じて、操作挙動を受けるデバイスのデバイス情報を収集するよう構成されたデバイス情報収集モジュール（３１０）と；

前記現在の操作挙動に先立つ所定の期間内における前記デバイス上の過去の操作挙動に関するすべてのユーザアイデンティティ情報を取得するよう構成されたユーザ情報取得モジュール（３２０）と；

前記ユーザアイデンティティ情報の各々において示されるユーザアイデンティティ解析位置を解析し、前記期間における前記デバイス上のユーザアイデンティティ解析位置の数を算定するよう構成されたユーザアイデンティティ解析モジュール（３３０）と；

前記期間における前記デバイス上のユーザアイデンティティ解析位置の数に応じて、前記現在の操作挙動がアカウント盗難リスクを有するか否かを判定するよう構成されたアカウント盗難リスク評価モジュール（３４０）と；を備える、

アカウント盗難リスク識別装置（３００）。

【請求項１０】

前記ユーザアイデンティティ情報は、ユーザ登録情報におけるクレデンシャル情報を含み；

前記ユーザアイデンティティ解析モジュール（３３０）は、各ユーザ登録情報におけるクレデンシャルタイプ及びクレデンシャル番号に応じて、前記ユーザアイデンティティ解析位置を取得し、前記デバイス上のユーザアイデンティティ解析位置の数を算定する、

請求項９に記載のリスク識別装置（３００）。

【請求項１１】

前記ユーザアイデンティティ解析モジュール（３３０）は：

前記クレデンシャルタイプのクラスに応じて、前記ユーザアイデンティティ解析位置の解析モードを決定し；

前記クレデンシャルタイプが中国の国内居住者のＩＤカードである場合、各クレデンシャル番号の先頭６桁を解析して、前記ユーザアイデンティティ解析位置を取得し、それに応じて、前記デバイス上のユーザアイデンティティ解析位置の数を算定し；又は、前記クレデンシャルタイプが中国の国内非居住者のＩＤカードであるか国外のクレデンシャルである場合、各クレデンシャルタイプ又は各クレデンシャル番号が１つのユーザアイデンティティ解析位置に対応すると推定し、それに応じて、前記デバイス上のユーザアイデンティティ解析位置の数を算定する；

請求項１０に記載のリスク識別装置。

【請求項１２】

前記デバイス情報収集モジュール（３１０）は、前記デバイスのデバイス識別コードを収集することによって前記デバイスの対応するデバイス情報を取得する、

請求項９に記載のリスク識別装置。
【請求項１３】
前記デバイス情報収集モジュールは：
前記デバイスのタイプに応じて、前記収集したデバイス情報のコンテンツを決定し；
前記デバイスがＰＣである場合、前記収集したデバイス情報はＭＡＣ、ＩＰ、及び／又はＵＭＩＤを含み；
前記デバイスが携帯端末である場合、前記収集したデバイス情報はＭＡＣ、ＩＭＥＩ、ＴＩＤ、及び／又は携帯電話番号を含む；
請求項１２に記載のリスク識別装置。
【請求項１４】
前記ユーザアイデンティティ解析モジュール（３３０）は：
前記デバイス情報収集モジュールによって識別されるデバイスの数量に応じて、前記デバイス上のユーザアイデンティティ解析位置の数を算定するモードを決定し；
一意のデバイスが識別された場合、前記デバイス上のユーザアイデンティティ解析位置の数を解析及び算定し；又は、複数のデバイスが識別された場合、各デバイス上のユーザアイデンティティ解析位置の数を解析及び算定し；又は、デバイスが識別されない場合、前記デバイス上のユーザアイデンティティ解析位置の数を０に設定し；
得られた前記デバイス上のユーザアイデンティティ解析位置の数を、前記アカウント盗難リスク評価モジュールの所定のスコアリングモデルの入力変数として用いて、前記デバイスのアカウント盗難リスクレベルを評価する；
請求項９に記載のリスク識別装置。
【請求項１５】
前記アカウント盗難リスク評価モジュール（３４０）は、前記デバイス上のユーザの総数、前記現在の操作挙動のユーザにバインドされた携帯電話番号の数、前記現在のユーザの過去の操作挙動に対するデバイスの数、前記現在のユーザの前記過去の操作挙動のＩＰアドレスの数、前記現在のユーザの前記現在の操作挙動に関する前記情報と前記過去の操作挙動に関する情報との差分、及び／又は前記現在の操作挙動のルーティング特徴情報が前記過去の操作挙動のルーティング特徴情報と同一であるか否か、と組み合わせて、前記現在の操作挙動のユーザのアカウント盗難リスクレベルを評価する、
請求項９乃至請求項１４のいずれか一項に記載のリスク識別装置。
【請求項１６】
前記アカウント盗難リスク評価モジュールは、前記デバイスの前記アカウント盗難リスクレベル及び前記現在の操作挙動のユーザの前記アカウント盗難リスクレベルと組み合わせてアカウント盗難リスク値を算定し、前記リスク値が所定の閾値を超える場合にアカウント盗難を識別する、
請求項１５に記載のリスク識別装置。
【請求項１７】
請求項９乃至請求項１６のいずれか一項に記載の前記リスク識別装置（３００）と、アカウント盗難通知装置（２００）と、リスク処理装置（１００）とを備えるアカウント盗難リスク防止・制御システムであって、
前記リスク識別装置（３００）は、操作挙動プラットフォームにおけるアカウント盗難リスク値を算定し、前記リスク値が所定の閾値を超える場合、アカウント盗難を識別するよう構成され；
前記アカウント盗難通知装置（２００）は、前記リスク識別装置（３００）がアカウント盗難を識別した場合、前記リスク処理装置及びユーザ受信デバイスへアカウント盗難メッセージを通知するよう構成され；
前記リスク処理装置（１００）は、前記アカウント盗難メッセージを受信した場合、ユーザの盗難に遭ったアカウントをブロックし、前記盗難に遭ったアカウントに関連するリスクデータを傍受するよう構成された；
アカウント盗難リスク防止・制御システム。

【請求項１８】
前記リスク処理装置（１００）が前記リスクデータを検査し、前記リスク識別装置（３００）がアカウント盗難リスクを評価するためのスコアリングモデルを認証するために、前記リスク処理装置（１００）が傍受した前記リスクデータを記憶するよう構成された事例データベースを備える、
請求項１７に記載のリスク防止・制御システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本願は、ネットワークセキュリティ技術に関し、特に、アカウント盗難リスクの識別方法、識別装置、及び防止・制御システムに関する。
【背景技術】
【０００２】
オンライントランザクション、モバイル決済（モバイルペイメント）、他のアプリケーションは、ユーザにとって便利である反面、セキュリティリスクが極めて高い。アカウントが盗難に遭うと、ユーザは財産を失うだけでなく、場合によってはアカウントを盗んだ者が盗んだアカウントを用いて行う不法行為のリスクに対応しなければならない。ユーザに対して最大限安全なネットワーク環境を提供するため、アカウントが盗まれたか否かをどのようにして迅速かつ効果的に認識するかは、ネットワークアプリケーションサービスプロバイダが解決すべき、避けられない重要な課題である。従来技術において、アカウント盗難リスクを認識するための解決策が数多く提案されており、以下では、それらを例に取って簡単に説明する。
【０００３】
あるタイプの解決策は、トランザクションユーザのトランザクション要求が異常であるか否かを監視することによってアカウント盗難リスクを識別する。例えば、ユーザによるアカウントへのログインが遠隔地でなされているかを検出し、遠隔ログインであれば、ユーザは認証を得ねばならず、認証に失敗するとユーザアカウントはブロックされる。アカウントの盗難は遠隔ログインとして表面化することがよくある。よって、遠隔ログイン要求の監視は、アカウント盗難リスクを適時に識別し易くする。しかし、ネットワークオペレータは、特にＩＰアドレスの都市（city）間での割り振りに際して、自身のＩＰアドレスプールを変更する可能性があるため、正常なユーザが危険なユーザとして識別されるおそれがあり、それによりアカウント盗難識別のエラー率が相対的に高くなるおそれがある。
【０００４】
別のタイプの解決策は、キーデバイスを監視することによってアカウント盗難リスクを識別する。例えば、トランザクションログオンデバイスにログオンするトランザクションユーザの人数を算定し、算定された人数を、アカウント盗難リスクを識別するためのスコアリングモデルの入力変数として用いて、当該デバイスのアカウント盗難リスクレベルを評価する。デバイス上のトランザクションユーザが相対的に少ない場合はアカウント盗難リスクの可能性も相対的に低いが、デバイス上のトランザクションユーザが多い場合、アカウント盗難リスクの可能性は著しく高まる。よって、このようにトランザクションユーザが多いタイプのデバイスを主に監視することによって、ある程度はアカウント盗難を識別できる。しかし、変数、すなわちデバイス上のトランザクションユーザの人数は、判別力（distinguishing capability）及び安定性が比較的低く、単一デバイスに対して複数のユーザがトランザクションを行う通常の状況において、この解決策は識別エラーを引き起こす傾向がある。
【０００５】
他のネットワーク操作挙動（operation behavior）に対してアカウント盗難リスクを識別する解決策についても、通常、誤判断やフォールスネガティヴの問題があり、アカウント盗難リスクの判別力が十分に高くないため、その解決による全体的な効果は満足できる

ものではない。よって、アカウント盗難リスクを識別する新たな解決策を設計する必要がある。

【発明の概要】

【発明が解決しようとする課題】

【０００６】

従来技術における上記の欠陥に鑑み、本願の目的は、アカウント盗難リスクを判別する力を効果的に向上させる、アカウント盗難リスクの識別方法、識別装置、及び防止・制御システムを提供することである。

