(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2023-539711
(P2023-539711A)
(43)公表日　令和5年9月19日(2023.9.19)

(51)国際特許分類	FI	テーマコード（参考）
G06Q 30/018 (2023.01)	G06Q 30/018	5L049

審査請求　未請求　予備審査請求　未請求　（全41頁）

(21)出願番号　特願2022-575881(P2022-575881)
(86)(22)出願日　令和3年6月22日(2021.6.22)
(85)翻訳文提出日　令和4年12月9日(2022.12.9)
(86)国際出願番号　PCT/US2021/038551
(87)国際公開番号　WO2021/262767
(87)国際公開日　令和3年12月30日(2021.12.30)
(31)優先権主張番号　63/042,527
(32)優先日　令和2年6月22日(2020.6.22)
(33)優先権主張国・地域又は機関
米国(US)
(81)指定国・地域　AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,
最終頁に続く

(71)出願人　519135574
アイディー メトリクス グループ インコーポレイテッド
アメリカ合衆国 ９８０３３ ワシントン州 カークランド カークランド アベニュー ８０５ スイート １０２
(74)代理人　100102978
弁理士　清水 初志
(74)代理人　100160923
弁理士　山口 裕孝
(74)代理人　100119507
弁理士　刑部 俊
(74)代理人　100142929
弁理士　井上 隆一
(74)代理人　100148699
最終頁に続く

(54)【発明の名称】　機密データに対する不正防止およびデータ保護のための速度システム

(57)【要約】
共有データベースを更新し、かつ取引を処理するための、コンピュータ記憶媒体上に符号化されたコンピュータプログラムを含む、方法、システム、および装置を開示する。いくつかの実装形態では、取引に関連する第1のデータが、第1の企業取引検証システムによって受け取られる。第1の企業取引検証システムは、セキュリティ特徴識別器層を含むように訓練されている機械学習モデルを使用して第1のデータを難読化し、かつ機械学習モデルのセキュリティ特徴識別器層によって出力されたアクティベーションのセットを取得することによって、第2のデータを生成する。第2のデータは、アクティベーションのセットを含み、共有データベースに記憶され得、ここで、認証および不正検出を支援するために、他の取引からの他のアクティベーションと比較され得る。

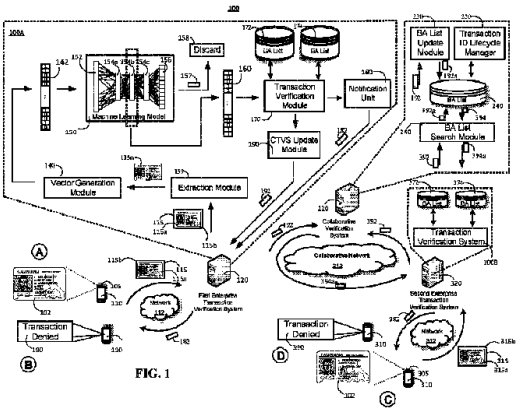


FIG. 1

【特許請求の範囲】
【請求項１】
取引検証のためのシステムであって、
1つまたは複数のプロセッサと、
該1つまたは複数のプロセッサによって実行されると、該1つまたは複数のプロセッサに、以下:
取引の当事者を識別する物理的文書の少なくとも一部分を表す第1のデータを、第1の企業取引検証システムにより受け取ること;
該第1のデータの難読化を表す第2のデータを生成することであって、
セキュリティ特徴識別器層を含むように訓練されている機械学習モデルへと、該第1のデータを入力として提供することと、
該機械学習モデルのセキュリティ特徴識別器層によって出力されたアクティベーションのセットを取得することであって、該第2のデータが該アクティベーションのセットを含む、取得することと
を含む、生成すること;
該取引が拒否されるべき取引であるかどうかを、該第1の企業取引検証システムにより、かつ該第2のデータに基づいて判定すること;
該取引が拒否されるべきであると判定したことに基づき、所定の時間量にわたって該第2のデータを含む1つまたは複数のデータレコードを含むように協調検証システムのデータベースを更新することであって、該協調検証システムが、該協調検証システムのメンバーである他の企業における該当事者による1つまたは複数の他の取引についての先制拒否を可能にする、更新すること
を含む動作を行わせる、命令
を含む、1つまたは複数の記憶デバイスと
を含む、システム。
【請求項２】
前記動作が、
前記協調検証システムによって記憶されたデータを、1つまたは複数の他の企業取引検証システムに提供すること
をさらに含む、請求項1記載のシステム。
【請求項３】
前記1つまたは複数のデータレコードが、前記協調検証システムのメンバーである前記他の企業の1つまたは複数の他の企業検証システムによってアクセス可能である、請求項1記載のシステム。
【請求項４】
所定の時間量にわたって前記第2のデータを含む1つまたは複数のデータレコードを含むように前記協調検証システムの前記データベースを更新することが、
前記第2のデータを悪質行為者リスト内の実体レコードに、前記協調検証システムにより記憶することであって、前記悪質行為者リストの各実体レコードが、少なくとも所定の時間量にわたって取引が拒否されるべき実体に対応する、記憶すること
を含む、請求項1記載のシステム。
【請求項５】
前記動作が、以下:
前記協調検証システムの前記データベースを更新した後に、
異なる取引の当事者を識別する前記物理的文書の少なくとも一部分を表す異なるデータを、第2の企業取引検証システムにより受け取ること;
該異なるデータの難読化を表す第3のデータを生成することであって、
セキュリティ特徴識別器層を含むように訓練されている第2の機械学習モデルへと、該異なるデータを入力として提供することと、
該第2の機械学習モデルのセキュリティ特徴識別器層によって出力された異なるアク

ティベーションのセットを取得することであって、該第3のデータが該異なるアクティベーションのセットを含む、取得することと
を含む、生成すること;
該第3のデータが、前記協調検証システムの前記データベースに記憶された前記第2のデータに対して所定の類似度レベルの範囲内にあると、該第2の企業取引検証システムにより判定すること;および
該第3のデータが前記第2のデータに対して所定の類似度レベルの範囲内にあると判定したことに基づき、該異なる取引が拒否されるべきであると判定すること
をさらに含む、請求項1記載のシステム。
【請求項６】
正規の物理的文書の少なくとも一部分を、入力画像を表すデータが描写している可能性を判定するように、前記機械学習モデルが訓練されている、請求項1記載のシステム。
【請求項７】
前記物理的文書の画像内の文書セキュリティ特徴の存在または前記物理的文書の画像内の文書セキュリティ特徴の欠如を検出するように、前記セキュリティ特徴識別器層が訓練される、請求項1記載のシステム。
【請求項８】
取引検証のための方法であって、以下の工程:
取引の当事者を識別する物理的文書の少なくとも一部分を表す第1のデータを、第1の企業取引検証システムにより受け取る工程;
該第1のデータの難読化を表す第2のデータを生成する工程であって、
セキュリティ特徴識別器層を含むように訓練されている機械学習モデルへと、該第1のデータを入力として提供することと、
該機械学習モデルのセキュリティ特徴識別器層によって出力されたアクティベーションのセットを取得することであって、該第2のデータが該アクティベーションのセットを含む、取得することと
を含む、生成する工程;
該取引が拒否されるべき取引であるかどうかを、該第1の企業取引検証システムにより、かつ該第2のデータに基づいて判定する工程;
該取引が拒否されるべきであると判定したことに基づき、所定の時間量にわたって該第2のデータを含む1つまたは複数のデータレコードを含むように協調検証システムのデータベースを更新する工程であって、該協調検証システムが、該協調検証システムのメンバーである他の企業における該当事者による1つまたは複数の他の取引についての先制拒否を可能にする、更新する工程
を含む、方法。
【請求項９】
前記協調検証システムによって記憶されたデータを、1つまたは複数の他の企業取引検証システムに提供する工程
をさらに含む、請求項8記載の方法。
【請求項１０】
前記1つまたは複数のデータレコードが、前記協調検証システムのメンバーである前記他の企業の1つまたは複数の他の企業検証システムによってアクセス可能である、請求項8記載の方法。
【請求項１１】
所定の時間量にわたって前記第2のデータを含む1つまたは複数のデータレコードを含むように前記協調検証システムの前記データベースを更新する工程が、
前記第2のデータを悪質行為者リスト内の実体レコードに、前記協調検証システムにより記憶することであって、前記悪質行為者リストの各実体レコードが、少なくとも所定の時間量にわたって取引が拒否されるべき実体に対応する、記憶すること
を含む、請求項8記載の方法。

