【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】令和1年6月13日(2019.6.13)

【公表番号】特表2018-519586(P2018-519586A)
【公表日】平成30年7月19日(2018.7.19)
【年通号数】公開・登録公報2018-027
【出願番号】特願2017-562009(P2017-562009)
【国際特許分類】
Ｇ０６Ｆ　21/55　(2013.01)
Ｈ０４Ｍ　11/00　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　21/55　３２０
Ｈ０４Ｍ　11/00　３０２

【手続補正書】
【提出日】令和1年5月7日(2019.5.7)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【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；
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。
【手続補正２】
【補正対象書類名】明細書

【補正対象項目名】００９３
【補正方法】変更
【補正の内容】
【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。