【課題を解決するための手段】

【０００７】

上記技術的問題を解決するため、本願は、アカウント盗難リスクの識別方法を提供し、本方法は：

現在の操作挙動に関する情報に応じて操作挙動を受けるデバイスのデバイス情報を収集するステップと；

前記現在の操作挙動に先立つ所定の期間（time period）内における前記デバイス上の複数の過去の操作挙動に関するすべてのユーザアイデンティティ情報を取得するステップと；

前記ユーザアイデンティティ情報の各々において表現されるユーザアイデンティティ解析位置を解析し、前記期間における前記デバイス上のユーザアイデンティティ解析位置の数を算定するステップと；

前記期間における前記デバイス上のユーザアイデンティティ解析位置の数に応じて前記現在の操作挙動がアカウント盗難リスクを有するか否かを判定するステップと；を備える。

【０００８】

好ましくは、前記ユーザアイデンティティ情報は、ユーザ登録情報におけるクレデンシャル情報を含み；前記ユーザアイデンティティ情報の各々において表現されるユーザアイデンティティ解析位置を解析し、前記期間における前記デバイス上のユーザアイデンティティ解析位置の数を算定する前記ステップは：各ユーザ登録情報におけるクレデンシャルタイプ及びクレデンシャル番号に応じて前記ユーザアイデンティティ解析位置を取得し、前記デバイス上のユーザアイデンティティ解析位置の数を算定するステップを備える。

【０００９】

好ましくは、各ユーザ登録情報におけるクレデンシャルタイプ及びクレデンシャル番号に応じて前記ユーザアイデンティティ解析位置を取得し、前記デバイス上のユーザアイデンティティ解析位置の数を算定する前記ステップは：

前記クレデンシャルタイプのクラスに応じて前記ユーザアイデンティティ解析位置の解析モードを決定するステップと；

前記クレデンシャルタイプが中国の国内居住者のＩＤカードである場合、各クレデンシャル番号の先頭６桁を解析して、前記ユーザアイデンティティ解析位置を取得し、それに応じて前記デバイス上のユーザアイデンティティ解析位置の数を算定するステップ；又は

前記クレデンシャルタイプが中国の国内非居住者のＩＤカードであるか国外のクレデンシャルである場合、各クレデンシャルタイプ又は各クレデンシャル番号が１つのユーザアイデンティティ解析位置に対応すると推定し、それに応じて前記デバイス上のユーザアイデンティティ解析位置の数を算定するステップと；を備える。

【００１０】

好ましくは、現在の操作挙動に関する情報に応じて操作挙動を受けるデバイスのデバイス情報を収集する前記ステップは：前記デバイスのデバイス識別コードを収集することによって前記デバイスの対応するデバイス情報を取得するステップを備える。

【００１１】

好ましくは、前記デバイスのデバイス識別コードを収集することによって前記デバイスの対応するデバイス情報を取得する前記ステップは：

前記デバイスのタイプに応じて前記収集したデバイス情報のコンテンツを決定するステップを備え、
前記デバイスがＰＣである場合、前記収集したデバイス情報はＭＡＣ、ＩＰ、及び／又はＵＭＩＤを含み、
前記デバイスが携帯端末である場合、前記収集したデバイス情報はＭＡＣ、ＩＭＥＩ、ＴＩＤ、及び／又は携帯電話番号を含む。

【００１２】

好ましくは、前記デバイスのデバイス識別コードを収集することによって前記デバイスの対応するデバイス情報を取得する前記ステップは：
前記デバイス識別コードから識別されるデバイスの数量に応じて前記デバイス上のユーザアイデンティティ解析位置の数を算定するモードを決定するステップと；
一意のデバイスが識別された場合、前記デバイス上のユーザアイデンティティ解析位置の数を解析及び算定するステップ；又は
複数のデバイスが識別された場合、各デバイス上のユーザアイデンティティ解析位置の数を解析及び算定するステップ；又は
デバイスが識別されない場合、前記デバイス上のユーザアイデンティティ解析位置の数を０に設定するステップと；
得られた前記デバイス上のユーザアイデンティティ解析位置の数を所定のスコアリングモデルの入力変数として用いて、前記デバイスのアカウント盗難リスクレベルを評価するステップと；を備える。

【００１３】

好ましくは、前記期間における前記デバイス上のユーザアイデンティティ解析位置の数に応じて、前記現在の操作挙動がアカウント盗難リスクを有するか否かを判定する前記ステップは：前記デバイス上のユーザの総数、前記現在の操作挙動のユーザにバインドされた（結び付けられた）携帯電話番号の数、前記現在のユーザの過去の操作挙動に対するデバイスの数、前記現在のユーザの前記過去の操作挙動のＩＰアドレスの数、前記現在のユーザの前記現在の操作挙動に関する前記情報と前記過去の操作挙動に関する情報との差分、及び／又は前記現在の操作挙動のルーティング特徴情報が前記過去の操作挙動のルーティング特徴情報と同一であるか否か、と組み合わせて、前記現在の操作挙動の前記ユーザのアカウント盗難リスクレベルを評価するステップを備える。

【００１４】

好ましくは、前記期間における前記デバイス上のユーザアイデンティティ解析位置の数に応じて、前記現在の操作挙動がアカウント盗難リスクを有するか否かを判定する前記ステップは：前記デバイスの前記アカウント盗難リスクレベル及び前記現在の操作挙動の前記ユーザの前記アカウント盗難リスクレベルと組み合わせてアカウント盗難リスク値を算定し、前記リスク値が所定の閾値を超える場合にアカウント盗難を識別するステップを更に備える。

【００１５】

これに基づき、本願は、アカウント盗難リスクの識別装置を更に提供し、本装置は：
現在の操作挙動に関する情報に応じて操作挙動を受けるデバイスのデバイス情報を収集するよう構成されたデバイス情報収集モジュールと；
前記現在の操作挙動に先立つ所定の期間内における前記デバイス上の過去の操作挙動に関するすべてのユーザアイデンティティ情報を取得するよう構成されたユーザ情報取得モジュールと；
前記ユーザアイデンティティ情報の各々において表現されるユーザアイデンティティ解析位置を解析し、前記期間における前記デバイス上のユーザアイデンティティ解析位置の数を算定するよう構成されたユーザアイデンティティ解析モジュールと；
前記期間における前記デバイス上のユーザアイデンティティ解析位置の数に応じて、前記現在の操作挙動がアカウント盗難リスクを有するか否かを判定するよう構成されたアカウント盗難リスク評価モジュールと；を備える。

【００１６】
好ましくは、前記ユーザアイデンティティ情報は、ユーザ登録情報におけるクレデンシャル情報を含み；前記ユーザアイデンティティ解析モジュールは、各ユーザ登録情報におけるクレデンシャルタイプ及びクレデンシャル番号に応じて前記ユーザアイデンティティ解析位置を取得し、前記デバイス上のユーザアイデンティティ解析位置の数を算定する。
【００１７】
好ましくは、前記ユーザアイデンティティ解析モジュールは：
前記クレデンシャルタイプのクラスに応じて、前記ユーザアイデンティティ解析位置の解析モードを決定し；前記クレデンシャルタイプが中国の国内居住者のＩＤカードである場合、各クレデンシャル番号の先頭６桁を解析して、前記ユーザアイデンティティ解析位置を取得し、それに応じて前記デバイス上のユーザアイデンティティ解析位置の数を算定し、又は、前記クレデンシャルタイプが中国の国内非居住者のＩＤカードであるか国外のクレデンシャルである場合、各クレデンシャルタイプ又は各クレデンシャル番号が１つのユーザアイデンティティ解析位置に対応すると推定し、それに応じて前記デバイス上のユーザアイデンティティ解析位置の数を算定する。
【００１８】
好ましくは、前記デバイス情報収集モジュールは、前記デバイスのデバイス識別コードを収集することによって前記デバイスの対応するデバイス情報を取得する。
【００１９】
好ましくは、前記デバイス情報収集モジュールは、前記デバイスのタイプに応じて前記収集したデバイス情報のコンテンツを決定し、前記デバイスがＰＣである場合、前記収集したデバイス情報はＭＡＣ、ＩＰ、及び／又はＵＭＩＤを含み；前記デバイスが携帯端末である場合、前記収集したデバイス情報はＭＡＣ、ＩＭＥＩ、ＴＩＤ、及び／又は携帯電話番号を含む。
【００２０】
好ましくは、前記ユーザアイデンティティ解析モジュールは：前記デバイス情報収集モジュールによって前記デバイス識別コードから識別されるデバイスの数量に応じて、前記デバイス上のユーザアイデンティティ解析位置の数を算定するモードを決定し；一意のデバイスが識別された場合、前記デバイス上のユーザアイデンティティ解析位置の数を解析及び算定し、又は、複数のデバイスが識別された場合、各デバイス上のユーザアイデンティティ解析位置の数を解析及び算定し、又は、デバイスが識別されない場合、前記デバイス上のユーザアイデンティティ解析位置の数を０に設定し；得られた前記デバイス上のユーザアイデンティティ解析位置の数を、前記アカウント盗難リスク評価モジュールの所定のスコアリングモデルの入力変数として用いて、前記デバイスのアカウント盗難リスクレベルを評価する。
【００２１】
好ましくは、前記アカウント盗難リスク評価モジュールは、前記デバイス上のユーザの総数、前記現在の操作挙動のユーザにバインドされた携帯電話番号の数、前記現在のユーザの過去の操作挙動に対するデバイスの数、前記現在のユーザの前記過去の操作挙動のＩＰアドレスの数、前記現在のユーザの前記現在の操作挙動に関する前記情報と前記過去の操作挙動に関する情報との差分、及び／又は前記現在の操作挙動のルーティング特徴情報が前記過去の操作挙動のルーティング特徴情報と同一であるか否か、と組み合わせて、前記現在の操作挙動の前記ユーザのアカウント盗難リスクレベルを評価する。
【００２２】
好ましくは、前記アカウント盗難リスク評価モジュールは、前記デバイスの前記アカウント盗難リスクレベル及び前記現在の操作挙動の前記ユーザの前記アカウント盗難リスクレベルと組み合わせてアカウント盗難リスク値を算定し、前記リスク値が所定の閾値を超える場合にアカウント盗難を識別する。
【００２３】
これに基づき、本願は、アカウント盗難リスク防止・制御システムを提供し、本システ