【請求項１２】
前記協調検証システムの前記データベースを更新した後に、
異なる取引の当事者を識別する前記物理的文書の少なくとも一部分を表す異なるデータを、第2の企業取引検証システムにより受け取る工程;
該異なるデータの難読化を表す第3のデータを生成する工程であって、
セキュリティ特徴識別器層を含むように訓練されている第2の機械学習モデルへと、該異なるデータを入力として提供することと、
該第2の機械学習モデルのセキュリティ特徴識別器層によって出力された異なるアクティベーションのセットを取得することであって、該第3のデータが該異なるアクティベーションのセットを含む、取得することと
を含む、生成する工程;
該第3のデータが、前記協調検証システムの前記データベースに記憶された前記第2のデータに対して所定の類似度レベルの範囲内にあると、該第2の企業取引検証システムにより判定する工程;および
該第3のデータが前記第2のデータに対して所定の類似度レベルの範囲内にあると判定したことに基づき、該異なる取引が拒否されるべきであると判定する工程
をさらに含む、請求項8記載の方法。
【請求項１３】
正規の物理的文書の少なくとも一部分を、入力画像を表すデータが描写している可能性を判定するように、前記機械学習モデルが訓練されている、請求項8記載の方法。
【請求項１４】
前記物理的文書の画像内の文書セキュリティ特徴の存在または前記物理的文書の画像内の文書セキュリティ特徴の欠如を検出するように、前記セキュリティ特徴識別器層が訓練される、請求項8記載の方法。
【請求項１５】
1つまたは複数のコンピュータによって実行可能な命令を含むソフトウェアを記憶している、非一時的コンピュータ可読媒体であって、
該命令が、そのような実行時に、該1つまたは複数のコンピュータに、以下:
取引の当事者を識別する物理的文書の少なくとも一部分を表す第1のデータを、第1の企業取引検証システムにより受け取ること;
該第1のデータの難読化を表す第2のデータを生成することであって、
セキュリティ特徴識別器層を含むように訓練されている機械学習モデルへと、該第1のデータを入力として提供することと、
該機械学習モデルのセキュリティ特徴識別器層によって出力されたアクティベーションのセットを取得することであって、該第2のデータが該アクティベーションのセットを含む、取得することと
を含む、生成すること;
該取引が拒否されるべき取引であるかどうかを、該第1の企業取引検証システムにより、かつ該第2のデータに基づいて判定すること;
該取引が拒否されるべきであると判定したことに基づき、所定の時間量にわたって該第2のデータを含む1つまたは複数のデータレコードを含むように協調検証システムのデータベースを更新することであって、該協調検証システムが、該協調検証システムのメンバーである他の企業における該当事者による1つまたは複数の他の取引についての先制拒否を可能にする、更新すること
を含む動作を行わせる、
非一時的コンピュータ可読媒体。
【請求項１６】
前記動作が、
前記協調検証システムによって記憶されたデータを、1つまたは複数の他の企業取引検証システムに提供すること

をさらに含む、請求項15記載のコンピュータ可読媒体。
【請求項１７】
前記1つまたは複数のデータレコードが、前記協調検証システムのメンバーである前記他の企業の1つまたは複数の他の企業検証システムによってアクセス可能である、請求項15記載のコンピュータ可読媒体。
【請求項１８】
所定の時間量にわたって前記第2のデータを含む1つまたは複数のデータレコードを含むように前記協調検証システムの前記データベースを更新することが、
前記第2のデータを悪質行為者リスト内の実体レコードに、前記協調検証システムにより記憶することであって、前記悪質行為者リストの各実体レコードが、少なくとも所定の時間量にわたって取引が拒否されるべき実体に対応する、記憶すること
を含む、請求項15記載のコンピュータ可読媒体。
【請求項１９】
前記動作が、以下:
前記協調検証システムの前記データベースを更新した後に、
異なる取引の当事者を識別する前記物理的文書の少なくとも一部分を表す異なるデータを、第2の企業取引検証システムにより受け取ること;
該異なるデータの難読化を表す第3のデータを生成することであって、
セキュリティ特徴識別器層を含むように訓練されている第2の機械学習モデルへと、該異なるデータを入力として提供することと、
該第2の機械学習モデルのセキュリティ特徴識別器層によって出力された異なるアクティベーションのセットを取得することであって、該第3のデータが該異なるアクティベーションのセットを含む、取得することと
を含む、生成すること;
該第3のデータが、前記協調検証システムの前記データベースに記憶された前記第2のデータに対して所定の類似度レベルの範囲内にあると、該第2の企業取引検証システムにより判定すること;および
該第3のデータが前記第2のデータに対して所定の類似度レベルの範囲内にあると判定したことに基づき、該異なる取引が拒否されるべきであると判定すること
をさらに含む、請求項15記載のコンピュータ可読媒体。
【請求項２０】
正規の物理的文書の少なくとも一部分を、入力画像を表すデータが描写している可能性を判定するように、前記機械学習モデルが訓練されている、請求項15記載のコンピュータ可読媒体。
【請求項２１】
前記物理的文書の画像内の文書セキュリティ特徴の存在または前記物理的文書の画像内の文書セキュリティ特徴の欠如を検出するように、前記セキュリティ特徴識別器層が訓練される、請求項15記載のコンピュータ可読媒体。
【請求項２２】
取引検証のためのシステムであって、
1つまたは複数のプロセッサと、
該1つまたは複数のプロセッサによって実行されると、該1つまたは複数のプロセッサに、以下:
取引の当事者を識別する物理的文書の少なくとも一部分を表す第1のデータを、第1の企業取引検証システムにより受け取ること;
該第1のデータの難読化を表す第2のデータを生成することであって、
セキュリティ特徴識別器層を含むように訓練されている機械学習モデルへと、該第1のデータを入力として提供することと、
該機械学習モデルのセキュリティ特徴識別器層によって出力されたアクティベーションのセットを取得することであって、該第2のデータが該アクティベーションのセッ