ムは：上記のリスク識別装置と、アカウント盗難通知装置と、リスク処理装置とを備え、
前記リスク識別装置は、操作挙動プラットフォームにおけるアカウント盗難リスク値を算定し、前記リスク値が所定の閾値を超える場合、アカウント盗難を識別するよう構成され；
前記アカウント盗難通知装置は、前記リスク識別装置がアカウント盗難を識別した場合、前記リスク処理装置及びユーザ受信デバイスへアカウント盗難メッセージを通知するよう構成され；
前記リスク処理装置は、前記アカウント盗難メッセージを受信した場合、ユーザの盗難に遭ったアカウントをブロックし、前記盗難に遭ったアカウントに関連するリスクデータを傍受するよう構成される。

【００２４】
好ましくは、本システムは、前記リスク処理装置が前記リスクデータを検査し、前記リスク識別装置が前記スコアリングモデルを認証するために、前記リスク処理装置が傍受した前記リスクデータを記憶するよう構成された事例データベースを備える。

【００２５】
従来技術に対し、本願は、デバイス上のユーザアイデンティティ解析位置の数に基づきアカウント盗難リスクを識別する解決策を提供する。それは、操作挙動に先立つ期間におけるログオンデバイス上のすべてのユーザアイデンティティ情報を収集してデバイス上のユーザアイデンティティ解析位置の数を解析及び算定し、当該算定をリスクスコアリングモデルの入力変数として用いてアカウント盗難リスクレベルを評価し、それによりアカウント盗難リスクを判別する力を効果的に向上させる。なぜなら、近過去（a recent period）におけるログオンデバイス上の操作挙動のすべてのユーザの異なるアイデンティティ解析位置は、より効果的で安定した変数だからである。操作挙動が起きた際、もしデバイスが近過去において複数の異なるアイデンティティ解析位置を有するならば、操作挙動のアカウントは盗難に遭っているリスクが高い。一方、１つのデバイス上では、異なるユーザの操作挙動が同一箇所にある状況の方が、異なるユーザの操作挙動が異なる箇所にある状況よりも一般的であるため、当該変数は、複数のユーザが操作挙動を起こしているがリスクは高くない幾つかの状況を効果的に排除でき、よってリスクスコアリングモデルの変数のリスク判別力及び安定性を向上し易くする。

【図面の簡単な説明】

【００２６】
上記以外の様々な利点及び便益は、以下の好ましい実施に関する詳細な記載を読んだ当業者には明らかとなろう。添付の図面は単に好ましい実施を例示するためのものにすぎず、本願をそれらに限定するとみなすべきではない。また、添付するすべての図面において、同一の符号を用いて同一の部分を表す。

【００２７】
添付の図面において：
【図１】図１は、現在の操作挙動に先立つ７日間におけるネットワークプラットフォームのＭＡＣデバイス上のユーザアイデンティティ解析位置の数とアカウント盗難リスクとの関係を示す。
【図２】図２は、本願の実施の形態によるアカウント盗難リスクの識別方法のフローチャートである。
【図３】図３は、本願の実施の形態によるアカウント盗難リスクの識別装置のブロック図である。
【図４】図４は、本願の実施の形態によるアカウント盗難リスクの防止・制御システムのブロック図である。

【発明を実施するための形態】

【００２８】
以下、本願の実施の形態のそれぞれにおいて、このような入力変数、すなわち現在の操作挙動に先立つ期間におけるデバイス上のユーザアイデンティティ解析位置の数、をリス

クスコアリングモデルへ導入し、モデルの変数のリスク判別力を向上させる。この解決策は、データマイニング技術に基づくリスクスコアリングモデルを確立する必要がある。モデリングの主要ステップには、調査対象を決定ステップ、データソースを決定するステップ、サンプリングステップ、データを探索するステップ、モデルを開発するステップ、モデルを検証するステップ等が含まれる。本願の主眼は、スコアリングモデルのための好適な入力変数を構築することである。スコアリングモデルは本願の主眼ではないため、モデリングの他の詳細については説明しない。詳細については従来技術を参照されたい。

【００２９】

好適な変数を構築するために、本願の発明者は、ネットワークプラットフォーム上でユーザの操作挙動の大規模なデータを収集して、データ解析及びデータマイニングを実行する。例えば、プラットフォームについては、ユーザの操作挙動が起こる毎にデバイス情報を収集してよく、更に、プラットフォーム上で、近過去においてこれらデバイスで操作挙動を起こしたユーザの人数を算定してもよい。アカウント盗難リスクは、プラットフォーム上の各デバイスのユーザの人数に応じて識別してよい。しかし、誤判断の問題が起きやすい。上記データ解析により、本願の発明者は次のことを発見する。すなわち、プラットフォーム上の同一デバイス上の操作挙動について、同一位置において人々が操作挙動を起こす状況の方が、複数の異なる位置において人々が操作挙動を起こす状況よりも一般的である。よって、より効果的で安定性のある変数は、近過去においてプラットフォーム上のデバイス上で操作挙動を起こした複数のユーザの異なるアイデンティティ解析位置の数であり、アイデンティティ解析位置の解析の粒度は好ましくは県（市）である。操作挙動が起きた際、近過去においてデバイスが複数の異なるアイデンティティ解析位置を有する場合、そのような操作挙動のリスクは極めて高い。

【００３０】

上記の法則の不変性はプラットフォーム上の操作挙動において非常に高い。この法則が他のネットワークアプリケーションの操作挙動にも適用されることは言うまでもない。よって、本願における「操作挙動（operation behavior）」は、一般化された概念であって、上記のプラットフォーム上における資金及び物品の移転のビジネス行為に限定されるものではない。ユーザとサービスプラットフォームとの間のデータ交換及び様々なネットワークアプリケーションにおける複数のユーザ間のデータ交換も、本願の「操作挙動」の範囲に属する。例えば、ソーシャルネットワークのログオンは本願の「操作挙動」に属する。

【００３１】

現在の操作挙動に先立つ期間におけるデバイス上のユーザアイデンティティ解析位置の数はアカウント盗難リスクとの関連性が高いため、本願の発明者は操作挙動に先立つ所定の期間におけるデバイス上のユーザアイデンティティ解析位置の数をリスクスコアリングモデルの入力変数として用いる。このような変数によって、複数のユーザが操作挙動を起こしていてもリスクは高くない状況をある程度は排除できるため、変数のリスク判別力及び安定性は向上する。

【００３２】

以上に基づき、本願の発明者は以下の基本的概念を提案する。すなわち、現在の操作挙動に先立つ期間におけるデバイス上のユーザアイデンティティ解析位置の数を入力変数とし、デバイスのアカウント盗難リスクのレベルを所定のスコアリングモデルを用いて評価することにより、ユーザのアカウント盗難リスクをより適時に且つ効果的に識別する。この技術的概念の内容は主に３つの側面を持つ。すなわち、以下に詳述する、変数の構築、識別処理、及びモデル認証である。

【００３３】

１．変数の構築

有効な変数を構築する際には、以下で具体的に説明する変数主体、変数対象、期間、統計的指数等の因子を考慮する必要がある。

【００３４】

（１）変数主体：操作挙動（決済プラットフォーム上の操作挙動等）のログオンデバイスのデバイス情報。デバイス情報は、メディアアクセス制御（Ｍｅｄｉｕｍ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ （ＭＡＣ））物理アドレス、標準映像素材識別子（Ｕｎｉｑｕｅ Ｍａｔｅｒｉａｌ Ｉｄｅｎｔｉｆｉｅｒ （ＵＭＩＤ））、インターネットプロトコル（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ （ＩＰ））アドレス、国際移動体装置識別番号（Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｍｏｂｉｌｅ Ｅｑｕｉｐｍｅｎｔ Ｉｄｅｎｔｉｔｙ （ＩＭＥＩ））、スレッド識別子（ＴＨＲＥＡＤ Ｉｄｅｎｔｉｆｉｅｒ （ＴＩＤ）、携帯電話番号などの、デバイスのデバイス識別コードを収集することによって識別してよい。一般に、パーソナルコンピュータ（ＰＣ）については、デバイスのＭＡＣ、ＩＰ、及び／又はＵＭＩＤが収集されてよく、携帯端末については、デバイスのＭＡＣ、ＩＭＥＩ、ＴＩＤ、及び／又は携帯電話番号が収集されてよい。具体的な収集及び識別の解決策については従来技術を参照されたい。詳細については繰り返し説明しない。

【００３５】

（２）変数対象：操作挙動のログオンデバイス上のユーザアイデンティティ解析位置。ユーザアイデンティティ解析位置は、通常、クレデンシャルタイプ及びクレデンシャル番号によって判定される。例えば、中国の居住者のＩＤカードの先頭６桁は県（市）を表現し得る。先頭６桁を識別することで、ユーザが属する行政区を知ることができ、よってユーザアイデンティティ解析位置が取得される。

【００３６】

（３）期間：操作挙動に先立つ期間（例えば、３０分、２時間、１２時間、１日、３日、７日等）。期間は様々な操作挙動プラットフォーム間で大きく異なるが、操作挙動の要求や操作挙動の性質といった因子により具体的に判定できる。ここでは詳細に説明しない。

【００３７】

（４）統計的指数：デバイス上のユーザアイデンティティ解析位置の数を算定する。通常の操作挙動環境においては、一般に、デバイス上のユーザアイデンティティ解析位置の数は小さい。もしデバイス上のユーザアイデンティティ解析位置の数が相対的に大きければ、それは、アカウント盗難リスクが相対的に高いことを示す。これは、大規模データの解析によって得られた、非常に信頼性の高い結論である。

【００３８】

上記の各因子の組み合わせにより、本願では、具体的な変数を、現在の操作挙動に先立つ所定の期間においてデバイス上で操作挙動を起こしたすべてのユーザの異なるアイデンティティ解析位置の数として決定する。この統計的変数はモデル変数のリスク判別力を高めることができる。当該変数はアカウント盗難リスクとの関連性が高い。操作挙動に先立つ近過去においてデバイス上に複数の異なるアイデンティティ解析位置がある場合、当該デバイス上の操作挙動は相対的に高いアカウント盗難リスクを持つ。

【００３９】

２．識別工程

上記の統計をリスクスコアリングモデルの入力変数として用いた後、異なるデバイス上の複数のユーザアイデンティティ解析位置に基づきアカウント盗難リスクを識別してもよい。この利点は、変数のリスク判別力及び安定性を向上できることにある。具体的に、アカウント盗難リスクの識別は、以下の各手順に従う。

【００４０】

（１）デバイス上のアイデンティティ解析位置の数の取得。この手順は以下を含む：

ａ．現在の操作挙動のデバイス情報を取得し；操作挙動に先立つ特定の期間（例えば３日間）におけるデバイス上の操作挙動に関するすべてのユーザアイデンティティ情報を取得する；

ｂ．アイデンティティ情報を解析してアイデンティティ情報内の対応するユーザ領域を取得し、デバイス上の異なるユーザアイデンティティ解析位置の数を算定する。ここでのユーザアイデンティティ解析位置は一般に市として識別される。ここでいう「市」とは、行政区を意味し、農村地域に対する対義の概念として狭義に解釈されるべきものではない

。
ｃ．特別な場合の処理：デバイスが複数ある場合、それぞれユーザアイデンティティ解析位置の数が算定される；デバイス情報が取得できない場合、ユーザアイデンティティ解析位置の数を０に設定する。
【００４１】
（２）リスクレベルの評価
ユーザアイデンティティ解析位置の数に応じてデバイスのリスクレベルを評価する。具体的には、現在の操作挙動に先立つ所定の期間におけるデバイス上のユーザアイデンティティ解析位置の数を取得した後、それを、スコアリングのためリスクスコアリングモデルの変数として入力する。モデル内の様々な変数の各重みを包括的に考慮した後、デバイスのアカウント盗難リスクレベルが得られる。高いスコアは高いアカウント盗難リスクを示し、その場合、当該デバイスを主に監視する必要がある。
【００４２】
３．モデルの検証
入力変数「現在の操作挙動に先立つ所定の期間におけるデバイス上のユーザアイデンティティ解析位置の数」がリスクスコアリングモデルの予測効果に及ぼす影響を検証する必要がある。変数が効果的であれば、上記第２のステップの処理に応じてユーザのアカウント盗難リスクを自動的に識別できる；そうでなければ、スコアリングモデル及び関連する入力変数を再調整する必要がある。
【００４３】
本願については、モデル検証において以下の各因子を考慮する必要がある。
（１）過去の操作挙動タグが事例であるかどうか。統計的な「現在の操作挙動に先立つ所定の期間におけるデバイス上のユーザアイデンティティ解析位置の数」は、それが本願において導入される際、デバイス上の過去の操作挙動のデータと関連付けられる必要がある。それにより、導入する変数が効果的であることを証明するためである。すなわち、過去の操作挙動のデータを用いて、変数が効果的であるかどうか測定する必要がある。換言すれば、過去の操作挙動のデータは、アカウントが盗難に遭っているか否かを判別し得るということである。
【００４４】
過去の操作挙動がアカウント盗難である場合、タグは「不良」とされる。それ以外の場合、タグは「良」とされる。第２のステップを通じて識別したアカウント盗難リスクの結果が「不良」であり過去の操作挙動のタグも「不良」である場合、あるいは、第２のステップを通じて識別したアカウント盗難リスクの結果が「良」であり過去の操作挙動のタグも「良」である場合、検証に成功していると認識される。それ以外の場合、検証は失敗である。検証に成功している可能性が高い場合、それは、スコアリングモデルへ入力変数として導入した現在の操作挙動に先立つ所定の期間におけるデバイス上のユーザアイデンティティ解析位置の数が効果的であることを示す、すなわち、変数のリスク判別力が相対的に高いことを示す。
【００４５】
（２）リスク判別力の定量化
変数のリスク判別力は更に、定量化されてもよい。具体的には、アカウント盗難判別力指数「現在の操作挙動に先立つ所定の期間におけるデバイス上のアイデンティティ解析位置の数」を区分的に算定し定量化してもよい。これら定量的指数は主には２つのタイプがある。すなわち、リフト及び区間情報値（an lift and an interval Information Value）（ＩＶ）である。
【００４６】
アカウント盗難判別力指数を算定する式を以下に記載する。
リフト＝区間盗難アカウントトランザクション集中率／平均盗難アカウントトランザクション集中率
ＷＯＥ＝ｌｎ（区間非盗難アカウントトランザクションと全非盗難アカウントトランザ

クションとの比／区間盗難アカウントトランザクションと全盗難アカウントトランザクションとの比）×１００

区間ＩＶ＝ＷＯＥ×（区間非盗難アカウントトランザクションと全非盗難アカウントトランザクションとの比－区間盗難アカウントトランザクションと全盗難アカウントトランザクションとの比）

ＩＶ＝区間ＩＶの合計

【００４７】

上記の各式においては、解析の容易化のため、証拠の重み付け（Ｗｅｉｇｈｔ　Ｏｆ　Ｅｖｉｄｅｎｃｅ　（ＷＯＥ））に係数１００を乗算するが、それはデータマイニングにおける指数ｗｏｅと本質的に意味は同じである。なお、上式における「トランザクション」は一般化されたネットワーク操作挙動として解釈され得るものの、資金の支払いや商品の輸送等の実際のビジネス行為に限定されるものでないことは言うまでもない。

【００４８】

上の各式に基づき、変数「現在の操作挙動に先立つ所定の期間におけるデバイス上のアイデンティティ解析位置の数」のリスク判別力の結果を算定することにより、スコアリングモデルに導入される変数の効力を効果的に検証できる。「現在の操作挙動に先立つ７日間におけるＭＡＣデバイス上のユーザアイデンティティ解析位置の数」のアカウント盗難判別力指数を、説明のための一例として用いる。算定結果は表１に記す通りである。

【表１】

表１:操作挙動に先立つ7日間におけるMACデバイス上のユーザアイデンティティ解析位置の数のアカウント盗難判別力

区間	区間操作挙動の数	アカウント盗難操作挙動の数	区間アカウント盗難操作挙動集中率	平均アカウント盗難操作挙動集中率	リフト	区間IV値	IV値
0	578,007	1,934	0.3%	1.0%	0.33	32.07	171.74
[1,2]	704,478	4,602	0.7%	1.0%	0.65	7.9	171.74
(2,327]	48,887	6,756	13.8%	1.0%	13.82	131.77	171.74

【００４９】

表１を図形化して表現してもよい。図１において、現在の操作挙動に先立つ７日間における決済（ペイメント）プラットフォームのＭＡＣデバイス上のユーザアイデンティティ解析位置の数と、アカウント盗難リスクとの関係を示す。表１及び図１は、次のことを教示している。すなわちデバイス上のユーザアイデンティティ解析位置の数が２を上回る場合にはリフト値が１３．８２であること、つまり、７日間におけるＭＡＣデバイス上の操作挙動のユーザアイデンティティ解析位置の数に基づくアカウント盗難リスク判別力が、１３．８２倍にリフトしていることである。これは、変数のアカウント盗難判別力が非常に効果的であることを示している。

【００５０】

他の特定の場合における検証についても、同様に、定量的指数が比較的望ましい。これは、リスクスコアリングモデルに上記のような入力変数、すなわち現在の操作挙動に先立つ期間におけるデバイス上のユーザアイデンティティ解析位置の数を導入し、アカウント盗難リスクレベルを評価することにより、本願はモデル変数のリスク判別力を向上させることができ、従ってアカウント盗難リスク識別効果が比較的望ましいこと、を示している。

【００５１】

なお、表１及び図１においてはＩＶ値が比較的大きく、場合によっては「過剰な予測」という現象が起こり得る。このような現象を除去するため、本願では、デバイス上のユーザの総数、現在の操作挙動のユーザにバインドされた携帯電話番号の数、現在のユーザの過去の操作挙動に対するデバイスの数、現在のユーザの過去の操作挙動のＩＰアドレスの