トを含む、取得することと
を含む、生成すること;
第1の所定の時間量にわたって該第1の企業取引検証システムのデータベースに該第2のデータを記憶すること;
該第2のデータを記憶した後に、
該取引が正規の取引ではないと、第1の企業取引検証システムにより判定すること;
該取引が正規の取引ではないと判定したことに基づき、第2の所定の時間量にわたって該第2のデータを含む1つまたは複数のデータレコードを含むように協調検証システムのデータベースを更新することであって、該協調検証システムが、該協調検証システムのメンバーである他の企業における該当事者による1つまたは複数の他の取引についての先制拒否を可能にする、更新すること
を含む動作を行わせる、命令
を含む、1つまたは複数の記憶デバイスと
を含む、システム。
【請求項２３】
取引検証のための方法であって、以下の工程:
取引の当事者を識別する物理的文書の少なくとも一部分を表す第1のデータを、第1の企業取引検証システムにより受け取る工程;
該第1のデータの難読化を表す第2のデータを生成する工程であって、
セキュリティ特徴識別器層を含むように訓練されている機械学習モデルへと、該第1のデータを入力として提供することと、
該機械学習モデルのセキュリティ特徴識別器層によって出力されたアクティベーションのセットを取得することであって、該第2のデータが該アクティベーションのセットを含む、取得することと
を含む、生成する工程;
第1の所定の時間量にわたって該第1の企業取引検証システムのデータベースに該第2のデータを記憶する工程;
該第2のデータを記憶した後に、
該取引が正規の取引ではないと、第1の企業取引検証システムにより判定する工程;
該取引が正規の取引ではないと判定したことに基づき、第2の所定の時間量にわたって該第2のデータを含む1つまたは複数のデータレコードを含むように協調検証システムのデータベースを更新する工程であって、該協調検証システムが、該協調検証システムのメンバーである他の企業における該当事者による1つまたは複数の他の取引についての先制拒否を可能にする、更新する工程
を含む、方法。
【請求項２４】
1つまたは複数のコンピュータによって実行可能な命令を含むソフトウェアを記憶している、非一時的コンピュータ可読媒体であって、
該命令が、そのような実行時に、該1つまたは複数のコンピュータに、以下:
取引の当事者を識別する物理的文書の少なくとも一部分を表す第1のデータを、第1の企業取引検証システムにより受け取ること;
該第1のデータの難読化を表す第2のデータを生成することであって、
セキュリティ特徴識別器層を含むように訓練されている機械学習モデルへと、該第1のデータを入力として提供することと、
該機械学習モデルのセキュリティ特徴識別器層によって出力されたアクティベーションのセットを取得することであって、該第2のデータが該アクティベーションのセットを含む、取得することと
を含む、生成すること;
第1の所定の時間量にわたって該第1の企業取引検証システムのデータベースに該第2のデータを記憶すること;

該第2のデータを記憶した後に、
該取引が正規の取引ではないと、第1の企業取引検証システムにより判定すること;
該取引が正規の取引ではないと判定したことに基づき、第2の所定の時間量にわたって該第2のデータを含む1つまたは複数のデータレコードを含むように協調検証システムのデータベースを更新することであって、該協調検証システムが、該協調検証システムのメンバーである他の企業における該当事者による1つまたは複数の他の取引についての先制拒否を可能にする、更新すること
を含む動作を行わせる、
非一時的コンピュータ可読媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

関連出願の相互参照

本出願は、その全体が参照により本明細書に組み入れられる、2020年6月22日に出願された、「VELOCITY SYSTEM FOR FRAUD AND DATA PROTECTION FOR SENSITIVE DATA」という名称の米国特許出願第63/042,527号の米国特許法第119条（e）による恩典を主張するものである。

【背景技術】

【０００２】

背景

人は様々な理由で偽造文書を作成する可能性がある。そのような偽造文書の検出は、多くの中でも特に、金融サービス機関、小売店、政府機関を含む多くの実体にとって重要な業務である。

【発明の概要】

【０００３】

概要

本開示の1つの革新的な局面によれば、機密データに対する不正防止およびデータ保護のための速度システムが開示される。一局面では、方法は、取引の当事者を識別する物理的文書の少なくとも一部分を表す第1のデータを、第1の企業取引検証システムにより受け取る工程;第1のデータの難読化を表す第2のデータを生成する工程であって、セキュリティ特徴識別器層を含むように訓練されている機械学習モデルへと、第1のデータを入力として提供することと、機械学習モデルのセキュリティ特徴識別器層によって出力されたアクティベーションのセットを取得することであって、第2のデータがアクティベーションのセットを含む、取得することとを含む、生成する工程;取引が拒否されるべき取引であるかどうかを、第1の企業取引検証システムにより、かつ第2のデータに基づいて判定する工程;ならびに取引が拒否されるべきであると判定したことに基づき、所定の時間量にわたって第2のデータを含む1つまたは複数のデータレコードを含むように協調検証システムのデータベースを更新する工程であって、協調検証システムが、協調検証システムのメンバーである他の企業における前記当事者による1つまたは複数の他の取引についての先制拒否を可能にする、更新する工程を含むことができる。

【０００４】

他のバージョンは、コンピュータ可読記憶デバイス上に符号化された命令によって定義された方法の動作を実行するか、または他の態様で実現するための対応するシステム、装置、およびコンピュータプログラムを含む。

【０００５】

上記その他のバージョンは、任意で以下の特徴のうちの1つまたは複数を含んでいてもよい。例えば、いくつかの実装形態では、方法は、協調検証システムによって記憶されたデータを1つまたは複数の他の企業取引検証システムに提供する工程をさらに含むことができる。

【０００６】

いくつかの実装形態では、1つまたは複数のデータレコードは、協調検証システムのメンバーである他の企業の1つまたは複数の他の企業検証システムによってアクセス可能である。

【０００７】

いくつかの実装形態では、所定の時間量にわたって第2のデータを含む1つまたは複数のデータレコードを含むように協調検証システムのデータベースを更新する工程は、第2のデータを悪質行為者リスト内の実体レコードに、協調検証システムにより記憶することを含むことができる。そのような実装形態では、悪質行為者リストの各実体レコードは、少なくとも所定の時間量にわたって取引が拒否されるべき実体に対応し得る。

【０００８】

いくつかの実装形態では、方法は、協調検証システムのデータベースを更新した後に、異なる取引の当事者を識別する物理的文書の少なくとも一部分を表す異なるデータを、第2の企業取引検証システムにより受け取る工程、および異なるデータの難読化を表す第3のデータを生成する工程をさらに含むことができる。そのような実装形態では、第3のデータを生成する工程は、セキュリティ特徴識別器層を含むように訓練されている第2の機械学習モデルへと、異なるデータを入力として提供することと、第2の機械学習モデルのセキュリティ特徴識別器層によって出力された異なるアクティベーションのセットを取得することであって、第3のデータが異なるアクティベーションのセットを含む、取得することとを含むことができる。そのような実装形態では、方法は、第3のデータが、協調検証システムのデータベースに記憶された第2のデータに対して所定の類似度レベルの範囲内にあると、第2の企業取引検証システムにより判定する工程、および第3のデータが第2のデータに対して所定の類似度レベルの範囲内にあると判定したことに基づき、異なる取引が拒否されるべきであると判定する工程をさらに含むことができる。

【０００９】

いくつかの実装形態では、機械学習モデルは、正規の物理的文書の少なくとも一部分を、入力画像を表すデータが描写している可能性を判定するように訓練されている。

【００１０】

いくつかの実装形態では、セキュリティ特徴識別器層は、物理的文書の画像内の文書セキュリティ特徴の存在または物理的文書の画像内の文書セキュリティ特徴の欠如を検出するように訓練される。

【００１１】

本開示の別の革新的な局面によれば、取引検証のための方法が開示される。一局面では、方法は、取引の当事者を識別する物理的文書の少なくとも一部分を表す第1のデータを、第1の企業取引検証システムにより受け取る工程;第1のデータの難読化を表す第2のデータを生成する工程であって、セキュリティ特徴識別器層を含むように訓練されている機械学習モデルへと、第1のデータを入力として提供することと、機械学習モデルのセキュリティ特徴識別器層によって出力されたアクティベーションのセットを取得することであって、第2のデータがアクティベーションのセットを含む、取得することとを含む、生成する工程;第1の所定の時間量にわたって第1の企業取引検証システムのデータベースに第2のデータを記憶する工程;第2のデータを記憶した後に、取引が正規の取引ではないと、第1の企業取引検証システムにより判定する工程;および取引が正規の取引ではないと判定したことに基づき、第2の所定の時間量にわたって第2のデータを含む1つまたは複数のデータレコードを含むように協調検証システムのデータベースを更新する工程であって、協調検証システムが、協調検証システムのメンバーである他の企業における前記当事者による1つまたは複数の他の取引についての先制拒否を可能にする、更新する工程を含むことができる。