数、現在のユーザの現在の操作挙動に関する情報と過去の操作挙動に関する情報との差分、及び／又は現在の操作挙動のルーティング特徴情報が過去の操作挙動のルーティング特徴情報と同一であるか否か、と組み合わせて、ユーザアカウントが盗難に遭ったか否かのリスクをより包括的に評価し、単一の変数の「過剰な予測」に起因する悪影響を除去する。

【００５２】

以上、本願において現在の操作挙動に先立つ所定の期間におけるデバイス上のユーザアイデンティティ解析位置の数の統計を用いてアカウント盗難リスクを識別することの技術的概念を、体系的かつ原理的に説明した。以下では、この技術的概念の具体的な実行の解決策を更に説明する。上記の解析に基づけば、リスクスコアリングモデル及び入力変数を決定しそれらの検証に成功した後であれば、具体的な実行にあたっては、上記の第２のステップに従いサーバ区域においてアプリケーションを展開するだけでよく、モデリング及び検証を繰り返す必要はない。

【００５３】

図２を参照すると、当図は、本願の実施の形態に係るアカウント盗難リスクの識別方法のフローチャートである。図２に示す通り、このリスク識別方法は以下に詳述するステップ２１０乃至ステップ２４０のような主要ステップを含む。

【００５４】

Ｓ２１０：現在の操作挙動に関する情報に応じて、操作挙動のログオンデバイスのデバイス情報が収集される。

【００５５】

このステップは現在の操作挙動に関する情報に応答するものであり、サーバ端末の対応するデバイスは、操作挙動のログオンデバイスのデバイス情報を収集する。このデバイス情報は、一般に、デバイスのデバイス識別コードを収集することによって得られる。

【００５６】

一般に、クライアント端末のログオンデバイスは複数のタイプに分類される。例えば、ＰＣデバイスは、通常、ＭＡＣ、ＩＰ及び／又はＵＭＩＤを有し、携帯端末は、通常、ＭＡＣ、ＩＭＥＩ、ＴＩＤ及び／又は携帯電話番号等を有する。従って、収集したデバイス情報のコンテンツはデバイスのタイプに応じて決定する必要がある。一般に、ＰＣについては、ＭＡＣ、ＩＰ及び／又はＵＭＩＤが収集され、携帯端末については、ＭＡＣ、ＴＩＤ及び／又は携帯電話番号が収集される。具体的な情報の収集及び識別方法については、従来技術を参照されたい。ここでは詳細に説明はしない。

【００５７】

なお、ステップＳ２１０における現在の操作挙動はユーザアカウントに対するログイン要求、ユーザアカウントに対する所定のデータ操作要求等であってよい。ユーザアカウントに対する所定のデータ操作要求は、ユーザアカウントに対するパスワード変更要求、ユーザアカウントに対する残高の移行要求、ユーザアカウントに対する物品のトランザクション要求等を含み得る。所定のデータ操作要求は、サーバによって事前に設定されてもよく、またクライアント端末を介しユーザによって事前に設定されてもよく、ここでは限定されないことが理解されよう。

【００５８】

ユーザがクライアント端末でユーザアカウントに対するログイン要求を開始する際、ユーザのログイン情報は一般に、ユーザ識別子、ユーザがログイン要求を開始するクライアント端末に関する情報、及びログイン要求を受け付けるサーバに関する情報を含む。よって、ユーザのログイン情報に応じてユーザのログインルーティング経路を取得し、ユーザのログインルーティング経路から現在のルーティング特徴情報を抽出する。現在の操作挙動のルーティング特徴情報が過去の操作挙動のルーティング特徴情報と同一であるか否かを比較することにより、現在の操作挙動のユーザのアカウント盗難リスクレベルも評価することができる。

【００５９】

Ｓ２２０：前記操作挙動に先立つ所定の期間内における前記デバイス上の過去の操作挙動に関するすべてのユーザアイデンティティ情報が取得される。

【００６０】

単一のアカウントの単一の操作挙動のリスクを識別することが非常に複雑で困難である一方、複数のアカウントの複数の操作挙動間の関連性をマイニングすることによるリスク識別が、非常に効果的な方法であることが理解されよう。上記の通り、本願では、現在の操作挙動に先立つ所定の期間におけるデバイス上のユーザアイデンティティ解析位置の数に応じて、デバイスのアカウント盗難リスクが評価される。これには、この期間におけるデバイス上の複数の過去の操作挙動に関するすべてのユーザアイデンティティ情報を抽出する必要があり、ユーザアイデンティティ解析位置の抽出は特に重要である。

【００６１】

実際の適用において、デバイス上のユーザについての期間（３０分、２時間、１２時間、１日、３日、７日等）は、一般に、操作挙動プラットフォーム、操作挙動要求、操作挙動の性質といった因子に応じて決定されてよい。当該期間における過去の操作挙動のユーザ情報を取得した後、ユーザのアイデンティティ領域を更に解析してもよい。当該期間におけるデバイス上のユーザアイデンティティ解析位置の数を算定した後、それをスコアリングのためリスクスコアリングモデルの変数として用いることができる。

【００６２】

Ｓ２３０：前記ユーザアイデンティティ情報の各々において表現されるユーザアイデンティティ解析位置が解析され、前記期間における前記デバイス上のユーザアイデンティティ解析位置の数が算定される。

【００６３】

上記の通り、現在の操作挙動に先立つ近過去の期間内でデバイスの決済プラットフォーム上で操作挙動を起こしたユーザの異なるアイデンティティ解析位置の数は、効果的で安定した変数である。よって、当該期間におけるデバイス上のユーザアイデンティティ解析位置の数の統計を、スコアリングのため、変数としてリスクスコアリングモデルに入力し、ユーザアカウントが盗難に遭ったか否かを識別するとの目的を最終的に達成してもよい。

【００６４】

ユーザアイデンティティ解析位置の判別の粒度はスコアリングモデルの出力結果と高度に相関していることが理解されよう。好適には、本願において、比較的好ましいアカウント盗難リスク識別効果を得るために、ユーザアイデンティティ解析位置の判別の粒度を市とする。

【００６５】

多くのネットワーク操作挙動プラットフォームでは、ユーザアカウント登録中に本名認証を実行する必要があり、これは、ネットワークセキュリティを向上させるのに適している。したがって、

各ユーザ登録情報におけるクレデンシャルタイプ及びクレデンシャル番号に応じて、前記ユーザアイデンティティ解析位置を取得し、及び、前記デバイス上のユーザアイデンティティ解析位置の数を算定する、ステップ２３０は、具体的に、前記クレデンシャルタイプのクラスに応じて前記ユーザアイデンティティ解析位置の解析モードを決定するステップである。

【００６６】

クレデンシャルタイプが中国の国内居住者のＩＤカードである場合、その先頭６桁は県（市）レベルの行政区を表現し、よって、ユーザアイデンティティ解析位置は単に各クレデンシャル番号の先頭６桁を解析することによって取得でき、それに応じてデバイス上のユーザアイデンティティ解析位置の数を算定する。

【００６７】

クレデンシャルタイプが中国の国内非居住者のＩＤカード（軍事官の証明書等）又は国外のクレデンシャル（パスポート等）である場合、ユーザアイデンティティが位置する行

政区を直接的には識別できない。しかし、このような状況は比較的稀であるため、単純に、各クレデンシャルタイプ又は各クレデンシャル番号は１つのユーザアイデンティティ解析位置に対応すると推定してよく、それに応じてデバイス上のユーザアイデンティティ解析位置の数を算定する。もちろん、モデリングの間にこれらのクレデンシャルタイプをナンバリングするモードが得られた場合は、特定のクレデンシャル番号に応じてユーザアイデンティティ解析位置を得てもよい。ここで詳細な説明は行わない。

【００６８】

なお、ステップＳ２１０で取得したデバイス情報は複数の異なる状況を含み得る。すなわち、殆どの場合、例えばＭＡＣ、ＩＭＥＩ等、複数のタイプのデバイス情報が同時に収集され得る。しかし、技術的な理由から、シナリオやシステム制約条件によっては操作挙動時のデバイス情報が収集できなかったり、あるいは、操作挙動時に収集したデバイス情報が明らかにホットスポットであり除去すべきものであったりする。このような場合には、デバイス上のユーザアイデンティティ解析位置の数を解析及び算定するモードを状況に応じて調整する必要がある。

【００６９】

よって、ステップＳ２２０乃至Ｓ２３０では、デバイス識別コードから識別されるデバイスの数量に応じてデバイス上のユーザアイデンティティ解析位置の数を算定するモードを決定する必要があり、それは具体的に：

一意のデバイスが識別された場合、一意のデバイス上の各ユーザアイデンティティ解析位置を解析し、デバイス上のユーザアイデンティティ解析位置の数を算定するステップ；

複数のデバイスが識別された場合、各デバイス上の各ユーザアイデンティティ解析位置を個別に解析し、各デバイス上のユーザアイデンティティ解析位置の数を算定するステップ；及び

デバイスが識別されない場合、デバイス上のユーザアイデンティティ解析位置の数を０に設定するステップ；を含む。

【００７０】

上記の方法で得られたデバイス上のユーザアイデンティティ解析位置の数を、所定のスコアリングモデルの入力変数としてリスクスコアリングモデルに導入してデバイスのアカウント盗難リスクレベルを評価する。よって、スコアリングモデルの変数のアカウント盗難リスク判別力を、過去の操作挙動データを用いて測定する。

【００７１】

Ｓ２４０：前記現在の操作挙動がアカウント盗難リスクを有するか否かが、前記期間における前記デバイス上のユーザアイデンティティ解析位置の数に応じて判定される。

【００７２】

概して、デバイスのアカウント盗難リスクレベルを評価するため、当該期間におけるデバイス上のユーザアイデンティティ解析位置の数が所定スコアリングモデルの入力変数として用いられる。アカウント盗難リスクレベルはアカウント盗難リスクを表現するものであり、アカウント盗難リスクレベルが特定の閾値を超える場合はアカウントが盗難に遭ったと識別され、超えていなければアカウントは盗難に遭っていないと識別される。

【００７３】

上記ステップＳ２１０乃至Ｓ２３０に応じて操作挙動に先立つ所定の期間におけるデバイス上のユーザアイデンティティ解析位置の数の統計が得られた後、スコアリングのため当該統計をリスクスコアリングモデルに導入しデバイスのアカウント盗難リスクレベルを得てよく、これによりアカウント盗難リスクを識別し、リスクを除去すべく適時に処理措置をとる。

【００７４】

上記プロセスを通じて、前記デバイスの前記アカウント盗難リスクレベルが評価された後、アカウント盗難リスク識別能力をさらに向上させるために、本願は、前記デバイス上のユーザの総数、前記現在の操作挙動のユーザにバインドされた携帯電話番号の数、前記現在のユーザの過去の操作挙動に対するデバイスの数、前記現在のユーザの前記過去の操作

挙動のＩＰアドレスの数、前記現在のユーザの前記現在の操作挙動に関する前記情報と前記過去の操作挙動に関する情報との差分、及び／又は前記現在の操作挙動のルーティング特徴情報が前記過去の操作挙動のルーティング特徴情報と同一であるか否か、と組み合わせて、前記現在の操作挙動の前記ユーザのアカウント盗難リスクレベルを評価する。このように、複数の要因と組み合わせて、本願のアカウント盗難リスクの識別能力が大幅に改善される。

【００７５】

本願では、デバイスのアカウント盗難リスクレベル及び現在の操作挙動のユーザのアカウント盗難リスクレベルと組み合わせてアカウント盗難リスク値を算定し、リスク値が所定の閾値を超えた場合にアカウント盗難を識別し、アカウント盗難が識別された場合は対応するアカウント盗難プロンプト情報を出力するため、操作挙動プラットフォーム及びユーザは適時に処理を行って潜在的なアカウント盗難の危害を除去し、よって、財産の喪失他の問題を回避する。

【００７６】

以上は、アカウント盗難リスクの識別方法（以下、方法と呼ぶ）の詳細な説明である。これに基づき、本願は、上記に対応してアカウント盗難リスクの識別装置（以下、装置と呼ぶ）を更に提供する。それについて以下で詳細に説明する。

【００７７】

なお、この実施の形態の装置において詳細に説明されない部分については、上記の方法について説明した内容を参照されたい。同様に、上記の方法において装置の構造に関するものについては、以下で説明する内容を参照してもよい。

【００７８】

図３は本願の実施の形態に係るアカウント盗難リスクの識別装置を示す。装置３００は、以下で詳述するデバイス情報収集モジュール３１０、ユーザ情報取得モジュール３２０、ユーザアイデンティティ解析モジュール３３０、アカウント盗難リスク評価モジュール３４０等の部分を含む。

【００７９】

デバイス情報収集モジュール３１０は、現在の操作挙動に関する情報に応じて、操作挙動のログオンデバイスのデバイス情報を収集してもよい。ここで、デバイス情報収集モジュール３１０は、デバイスのデバイス識別コードを収集することによりデバイスの対応するデバイス情報を取得し、デバイスのタイプに応じて収集するデバイス情報のコンテンツを具体的に決定する。すなわち、ＰＣについては、ＭＡＣ、ＩＰ、及び／又はＵＭＩＤが収集され、携帯端末については、ＭＡＣ、ＩＭＥＩ、ＴＩＤ、及び／又は携帯電話番号が収集される。

【００８０】

ユーザ情報取得モジュール３２０は、操作挙動に先立つ所定の期間内におけるデバイス上の過去の操作挙動に関するすべてのユーザアイデンティティ情報を取得してよい。対応する期間における過去の操作挙動のユーザ情報を取得した後、ユーザ情報取得モジュール３２０はユーザアイデンティティ解析モジュール３３０に対してユーザ情報を提供して各ユーザのアイデンティティ領域を解析及び取得し当該期間におけるデバイス上のユーザアイデンティティ解析位置の数を算定する。その後、当該期間におけるデバイス上のユーザアイデンティティ解析位置の数を、スコアリングのためリスクスコアリングモデルの変数として用いてよい。

【００８１】

ユーザアイデンティティ解析モジュール３３０は、ユーザアイデンティティ情報の各々において表現されるユーザアイデンティティ解析位置を解析し、当該期間におけるデバイス上のユーザアイデンティティ解析位置の数を算定してよい。特に、ユーザアイデンティティ解析モジュール３３０はユーザアイデンティティ解析位置の判別の粒度として市を用いる。ユーザアイデンティティ情報はユーザ登録情報におけるクレデンシャル情報を含む。ユーザアイデンティティ解析位置は各ユーザ登録情報におけるクレデンシャルタイプ及

びクレデンシャル番号に応じて取得され、デバイス上のユーザアイデンティティ解析位置の数が算定され、それは具体的に、クレデンシャルタイプのクラスに応じてユーザアイデンティティ解析位置の解析モードを決定するステップを含む。具体的には、クレデンシャルタイプが中国の国内居住者のＩＤカードである場合、各クレデンシャル番号の先頭６桁を解析してユーザアイデンティティ解析位置を取得し、それに応じてデバイス上のユーザアイデンティティ解析位置の数を算定し、クレデンシャルタイプが中国の国内非居住者のＩＤカードであるか国外のクレデンシャルである場合、各クレデンシャルタイプ又は各クレデンシャル番号が１つのユーザアイデンティティ解析位置に対応すると推定し、それに応じてデバイス上のユーザアイデンティティ解析位置の数を算定する。

【００８２】

それに加え、ユーザアイデンティティ解析モジュール３３０は、デバイス情報収集モジュール３１０によってデバイス識別コードから識別されるデバイスの数量に応じてデバイス上のユーザアイデンティティ解析位置の数を算定するモードを決定してよい。すなわち、一意のデバイスが識別された場合、解析が行われデバイス上のユーザアイデンティティ解析位置の数が算定され、複数のデバイスが識別された場合、解析が行われ各デバイス上のユーザアイデンティティ解析位置の数が算定され、デバイスが識別されない場合、デバイス上のユーザアイデンティティ解析位置の数は０に設定される。得られたデバイス上のユーザアイデンティティ解析位置の数は、アカウント盗難リスク評価モジュール３４０の所定のスコアリングモデルの入力変数として用いられ、デバイスのアカウント盗難リスクレベルが評価される。

【００８３】

アカウント盗難リスク評価モジュール３４０は、前記期間の前記デバイス上のユーザアイデンティティ分析位置の数を、所定のスコアリングモデルの入力変数として使用して、前記デバイスのアカウント盗難リスクレベルを評価してもよい。前記アカウント盗難リスク評価モジュール３４０は、前記デバイス上のユーザの総数、前記現在の操作挙動のユーザにバインドされた携帯電話番号の数、前記現在のユーザの過去の操作挙動に対するデバイスの数、前記現在のユーザの前記過去の操作挙動のＩＰアドレスの数、前記現在のユーザの前記現在の操作挙動に関する前記情報と前記過去の操作挙動に関する情報との差分、及び／又は前記現在の操作挙動のルーティング特徴情報が前記過去の操作挙動のルーティング特徴情報と同一であるか否か、と組み合わせて、前記現在の操作挙動の前記ユーザのアカウント盗難リスクレベルを更に評価する。

これに基づき、アカウント盗難リスク評価モジュール３４０は、前記デバイスの前記アカウント盗難リスクレベル及び前記現在の操作挙動の前記ユーザの前記アカウント盗難リスクレベルと組み合わせてアカウント盗難リスク値を算定し、前記リスク値が所定の閾値を超える場合にアカウント盗難を識別する。

【００８４】

以上、本願のアカウント盗難リスクの識別装置を説明したが、それは、アカウント盗難リスクの識別において所望の判別力を有し、リスクの識別において比較的良好な安定性を有する。これに基づき、本願においては、上記に対応してアカウント盗難リスクの防止・制御システムが確立される。それについて簡単に以下説明する。

【００８５】

図４は、本願の実施の形態に係るアカウント盗難リスクの防止・制御システムを示す。当該リスク防止・制御システムは、ユーザ（不図示）と操作挙動プラットフォーム（不図示）との間の操作挙動リスクの防止・制御に適用できる。このシステムは、リスク識別装置３００、アカウント盗難通知装置２００、リスク処理装置１００及び事例データベース４００を含む。

【００８６】

リスク防止・制御システムの各部の接続関係は、図４に示すとおりであり、機能を実行するための対応するプロセスは以下のとおりである：前記リスク識別装置３００は、操作挙動プラットフォームにおけるアカウント盗難リスク値を算定し、前記リスク値が所定の

閾値を超える場合、アカウント盗難を識別し；前記アカウント盗難通知装置２００は、前記リスク識別装置１００がアカウント盗難を識別した場合、前記リスク処理装置４００及びユーザ受信デバイス（例えば、携帯電話）５００へアカウント盗難メッセージを通知し；　前記リスク処理装置１００は、前記アカウント盗難メッセージを受信した場合、ユーザの盗難に遭ったアカウントをブロックし、前記盗難に遭ったアカウントに関連するリスクデータを傍受し；事例データベース４００は、前記リスク処理装置３００が前記リスクデータを検査し前記リスク識別装置１００が前記スコアリングモデルを認証するために、前記リスク処理装置１００が傍受した前記リスクデータを記憶する。