【００１２】

他のバージョンは、コンピュータ可読記憶デバイス上に符号化された命令によって定義された方法の動作を実行するか、または他の態様で実現するための対応するシステム、装置、およびコンピュータプログラムを含む。

【００１３】
有利な実装形態は、以下の特徴のうちの1つまたは複数を含むことができる。例えば、ユーザまたは実体は、システムの様々な要素（例えば、データがシステム内に記憶される時間量データ、不正検出のための閾値、悪質行為者リストのための閾値、人間の検討を呼び出すための閾値など）をカスタマイズすることができる。
【００１４】
有利な実装形態は、第1の企業によって内部的にまたは2つ以上の異なる企業間で外部的に共有されるべき、取引または不正検出を含むデータを記憶することをさらに含むことができる。データは、データベースまたは別のデータ記憶システムに記憶することができる。個人を特定できる情報の共有を防止するために、データを難読化することができる。難読化プロセスは、機械学習モデルのセキュリティ特徴識別器層からのアクティベーション出力を使用することを含むことができ、セキュリティ特徴識別器層は、難読化のレベルおよびデータの非可逆性を提供するのを助けることができる。1つまたは複数の取引から生じるアクティベーション出力を比較して、類似度を判定し、不正の検出を知らせることができる。機械学習モデルのセキュリティ特徴識別器層を介して取引データの要素を抽象化することにより、システムは、個人を特定できる情報を公開することなく、個人を特定できる情報を表すデータの比較および共有を可能にすることができる。
【００１５】
添付の図面および以下の説明において本発明の1つまたは複数の態様の詳細を示す。本発明の他の特徴および利点は、それらの説明、図面、および特許請求の範囲を読めば明らかになるであろう。
【図面の簡単な説明】
【００１６】
【図１】協調取引検証システムの一例のコンテキスト図である。
【図２】取引をスクリーニングするために協調取引検証システムを使用して取引を検証するためのプロセスの一例のフローチャートである。
【図３】協調取引検証システムの一例のコンテキスト図である。
【図４】協調取引検証システムを使用して取引を検証するためのプロセスの一例のフローチャートである。
【図５】協調取引検証システムを実装するために使用することができるシステム構成要素のブロック図である。
【００１７】
種々の図面中の同様の符番および名称は、同様の要素を示す。
【発明を実施するための形態】
【００１８】
詳細な説明
本開示は、協調取引検証システムを可能にするための方法、システム、およびコンピュータプログラムを対象とする。協調取引検証システムは、異なる企業間で取引が拒否されるべき実体を各々識別する悪質行為者データレコードの共有を容易にする。悪質行為者データレコードのこの共有は、第2の企業が、第1の企業によって生成された悪質行為者データレコードから利益を得ることを可能にする。そのような情報の共有は、消費者プライバシー保護に関連する理由により、抑止される可能性があり、特定の状況では禁止される可能性さえある。しかしながら、本開示は、異なる企業間で悪質行為者データレコードを共有する一方で関連する規制も満たす、協調取引検証システムを実現することができる。本開示は、企業を横断して悪質行為者を識別する一方で悪質行為者の身元を隠すためにも使用することができる、識別テンプレートと呼ばれる、特殊なタイプの難読化された悪質行為者データレコードを生成することによってこの利益を実現する。
【００１９】
本明細書の目的では、「企業」は、販売、リース、または他の形態の享受のための商品またはサービスを別の実体に提供する任意の実体を含むことができる。商品またはサービ

スという用語は、幅広く考えられることを意図しており、例えば、商品販売、商品レンタル、電気通信サービス、金融商品、金融サービス、または任意の他の形態の商品もしくはサービスを含むがこれらに限定されない任意の商品またはサービスを含むことができる。実体は、人、小企業、企業、官公庁もしくは政府機関、または任意の他の組織を含むことができる。

【００２０】

いくつかの実装形態では、各難読化された識別テンプレートは、機械学習モデルの隠れ層によって出力されたアクティベーションデータを含むことができる。いくつかの実装形態では、機械学習モデルは、正規の物理的文書の少なくとも一部分を、画像を表す入力データが描写している可能性を判定するように訓練されている機械学習モデルを含むことができる。機械学習モデルが物理的文書の少なくとも一部分の画像を表す入力データを処理するときに機械学習モデルの隠れ層によって生成されるアクティベーションデータ自体を使用して、機械学習モデルによって処理された画像データによって描写されている物理的文書にリンクされた人物などの実体を一意に識別することができる。この識別テンプレートはセキュアであり、機械学習モデルによって機械学習モデルの隠れ層にアクティベーションデータを生成させるように処理された物理的文書の画像を復号して明らかにすることはできない。よって、この識別テンプレートは、取引検証アプリケーションなどの企業を横断した顧客情報の共有を含むアプリケーションにおいて重要なセキュリティ上の利点を提供する。

【００２１】

難読化された識別テンプレートは、難読化された身元テンプレートがコンピューティングプラットフォームを横断して共有される場合に物理的文書にリンクされた人物の身元を隠すことができるが、難読化された識別テンプレートは「暗号化データ」ではないことに留意することが重要である。そのような暗号化データは、典型的には、ターゲットデータに暗号化アルゴリズムを適用してターゲットデータの内容を隠すことによって生成される。これが重要なのは、暗号化アルゴリズムを使用して暗号化されたターゲットデータは、暗号解読アルゴリズム、秘密鍵など、またはそれらの何らかの組み合わせのうちの1つまたは複数を使用して解読することができるからである。対照的に、本開示の識別テンプレートは、正規の物理的文書の少なくとも一部分を、画像を表す入力データが描写している可能性を判定するように訓練されている機械学習モデルなどの機械学習モデルの隠れ層によって出力されたアクティベーションデータを使用して生成される。このアクティベーションデータは、例えば、たとえ機械学習モデルを所有していても、機械学習モデルによって機械学習モデルの隠れ層にアクティベーションデータを生成させるように処理された物理的文書の画像を復号して明らかにすることはできない。このことにより、本明細書に記載される難読化された識別テンプレートは、アクティベーションデータを生成するように処理された物理的文書にリンクされた人物の身元を保護しながら、顧客または取引の認証/検証プラットフォームを横断して共有するのに理想的なものになる。

【００２２】

いくつかの実装形態では、正規の物理的文書は、正規の偽造防止アーキテクチャに準拠した文書である。他の実装形態では、正規の文書は、合法であると判定され、特定の法律、規則、または規制によって認められた任意の文書とすることができる。正規の物理的文書は、偽の物理的文書ではない。偽の物理的文書は、正規の偽造防止アーキテクチャに準拠していない文書を含む可能性がある。正規の偽造防止アーキテクチャは、本明細書では「偽造防止アーキテクチャ」と呼ばれる場合もあり、物理的文書の画像内のその集合的な有無が物理的文書の正当性のしるしを提供する2つ以上の偽造防止セキュリティ特徴のグループを含むことができる。本開示の目的では、物理的文書は、運転免許証、パスポート、または物理的身分証明の形態によって識別された人物の顔画像を含む任意の形態の物理的身分証明を含むことができる。偽造防止アーキテクチャの「セキュリティ特徴」は、物理的文書の画像内のその有無を本開示に従って訓練された機械学習モデルによって検出することができる偽造防止アーキテクチャの特徴を指す用語である。