【００８７】

上記のリスク防止・制御システムにおけるリスク識別装置３００については、図３に示す構造を参照されたい。他の各装置は、従来のデバイスやアプリケーションから選択してよい。このようなリスクの防止・制御システムはユーザアカウント盗難リスクを適時に識別でき、アカウントが盗難に遭ったと確認されると、安全なネットワーク操作挙動の環境が良好に提供されるよう適時に処理を実行できる。よって、所望のアプリケーション値を達成できる。

【００８８】

本願が十分に理解されるように、以下の説明では数々の詳細を例示する。しかし、本願は、ここで説明される形態とは異なる他の多くの形態で実施されてよい。当業者は、本願の概念から逸脱することなく、類似する一般化が可能であろう。よって本願は以下の具体的な実施の形態に限定されるものではない。

【００８９】

以上、好ましい実施の形態を用いて本願を説明したが、本願はこれらの好ましい実施の形態に限定することを意図してはいない。当業者は、本願の趣旨及び範囲から逸脱することなく可能な変更及び変形を施してもよい。よって、本願の保護範囲は、本願の請求の範囲によって規定される範囲に従うものである。

【００９０】

典型的な構成では、計算デバイスは１つ以上のプロセッサ（ＣＰＵ）、入／出力インターフェース、ネットワークインターフェース、及びメモリを含む。

【００９１】

メモリは、揮発性メモリ、ランダムアクセスメモリ（ＲＡＭ）、及び／又は、例えば読出し専用メモリ（ＲＯＭ）又はフラッシュＲＡＭのようなコンピュータで読取り可能な媒体内の不揮発性メモリなどを含んでよい。メモリはコンピュータで読取り可能な媒体の一例である。

【００９２】

コンピュータで読取り可能な媒体は、不揮発性又は揮発性媒体、可動又は非可動媒体を含み、また、任意の方法あるいは技術によって情報記憶を実行できる。情報はコンピュータで読取り可能な命令、数値構造、及びプログラム又はその他の数値のモジュールであってよい。コンピュータの記憶媒体は、例えば、相変化メモリ（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）、その他のタイプのランダムアクセスメモリ（ＲＡＭ）、読出し専用メモリ（ＲＯＭ）、電気的消去再書込み可能な読出し専用メモリ（ＥＥＰＲＯＭ）、フラッシュメモリ若しくはその他のメモリ技術、コンパクトディスク読取り専用メモリ（ＣＤ－ＲＯＭ）、デジタル多目的ディスク（ＤＶＤ）若しくはその他の光学記憶装置、カセットテープ、磁気テープ／磁気ディスク記憶装置若しくはその他の磁気記憶デバイス、又は任意のその他の非伝送媒体を非限定的に含み、また、アクセス可能な情報を保存するために計算デバイスを使用できる。本明細書での定義によれば、コンピュータで読取り可能な媒体は、変調データ信号及び搬送波のような一時的媒体を含まない。

【００９３】

当業者は、本願の実施の形態を、方法、システム、コンピュータプログラム製品として提供できることを理解すべきである。したがって、本願は、完全なハードウェアの実施の

形態、完全なソフトウェアの実施の形態、又はソフトウェアとハードウェアの組み合わせの実施の形態の形態で実施できる。さらに、本願は、１つ以上のコンピュータで使用可能な記憶媒体（磁気ディスクメモリ、ＣＤ－ＲＯＭ、光学メモリなどを非限定的に含む）上で実施できるコンピュータプログラム製品（コンピュータで使用可能なプログラムコードを含む）の形態を採ることができる。

［第１の局面］

アカウント盗難リスクの識別方法であって：

現在の操作挙動に関する情報に応じて操作挙動を受けるデバイスのデバイス情報を収集するステップと；

前記現在の操作挙動に先立つ所定の期間内における前記デバイス上の複数の過去の操作挙動に関するすべてのユーザアイデンティティ情報を取得するステップと；

前記ユーザアイデンティティ情報の各々において表現されるユーザアイデンティティ解析位置を解析し、前記期間における前記デバイス上のユーザアイデンティティ解析位置の数を算定するステップと；

前記期間における前記デバイス上のユーザアイデンティティ解析位置の数に応じて前記現在の操作挙動がアカウント盗難リスクを有するか否かを判定するステップと；を備える、

アカウント盗難リスクの識別方法。

［第２の局面］

前記ユーザアイデンティティ情報はユーザ登録情報におけるクレデンシャル情報を含み；

前記ユーザアイデンティティ情報の各々において表現されるユーザアイデンティティ解析位置を解析し、前記期間における前記デバイス上のユーザアイデンティティ解析位置の数を算定する前記ステップは：

各ユーザ登録情報におけるクレデンシャルタイプ及びクレデンシャル番号に応じて前記ユーザアイデンティティ解析位置を取得し、前記デバイス上のユーザアイデンティティ解析位置の数を算定するステップを備える、

第１の局面に記載のリスクの識別方法。

［第３の局面］

各ユーザ登録情報におけるクレデンシャルタイプ及びクレデンシャル番号に応じて前記ユーザアイデンティティ解析位置を取得し、前記デバイス上のユーザアイデンティティ解析位置の数を算定する前記ステップは：

前記クレデンシャルタイプのクラスに応じて前記ユーザアイデンティティ解析位置の解析モードを決定するステップと；

前記クレデンシャルタイプが中国の国内居住者のＩＤカードである場合、各クレデンシャル番号の先頭６桁を解析して、前記ユーザアイデンティティ解析位置を取得し、それに応じて前記デバイス上のユーザアイデンティティ解析位置の数を算定するステップ；又は

前記クレデンシャルタイプが中国の国内非居住者のＩＤカードであるか国外のクレデンシャルである場合、各クレデンシャルタイプ又は各クレデンシャル番号が１つのユーザアイデンティティ解析位置に対応すると推定し、それに応じて前記デバイス上のユーザアイデンティティ解析位置の数を算定するステップと；を備える、

第２の局面に記載のリスクの識別方法。

［第４の局面］

現在の操作挙動に関する情報に応じて操作挙動を受けるデバイスのデバイス情報を収集する前記ステップは：

前記デバイスのデバイス識別コードを収集することによって前記デバイスの対応するデバイス情報を取得するステップを備える、

第１の局面に記載のリスクの識別方法。

［第５の局面］

前記デバイスのデバイス識別コードを収集することによって前記デバイスの対応するデ

バイス情報を取得する前記ステップは：
前記デバイスのタイプに応じて前記収集したデバイス情報のコンテンツを決定するステップを備え、
前記デバイスがＰＣである場合、前記収集したデバイス情報はＭＡＣ、ＩＰ、及び／又はＵＭＩＤを含み、
前記デバイスが携帯端末である場合、前記収集したデバイス情報はＭＡＣ、ＩＭＥＩ、ＴＩＤ、及び／又は携帯電話番号を含む、
第４の局面に記載のリスクの識別方法。
［第６の局面］
前記デバイスのデバイス識別コードを収集することによって前記デバイスの対応するデバイス情報を取得する前記ステップは：
前記デバイス識別コードから識別されるデバイスの数量に応じて前記デバイス上のユーザアイデンティティ解析位置の数を算定するモードを決定するステップと；
一意のデバイスが識別された場合、前記デバイス上のユーザアイデンティティ解析位置の数を解析及び算定するステップ；又は、複数のデバイスが識別された場合、各デバイス上のユーザアイデンティティ解析位置の数を解析及び算定するステップ；又は、デバイスが識別されない場合、前記デバイス上のユーザアイデンティティ解析位置の数を０に設定するステップと；
得られた前記デバイス上のユーザアイデンティティ解析位置の数を所定のスコアリングモデルの入力変数として用いて、前記デバイスのアカウント盗難リスクレベルを評価するステップと；を備える、
第４の局面に記載のリスクの識別方法。
［第７の局面］
前記期間における前記デバイス上のユーザアイデンティティ解析位置の数に応じて、前記現在の操作挙動がアカウント盗難リスクを有するか否かを判定する前記ステップは：
前記デバイス上のユーザの総数、前記現在の操作挙動のユーザにバインドされた携帯電話番号の数、前記現在のユーザの過去の操作挙動に対するデバイスの数、前記現在のユーザの前記過去の操作挙動のＩＰアドレスの数、前記現在のユーザの前記現在の操作挙動に関する前記情報と前記過去の操作挙動に関する情報との差分、及び／又は前記現在の操作挙動のルーティング特徴情報が前記過去の操作挙動のルーティング特徴情報と同一であるか否か、と組み合わせて、前記現在の操作挙動の前記ユーザのアカウント盗難リスクレベルを評価するステップを備える、
第１の局面乃至第６の局面のいずれか一項に記載のリスクの識別方法。
［第８の局面］
前記期間における前記デバイス上のユーザアイデンティティ解析位置の数に応じて、前記現在の操作挙動がアカウント盗難リスクを有するか否かを判定する前記ステップは：
前記デバイスの前記アカウント盗難リスクレベル及び前記現在の操作挙動の前記ユーザの前記アカウント盗難リスクレベルと組み合わせてアカウント盗難リスク値を算定し、前記リスク値が所定の閾値を超える場合にアカウント盗難を識別するステップを更に備える、
第７の局面に記載のリスク識別方法。
［第９の局面］
アカウント盗難リスクの識別装置であって：
現在の操作挙動に関する情報に応じて操作挙動を受けるデバイスのデバイス情報を収集するよう構成されたデバイス情報収集モジュールと；
前記現在の操作挙動に先立つ所定の期間内における前記デバイス上の過去の操作挙動に関するすべてのユーザアイデンティティ情報を取得するよう構成されたユーザ情報取得モジュールと；
前記ユーザアイデンティティ情報の各々において表現されるユーザアイデンティティ解析位置を解析し、前記期間における前記デバイス上のユーザアイデンティティ解析位置の