【００２３】
いくつかの実装形態では、本開示の機械学習モードは、セキュリティ特徴識別器層を含むことができる。機械学習モデルのセキュリティ特徴識別器層は、文書のセキュリティ特徴の存在、文書のセキュリティ特徴の欠如、文書の誤ったセキュリティ特徴、または文書の異常なセキュリティ特徴を検出するように訓練されている層である。本開示によれば、セキュリティ特徴は、物理的文書の正当性を示す物理的文書の任意の属性とすることができる。セキュリティ特徴には、自然な背景、人工的な背景、自然照明、人工照明、自然な影、人工的な影の存在、欠如、または配置、ドロップシャドウなどのフラッシュシャドウの欠如、頭部サイズ異常、頭部アスペクト比異常、頭部平行移動異常、異常な色温度、異常な着色、位置合わせおよび構成されたフラッシュ照明、オフアングル照明、焦点面異常、焦点面の二等分、固定焦点レンズの使用、再量子化に関連するイメージング効果、圧縮に関連するイメージング効果、異常な頭部傾斜、異常な頭部姿勢、異常な頭部回転、非正面顔効果、眼鏡、帽子、頭部スカーフ、または他のカバー類などの顔のオクルージョンの存在、異常な頭部形状動力学、眼間距離に対する異常な頭部アスペクト比、前景と背景の間の異常な露出補正、異常な焦点効果、異なるデジタルソースを示す画像スティッチング効果、不適切な生体認証セキュリティ特徴の印刷、不適切なＯＶＤ、ＯＶＩ、ホログラム、顔または文書の他の部分の上の他の二次的なセキュリティ特徴のオーバーレイなどの不適切なセキュリティ特徴の層化、顔の近く、顔の上、または文書の他の部分の上の不適切な触覚セキュリティ特徴配置、不適切な最終顔印刷、不適切なレーザの白黒、不適切なカラーレーザ、不適切な層化インク印刷、不適切な印刷技術、不適切な印刷層順序付け、物理的文書を構築するために使用される不適切な材料、物理的文書の閾値レベルの材料劣化（例えば、傷、切れ目、曲がり、退色、色のにじみなど）、物理的文書のテキスト特徴（例えば、氏名、住所、経歴情報、または別のテキスト）、２Ｄ ＰＤＦ-４１７符号化、他の形態のバーコードまたはＱＲコード、２Ｄ ＰＤＦ-４１７/バーコード/ＱＲコードの配置などを含めることができる。いくつかの実装形態では、セキュリティ特徴は、2つ以上のセキュリティ特徴間の空間的関係などの関係を含み得る。このセキュリティ特徴のリストは網羅的ではなく、本開示の範囲内に入る他のタイプのセキュリティ特徴も存在し得、または作成することができる。

【００２４】
図1は、協調取引検証システムの一例のコンテキスト図である。システム１００は、1つまたは複数のユーザデバイス１１０、３１０、第1の企業取引検証サーバ１２０、第2の企業取引検証システム３２０、協調取引検証サーバ２２０、および1つまたは複数のネットワーク１１２、２１２、３１２を含むことができる。

【００２５】
第1の企業取引検証サーバ１２０は、第1の取引検証システム１００Ａを含むことができる。第1の取引検証システム１００Ａは、抽出モジュール１３０、ベクトル生成モジュール１４０、機械学習モデル１５０、取引検証モジュール１７０、第1のＧＡ（「善良行為者」）リスト１７２、第1のＢＡ（「悪質行為者」）リスト１７４、通知ユニット１８０、および協調取引検証システム（ＣＴＶＳ）更新モジュール１９０を含むことができる。

【００２６】
第1の企業取引検証サーバ１２０は、協調ネットワーク２１２と通信することができる。第1の企業取引検証サーバ１２０の構成要素の各々は、単一のコンピュータ上でホストされることもでき、または1つもしくは複数のネットワークを使用して互いに通信するように構成された複数のコンピュータを横断してホストされることもできる。本明細書の目的では、「モジュール」は、本開示によって「モジュール」に帰せられる機能を実行するように構成されたソフトウェア、ハードウェア、またはそれらの任意の組み合わせを含むことができる。システム１００は、第1の企業取引検証サーバ１２０に関して段階Ａから段階Ｂまで、第2の企業取引検証システム３２０に関して段階Ｃから段階Ｄまでのプロセスとして説明される。

【００２７】

図1の例を参照すると、会社「X」などの組織と関連付けられていると称する個人などの実体が、段階Aで第1の企業ABC Inc.から100個のウィジェットを購入するなどの第1の取引を完了しようとする。この第1の取引を容易にするために、個人は、身分証明の形態として物理的文書102を提示することができる。提示された物理的文書102の画像115を取り込むためにユーザデバイス110のカメラを使用することができる。ユーザデバイス110は、1つまたは複数のネットワーク112を使用して第1の企業取引検証サーバ120と通信することができる。

【００２８】

画像115は、物理的文書102の画像の少なくとも一部分を描写している第1の抽出画像部分115a、および物理的文書102の画像115が取り込まれたときの周囲環境の一部分を描写している第2の部分115bを含むことができる。ユーザデバイス110は、ネットワーク112を使用して第1の企業取引検証サーバ120に画像115を送ることができる。表されたネットワーク（例えば、ネットワーク112、協調ネットワーク212、ネットワーク312など）は、有線ネットワーク、無線ネットワーク、イーサネットネットワーク、LAN、WAN、セルラーネットワーク、インターネット、またはそれらの任意の組み合わせを含むことができる。

【００２９】

図1の例は、スマートフォンの形態のユーザデバイス110が画像115を取り込むために使用されていることを示しているが、本開示はそのように限定されるべきではない。例えば、ユーザデバイス110の代わりに、音声通話機能のないカメラを使用して画像115を取り込むことができる。次いでカメラは、ネットワーク112を使用して第1の企業取引検証サーバ120に画像115を送ることができる。他の実装形態では、音声通話機能のないカメラが、画像115を取り込み、画像115を別のコンピュータに通信することができる。これは、ブルートゥース短波無線ネットワークなどの1つもしくは複数のネットワークを介して、または例えばユニバーサルシリアルバス（USB）タイプCケーブルを使用したコンピュータへの直接接続を介して達成することができる。次いで、そのような実装形態では、ネットワーク112を使用して第1の企業取引検証サーバ120に画像115を送るためにコンピュータを使用することができる。さらに別の実装形態では、カメラを、各々がカメラおよび画像送信デバイスを装備し得る、タブレット、ラップトップ、スマートグラスなどといった別のユーザデバイスの一部とすることができる。一般に、画像を取り込むことができる任意のデバイスを、画像115などの画像を取り込むために使用することができる。

【００３０】

第1の企業取引検証サーバ120は、画像115を受け取り、画像115を入力として抽出モジュール130に提供することができる。抽出モジュール130は、画像115から物理的文書102の第1の抽出画像部分115aを抽出し、画像115の第2の部分115bを廃棄することができる。この機能は、物理的文書102の一部分を描写していない画像115の部分を除去するという目的を果たすことができる。しかしながら、他の実装形態では、抽出モジュール130を、画像115の第1の抽出画像部分115aの一部分のみを抽出するために使用することができる。例えば、抽出モジュール130は、画像115の第1の部分115aから人物の顔のプロファイル画像のみを抽出するように構成することができる。実際、抽出モジュールは、物理的文書102の少なくとも一部分を描写している画像115の第1の抽出画像部分115aの任意の部分を抽出するように構成することができる。

【００３１】

第1の企業取引検証サーバ120は、画像115の抽出画像部分115aをベクトル生成モジュール140に提供することができる。図1の例を参照すると、画像115の抽出部分は、画像115の第1の部分に対応し得る抽出画像部分115aを含む。この例では、画像115の抽出画像部分115aは、画像115の第2の部分115bが除去された後の物理的文書102の画像を含む。ベクトル生成モジュール140は、画像115の抽出画像部分115aを処理し、画像115の抽出画像部分115aを数値的に表すベクトル142を生成することができる。例え

ば、ベクトル142は、画像115の抽出画像部分115aの画素に各々対応する複数のフィールドを含むことができる。ベクトル生成モジュール140は、画像115の抽出画像部分115aの対応する画素を記述するフィールドの各々の数値を決定することができる。フィールドの各々決定された数値は、画像115の抽出画像部分115aによって描写されている物理的文書102の偽造防止アーキテクチャのセキュリティ特徴を、生成されたベクトル142に符号化するために使用することができる。画像115の抽出画像部分115aを数値的に表す生成されたベクトル142は、機械学習モデル150へと入力として提供される。

【００３２】

機械学習モデル150は、1つまたは複数のニューラルネットワークなどの複数の層を介してデータを処理する任意の機械学習モデルを含むことができる。機械学習モデル150は、いくつかの層を含む。これらの層は、入力ベクトル142などの入力データを受け取るために使用される入力層152、入力層152を介して受け取られた入力データまたは先行する隠れ層によって生成されたアクティベーションデータを処理するために使用される1つまたは複数の隠れ層154a、154b、または154c、および最終隠れ層によって生成されたアクティベーションデータに対して作用するように構成されたソフトマックス層などの出力層156を含むことができる。機械学習モデル150の各隠れ層154a、154b、または154cは、1つまたは複数の重みまたは他のパラメータを含むことができる。それぞれの隠れ層154a、154b、または154cの重みまたは他のパラメータは、訓練されたモデルが各訓練データセットに対応する所望のターゲットベクトルを生成するように調整することができる。

【００３３】

各隠れ層154a、154b、または154cの出力は、アクティベーションデータを含むことができる。いくつかの実装形態では、このアクティベーションデータを、隠れ層によって生成された数値を各々表す複数のフィールドを含むアクティベーションベクトルとして表すことができる。それぞれの隠れ層によって出力されたアクティベーションベクトルは、モデルの後続の層を介して伝播させ、出力層によって出力データ157を生成するために使用することができる。いくつかの実装形態では、出力層156は、ニューラルネットワーク出力データ157を生成するために、最終隠れ層154cから受け取られたアクティベーションベクトルに対して追加の計算を行うことができる。

【００３４】

図1の例は3つの隠れ層154a、154b、154cのみを示しているが、本開示はそのように限定されない。1つまたは複数の隠れ層は、機械学習モデル150内の隠れ層の完全な配列を構成し得る。よって、隠れ層の数は、図1に示される3つの隠れ層よりも少なくてもよく、これと等しくてもよく、これより多くてもよい。

【００３５】

機械学習モデル150は、隠れ層154a、154b、または154cのうちの1つまたは複数をセキュリティ特徴識別器層として機能するよう構成するように訓練することができる。セキュリティ特徴識別器層は、セキュリティ特徴識別器を含むように訓練されているニューラルネットワークの1つまたは複数の隠れ層を含むことができる。各セキュリティ特徴識別器を、偽造防止アーキテクチャの特定のセキュリティ特徴の有無を検出するように構成することができる。偽造防止アーキテクチャの特定のセキュリティ特徴の有無を検出することは、単一のセキュリティ特徴の有無を検出することを含むことができる。いくつかの実装形態では、特定のセキュリティ特徴の有無を検出することは、複数の異なるセキュリティ特徴間の空間的関係などの関係を検出することを含むことができる。よって、セキュリティ特徴識別器層のセキュリティ特徴識別器は、セキュリティ特徴として、1つまたは複数のセキュリティ特徴のグループが物理的文書の特定の位置内に個別にまたは1つもしくは複数の他のセキュリティ特徴を参照して配置されているか否かを検出するように訓練することができる。1つまたは複数の隠れ層154a、154b、または154cは、自己符号化プロセスを使用してセキュリティ特徴識別器層を含むように訓練することができる。

【００３６】

自己符号化は、ディープニューラルネットワーク出力層が、ディープニューラルネットワークによって処理されたラベル付き入力データを、入力データのラベルによって指定された特定のクラスに正確に分類するニューラルネットワーク出力データを駆動し始めるまで、ディープニューラルネットワーク層の重みまたは他のパラメータを調整するためのフィードバックループを使用する1つまたは複数のディープニューラルネットワーク層を生成するための訓練プロセスである。いくつかの実装形態では、出力データは類似度スコアを含むことができる。出力類似度スコアは次いで、入力データのクラスを決定するために出力類似度スコアに1つまたは複数の閾値を適用することなどによって評価することができる。図1を参照すると、抽出画像部分115aを表すベクトル142は、機械学習モデル150の入力層152に入力され、機械学習モデル150の各層を介して処理され、出力データ157がベクトル142の機械学習モデル150の処理に基づいて生成される。

【００３７】

セキュリティ特徴識別器層としての1つまたは複数の隠れ層154a、154b、154cの自己符号化は、訓練データベースから物理的文書の少なくとも一部分を描写している訓練画像を取得することを複数反復実行し、機械学習モデル150の訓練に使用するための訓練画像の一部分を抽出し（訓練画像の関連部分がまだ抽出されていない場合）、訓練画像の抽出部分に基づいて入力ベクトルを生成し、機械学習モデル150を使用して、生成された入力ベクトルを処理し、機械学習モデル150によって生成された出力と、機械学習モデル150によって処理された入力データベクトルで表された訓練画像に対応する訓練画像のラベルとの関数である損失関数を実行することによって達成することができる。システム100は、誤差逆伝播などによる確率的勾配降下法などの技術を使用して損失関数を最小化する目的で、各反復における損失関数の出力に基づいて機械学習モデル150のパラメータの値を調整することができる。損失関数の出力に基づく機械学習モデル150のパラメータの値の反復調整は、出力データが、所定の誤差量内で、出力データを生成するために機械学習モデル150によって処理された入力データベクトルに対応する画像の訓練ラベルと一致し始めるまで、隠れ層154a、154b、154cのうちの1つまたは複数の重みまたは他のパラメータの値を調整するフィードバックループである。

【００３８】

図1に示される例では、アクティベーションデータ160は隠れ層154bの出力として示されている。アクティベーションデータ160は、隠れ層154bが受け取った入力データを処理したことに基づいて隠れ層154bによって生成された出力アクティベーションデータである。本開示において、隠れ層154bは、文書の文書セキュリティ特徴の存在または文書セキュリティ特徴の欠如を検出するように訓練されたセキュリティ特徴識別器層である。区別のポイントとして、アクティベーションデータ160は、隠れ層154b（例えば、セキュリティ特徴識別器層）から取得され、隠れ層154b（例えば、セキュリティ特徴識別器層）によって生成され、隠れ層154b（例えば、セキュリティ特徴識別器層）によって出力される。アクティベーション160は、機械学習モデル150の出力層156の出力157ではない。

【００３９】

セキュリティ特徴識別器層は、抽出画像部分115aの表現を受け取って処理することができる。いくつかの実装形態では、セキュリティ特徴識別器層が受け取って処理する抽出画像部分115aの表現は、直接または入力層152などの先行層の出力としてセキュリティ特徴識別器層に提供することができる入力ベクトル142を含むことができる。いくつかの実装形態では、セキュリティ特徴識別器層によって受け取られ処理される抽出画像部分115aの表現は、隠れ層154aなどの別の隠れ層の出力を含むことができる。その正確な起源、形態、またはフォーマットにかかわらず、セキュリティ特徴識別器層によって受け取られ処理される入力データは、抽出画像部分115aを表す。

【００４０】

セキュリティ特徴識別器層が抽出画像部分115aを表す入力データを処理したことに基づいてセキュリティ特徴識別器層（例えば、隠れ層154b）によって生成される出力デー

タは、アクティベーションデータ160である。セキュリティ特徴識別器層（例えば、隠れ層154b）によるアクティベーションデータ160の生成は、セキュリティ特徴識別器層（例えば、隠れ層154b）により、セキュリティ特徴識別層によって処理された入力データに対応する物理的文書の画像（例えば、抽出画像部分115a）に描写されている偽造防止アーキテクチャのセキュリティ特徴の有無を表すデータを符号化することを含む。