数を算定するよう構成されたユーザアイデンティティ解析モジュールと；
前記期間における前記デバイス上のユーザアイデンティティ解析位置の数に応じて、前記現在の操作挙動がアカウント盗難リスクを有するか否かを判定するよう構成されたアカウント盗難リスク評価モジュールと；を備える、
アカウント盗難リスク識別装置。
［第１０の局面］
前記ユーザアイデンティティ情報は、ユーザ登録情報におけるクレデンシャル情報を含み；
前記ユーザアイデンティティ解析モジュールは、各ユーザ登録情報におけるクレデンシャルタイプ及びクレデンシャル番号に応じて前記ユーザアイデンティティ解析位置を取得し、前記デバイス上のユーザアイデンティティ解析位置の数を算定する、
第９の局面に記載のリスク識別装置。
［第１１の局面］
前記ユーザアイデンティティ解析モジュールは：
前記クレデンシャルタイプのクラスに応じて、前記ユーザアイデンティティ解析位置の解析モードを決定し；
前記クレデンシャルタイプが中国の国内居住者のＩＤカードである場合、各クレデンシャル番号の先頭６桁を解析して、前記ユーザアイデンティティ解析位置を取得し、それに応じて前記デバイス上のユーザアイデンティティ解析位置の数を算定し；又は、前記クレデンシャルタイプが中国の国内非居住者のＩＤカードであるか国外のクレデンシャルである場合、各クレデンシャルタイプ又は各クレデンシャル番号が１つのユーザアイデンティティ解析位置に対応すると推定し、それに応じて前記デバイス上のユーザアイデンティティ解析位置の数を算定する；
第１０の局面に記載のリスク識別装置。
［第１２の局面］
前記デバイス情報収集モジュールは、前記デバイスのデバイス識別コードを収集することによって前記デバイスの対応するデバイス情報を取得する、
第９の局面に記載のリスク識別装置。
［第１３の局面］
前記デバイス情報収集モジュールは：
前記デバイスのタイプに応じて前記収集したデバイス情報のコンテンツを決定し；
前記デバイスがＰＣである場合、前記収集したデバイス情報はＭＡＣ、ＩＰ、及び／又はＵＭＩＤを含み；
前記デバイスが携帯端末である場合、前記収集したデバイス情報はＭＡＣ、ＩＭＥＩ、ＴＩＤ、及び／又は携帯電話番号を含む；
第１２の局面に記載のリスク識別装置。
［第１４の局面］
前記ユーザアイデンティティ解析モジュールは：
前記デバイス情報収集モジュールによって前記デバイス識別コードから識別されるデバイスの数量に応じて、前記デバイス上のユーザアイデンティティ解析位置の数を算定するモードを決定し；
一意のデバイスが識別された場合、前記デバイス上のユーザアイデンティティ解析位置の数を解析及び算定し；又は、複数のデバイスが識別された場合、各デバイス上のユーザアイデンティティ解析位置の数を解析及び算定し；又は、デバイスが識別されない場合、前記デバイス上のユーザアイデンティティ解析位置の数を０に設定し；
得られた前記デバイス上のユーザアイデンティティ解析位置の数を、前記アカウント盗難リスク評価モジュールの所定のスコアリングモデルの入力変数として用いて、前記デバイスのアカウント盗難リスクレベルを評価する；
第９の局面に記載のリスク識別装置。
［第１５の局面］

前記アカウント盗難リスク評価モジュールは、前記デバイス上のユーザの総数、前記現在の操作挙動のユーザにバインドされた携帯電話番号の数、前記現在のユーザの過去の操作挙動に対するデバイスの数、前記現在のユーザの前記過去の操作挙動のＩＰアドレスの数、前記現在のユーザの前記現在の操作挙動に関する前記情報と前記過去の操作挙動に関する情報との差分、及び／又は前記現在の操作挙動のルーティング特徴情報が前記過去の操作挙動のルーティング特徴情報と同一であるか否か、と組み合わせて、前記現在の操作挙動の前記ユーザのアカウント盗難リスクレベルを評価する、

第９の局面乃至第１４の局面のいずれか一項に記載のリスク識別装置。

［第１６の局面］

前記アカウント盗難リスク評価モジュールは、前記デバイスの前記アカウント盗難リスクレベル及び前記現在の操作挙動の前記ユーザの前記アカウント盗難リスクレベルと組み合わせてアカウント盗難リスク値を算定し、前記リスク値が所定の閾値を超える場合にアカウント盗難を識別する、

第１５の局面に記載のリスク識別装置。

［第１７の局面］

第９の局面乃至第１６の局面のいずれか一項に記載の前記リスク識別装置と、アカウント盗難通知装置と、リスク処理装置とを備えるアカウント盗難リスク防止・制御システムであって、

前記リスク識別装置は、操作挙動プラットフォームにおけるアカウント盗難リスク値を算定し、前記リスク値が所定の閾値を超える場合、アカウント盗難を識別するよう構成され；

前記アカウント盗難通知装置は、前記リスク識別装置がアカウント盗難を識別した場合、前記リスク処理装置及びユーザ受信デバイスへアカウント盗難メッセージを通知するよう構成され；

前記リスク処理装置は、前記アカウント盗難メッセージを受信した場合、ユーザの盗難に遭ったアカウントをブロックし、前記盗難に遭ったアカウントに関連するリスクデータを傍受するよう構成される；

アカウント盗難リスク防止・制御システム。

［第１８の局面］

前記リスク処理装置が前記リスクデータを検査し、前記リスク識別装置が前記スコアリングモデルを認証するために、前記リスク処理装置が傍受した前記リスクデータを記憶するよう構成される事例データベースを更に備える、

第１７の局面に記載の前記リスク防止・制御システム。

【図１】

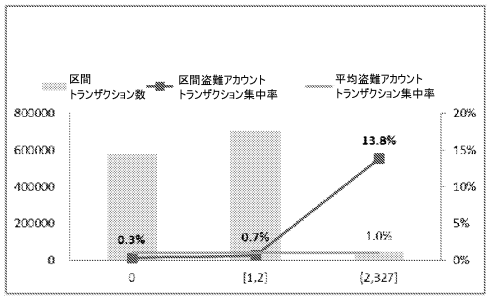

図1

【図２】

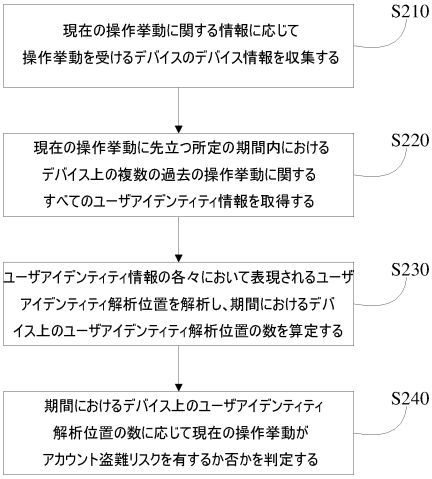

図2

【図３】

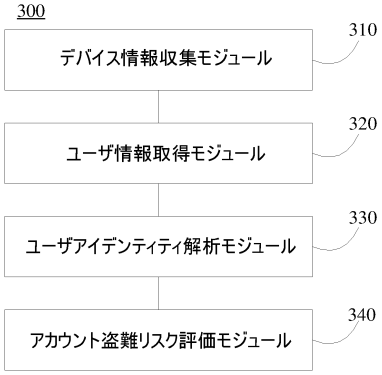

図3

【図４】

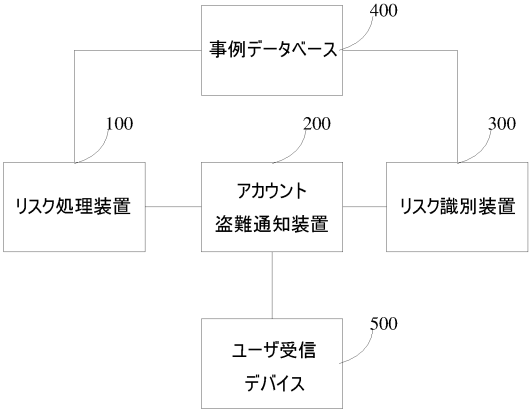

図4

フロントページの続き

(74)代理人 100155192
弁理士 金子 美代子
(74)代理人 100131820
弁理士 金井 俊幸
(74)代理人 100100398
弁理士 柴田 茂夫
(72)発明者 タン，チュンピン
中華人民共和国 ３１００９９，ハンヂョウ，ナンバー１８ ワンタン ロード，フアンロン タイムズ プラザ，ビルディング ビー １７エフ，アンツ パテント チーム内

審査官 平井 誠

(56)参考文献 米国特許出願公開第２０１３／０２５４８５７（ＵＳ，Ａ１）
米国特許出願公開第２０１０／０１３０１７２（ＵＳ，Ａ１）
特表２００８－５０３００１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／００－８８