【００４１】

アクティベーションデータ160は、その少なくとも一部分が画像115の抽出画像部分115aによって描写されており、入力ベクトル142によって表されている物理的文書102のための難読化された識別テンプレートとして使用することができる。いくつかの実装形態では、アクティベーションデータ160は、特定の隠れ層（例えば、セキュリティ特徴識別器層）によって生成されたデータを含むことができる。隠れ層によって生成されたこのデータは、特定の隠れ層が抽出画像部分115aを表す入力データを処理したことに基づいて、特定の隠れ層（例えば、セキュリティ特徴識別器層）のニューロンなどの処理要素によって生成されたパラメータのセットを表すことができる。例として、パラメータのセットは、隠れ層の1つまたは複数のニューロンの出力、そのような出力に関連する重みなど、またはそれらの任意の組み合わせを含むことができる。一実装形態では、例えば、アクティベーションデータ160は、入力ベクトル142によって表されている特定の画像データの抽出されたバイナリ表現、抽出されたバイナリに関連する隠れ層（例えば、セキュリティ特徴識別器層）のそれぞれのニューロンによって生成された重みもしくは値、またはそれらの組み合わせとすることができる。そのような実装形態では、バイナリ値は、抽出画像部分115aを表す処理データに基づいてセキュリティ特徴識別器層の特定の実装形態によって認識される抽出画像部分115asの特定の特徴に対応することができ、セキュリティ特徴識別器層によって処理される抽出画像部分115aを表すデータに特定のセキュリティ特徴が存在するか否かなどの情報を含むことができる。

【００４２】

セキュリティ特徴識別器層（例えば、隠れ層154a、154b、または154c）によって出力されたアクティベーションデータ160は、セキュリティ特徴識別器層が訓練された特定の偽造防止アーキテクチャの1つまたは複数のセキュリティ特徴の各々が、セキュリティ特徴識別器層によって処理された抽出画像部分115aを表す入力データに存在するか否かを示すデータで符号化されている。セキュリティ特徴識別器層による、特定の偽造防止アーキテクチャのセキュリティ特徴の有無の、アクティベーションデータ160への符号化により、抽出画像部分115aに対応する物理的身分証明書を表す難読化された識別テンプレートが作成される。

【００４３】

難読化された識別テンプレートは、特定の物理的身分証明書（例えば、物理的文書102）を一意に識別することができ、物理的文書のセキュリティ特徴のわずかな差異でさえも、アクティベーションデータの異なる符号化をもたらす。例えば、訓練されたセキュリティ特徴識別器層は、物理的文書の画像内のプロファイル画像の異なる頭部位置、物理的文書の画像内の異なる照明条件、物理的文書の画像内のセキュリティ特徴の異なる空間的関係、物理的文書の画像内のテキスト/グラフィック/画像の異なるインク特性、物理的文書の第1の画像内のバーコードの存在および物理的文書の第2の画像内のバーコードの欠如などといった捉え難い区別に基づいて、物理的文書のそれぞれの画像について異なるアクティベーションデータを生成することができる。これらの例がここに提示されているが、これらは限定することを意図するものではない。むしろ、これらの例は、異なる物理的文書の画像内のセキュリティ特徴の存在、欠如、配置（例えば、1つもしくは複数のセキュリティ特徴の空間的配置）または品質（例えば、インク品質、印刷品質、材料品質など）の任意の区別を、セキュリティ特徴識別器層によって検出し、これによりセキュリティ特徴識別器層に、異なるアクティベーションデータ160のセットを出力として生成させることができ、よって、アクティベーションデータ160が特定の物理的文書に対応する難読化された識別テンプレートとして使用されることが可能になるポイントを例示する

ために提供されている。

【００４４】

いくつかの実装形態では、アクティベーションデータ160を、教師なし学習技術を使用して生成することができる。例えば、教師なし学習の使用により、隠れ層154bによって生成されるアクティベーションデータ160などの生成されるアクティベーションデータの重み付けおよび構成は、画像115の抽出画像部分115aを表す入力ベクトル142が機械学習モデル150によって以降処理されるたびに、隠れ層154bによって生成されたアクティベーションデータの別のセットの所定の誤差範囲内になる。よって、追加の訓練、再訓練、またはそれらの組み合わせなしで、機械学習モデル150の隠れセキュリティ特徴識別器層154bは、物理的文書102の識別テンプレートとして使用することができるアクティベーションデータを確実に生成することができる。しかしながら、本開示は、物理的文書102全体の画像を処理することに限定される必要はない。代わりに、いくつかの実装形態では、アクティベーションデータ160は、物理的文書102の一部分のみの画像を表す処理データに基づいて難読化された識別要素を作成するために使用することができる。

【００４５】

アクティベーションデータ160は、取引の当事者によって提示された特定の物理的文書を一意に識別することができる。アクティベーションデータの固有の識別特性は、画像115の抽出画像部分115aに描写されているような物理的文書102のセキュリティ特徴の符号化の結果として生じる。いくつかの実装形態では、隠れ層154bは、例えば、本明細書に記載される自己符号化プロセスを使用して、画像115の抽出画像部分115aによって描写されているような物理的文書102のセキュリティ特徴のうちのセキュリティ特徴の有無を検出するように訓練されている。その結果、隠しセキュリティ特徴識別器層154bによって生成された、この例でアクティベーションデータ160として示されているアクティベーションデータ160は、画像115の抽出画像部分115aによって描写されている物理的文書102のセキュリティ特徴の存在、欠如、配置、または品質を表すデータの符号化を表すことになる。

【００４６】

いくつかの実装形態では、符号化データは、セキュリティ特徴が存在するが低品質のものであることを示すことができる。あるいは、いくつかの実装形態では、低品質のセキュリティ特徴（例えば、プロファイル画像の不十分な照明）の検出は、セキュリティ特徴（例えば、適切な照明条件）の欠如としてアクティベーションデータに符号化され得る。同様に、プロファイル画像内の適切な照明条件の検出は、セキュリティ特徴（例えば、適切な照明条件）の存在としてアクティベーションデータに符号化され得る。同様に、そのような実装形態では、符号化データは、1つまたは複数のセキュリティ特徴が適切な方法で空間的に配置されなかったことを示すこともできる。あるいは、いくつかの実装形態では、1つまたは複数のセキュリティ特徴の不適切な空間的配置の検出は、セキュリティ特徴の欠如（例えば、2D PDF-417が期待される場所に存在しない）としてアクティベーションデータに符号化され得る。同様に、1つまたは複数のセキュリティ特徴の適切な空間的位置を、セキュリティ特徴の存在（例えば、2D PDF-417が期待される場所に存在する）としてアクティベーションデータに符号化することもできる。

【００４７】

アクティベーションデータ160は、取引検証モジュール170へと入力として提供することができる。取引検証モジュール170は、物理的文書102を提示した実体によって要求された取引が許可されるべきか拒否されるべきかを判定することができる。取引検証モジュール170は、生成された入力ベクトル142の機械学習モデル150による処理に基づいて機械学習モデル150の隠れ層154bによって生成されたアクティベーションデータ160が、善良行為者リスト172に記憶されている、悪質行為者リスト174に記憶されている、または善良行為者リスト172にも悪質行為者リスト174にも記憶されていない対応するベクトルと一致するかどうかを判定することによってこの判定を行うことができる。

【００４８】
善良行為者リスト１７２は、取引が認められるべきである１人または複数人の当事者を記述するデータを含むデータベース、データ構造、または他のデータ編成を含むことができる。当事者は、何回かの期限内の支払いまたは他の正規の取引活動を達成するなどのいくつかの理由で、善良行為者リストに追加され得る。善良行為者リスト１７２は、特定の実装形態に応じて、ローカルな取引ネットワーク内の所与の企業によって排他的に使用されてもよく、またはより広く他の企業に提供されてもよい。いくつかの実装形態では、取引が認められるべき当事者を記述するデータは、機械学習モデル１５０の隠れ層１５４bまたは機械学習モデル１５０と同様に訓練されている別の機械学習モデルの隠れ層によって事前に生成されたアクティベーションデータを含むことができる。このアクティベーションデータは、図１に示されるアクティベーションデータ１６０と同様のこれらの機械学習モデルのうちの１つの隠れ層の出力とすることができる。
【００４９】
善良行為者リスト１７２に記憶されたこの記憶されたアクティベーションデータは、取引が事前検証されている実体と関連付けられた物理的文書の身元テンプレートとして機能することができる。いくつかの実装形態では、取引が認められるべきである１人または複数人の当事者を記述するデータは、９０日間などの所定の時間量にわたってのみ善良行為者リストに記憶され得る。そのような実装形態では、取引検証モジュール１７０または善良行為者リスト維持モジュールなどの他のモジュールを使用して、善良行為者リスト１７２に記憶された識別テンプレートの作成日と関連付けられたタイムスタンプを監視し、そのそれぞれのタイムスタンプが、身元テンプレートが善良行為者リスト１７２に記憶されることを認められている所定の時間量を満たしているかまたは超えている作成日を示す、各識別テンプレートを、削除することができる。
【００５０】
悪質行為者リスト１７３は、取引が拒否されるべきである１人または複数人の当事者を記述するデータを含むデータベース、データ構造、または他のデータ編成を含むことができる。当事者は、所与の取引、取引のセット、または所定の時間量についての特定の閾値を超えるリスク要因と関連付けられているなど、いくつかの理由で悪質行為者リストに追加され得る。例として、多額のローンを求める要求、貸し出された金銭または資産の返済不能、購入と関連付けられた商品の受け取りおよび保管後の、該購入のためのクレジットカード取引の取り消しなどの指標が挙げられる。悪質行為者リスト１７４は、実装形態に応じて、ローカルな取引ネットワーク内の所与の組織によって排他的に使用されてもよく、またはより広く他の状況、ユーザ、もしくは企業に提供されてもよい。いくつかの実装形態では、取引が拒否されるべき当事者を記述するデータは、機械学習モデル１５０の隠れ層１５４bまたは機械学習モデル１５０と同様に訓練されている別の機械学習モデルの隠れ層によって事前に生成されたアクティベーションデータを含むことができる。このアクティベーションデータは、図１に示されるアクティベーションデータ１６０と同様のこれらの機械学習モデルのうちの１つの隠れ層の出力とすることができる。
【００５１】
悪質行為者リスト１７４上のこの記憶されたアクティベーションデータは、取引拒否の事前フラグがたてられている実体と関連付けられた物理的文書の身元テンプレートとして機能することができる。いくつかの実装形態では、取引が拒否されるべきである１人または複数人の当事者を記述するデータは、９０日間などの所定の時間量にわたってのみ悪質行為者リストに記憶され得る。そのような実装形態では、取引検証モジュール１７０または悪質行為者リスト維持モジュールなどの他のモジュールを使用して、悪質行為者リスト１７４に記憶された識別テンプレートの作成日と関連付けられたタイムスタンプを監視し、そのそれぞれのタイムスタンプが、身元テンプレートが悪質行為者リスト１７４に記憶されることを認められている所定の時間量を満たしているかまたは超えている作成日を示す、悪質行為者リスト内の各識別テンプレートを、削除することができる。
【００５２】

実体の物理的身分証明書の画像、または実体を個人的に識別するために使用できる難読化されていないデータを含む他のデータの代わりに、善良行為者リスト172または悪質行為者リスト174に記憶された識別テンプレートを使用することにより、大きなセキュリティ上およびプライバシー上の利益が提供され、実際、このシステムを使用して実体識別情報をセキュアな方法でプライベートに記憶および共有することが可能になる。暗号化アルゴリズムでさえも本開示のセキュリティおよびプライバシーのレベルを達成することはできず、というのは、暗号化データは解読されることが少なくともあり得るからである。

【００５３】

取引検証モジュール170は、アクティベーションデータ160が取引検証モジュール170によって受け取られたことに応答して、善良行為者リスト172、悪質行為者リスト174、またはその両方の組み合わせを検索することによって取引検証を実行することができる。例えば、取引検証モジュール170は、受け取られたアクティベーションデータ160を検索パラメータとして使用して善良行為者リスト172の検索を実行することができる。ある事例では、取引検証モジュール170は、アクティベーションデータ160が、特定の誤差閾値内で、善良行為者リスト内の所与の識別テンプレートと一致すると判定することができる。そのような事例では、取引検証モジュール170は、入力ベクトル142によって表されている物理的文書102を取引検証プロセスの一部として提供した実体が認証されており、当事者の取引が承認されるべきであると判定することができる。あるいは、他の事例では、取引検証モジュール170が、アクティベーションデータ160が、特定の誤差閾値内で、善良行為者リスト172内のどの識別テンプレートとも一致しないと判定した場合には、取引検証モジュール170は、取引検証プロセスを継続して悪質行為者リスト174の検索を実行することができる。

【００５４】

善良行為者リスト172が検索された後で、取引検証モジュール170は悪質行為者リスト174の検索を実行することができる。ある事例では、例えば、第1の取引の取引検証に関して図1の例に描写されているように、取引検証モジュール170は、アクティベーションデータ160が、特定の誤差閾値内で、悪質行為者リスト174内の所与の識別テンプレートと一致すると判定することができる。そのような事例では、会社「X」の代理人と称する者による100個のウィジェットに対する第1の取引の取引検証に関して図1の例に描写されているように、取引検証モジュール170は、入力ベクトル142によって表されている物理的文書102を第1の取引の取引検証プロセスの一部として提供した実体が、取引を完了することを認められていないと判定することができる。そのような実装形態では、取引検証モジュール170は、会社「X」の代理人による100個のウィジェットに対する取引が拒否されるべきであることを示す通知182を生成するよう通知ユニット180に命令することができる。そのような事例では、第1の企業取引検証サーバ120は、要求元ユーザデバイス110に、状態Bでユーザデバイス110のディスプレイに表示するための通知182を送ることができる。これは図1の例で発生し、通知182は、ユーザデバイス110によって処理された場合にユーザデバイス110に、第1の取引が拒否されることを示すデータを出力させることができる。この出力データは、取引が拒否されることを示す「取引は拒否された」などのオーディオメッセージ、第1の取引が拒否されることを示すテキスト、グラフィック、もしくは両方を表示する視覚メッセージ、第1の取引が拒否されることを示す、ユーザデバイス110を振動させるなどの触覚フィードバック、またはそれらの任意の組み合わせを含むことができる。

【００５５】

上述した図1の例は、段階Aでユーザによって提示された物理的文書102の少なくとも一部分の画像に対応するアクティベーションデータまたは識別テンプレートが、所定の類似度の範囲内で、悪質行為者リスト上の識別と一致したために、第1の取引が拒否されたシナリオを説明しているが、本開示はそのように限定されない。むしろ、悪質行為者リストに関連しない幾つもの理由で第1の取引を拒否することもできる。例えば、段階Aでユ

ーザによって提示された支払い方法が、拒否された可能性もある。

【００５６】

あるいは、他の事例では、取引検証モジュール１７０は、アクティベーションデータ１６０が悪質行為者リスト１７４内のいかなる識別テンプレートとも一致しないと判定することができる。このシナリオでは、取引検証モジュール１７０は、アクティベーションデータ１６０が、特定の誤差閾値内で、善良行為者リストまたは悪質行為者リスト内のいかなる識別テンプレートとも一致しないと判定している。そのようなシナリオでは、取引検証モジュール１７０は、入力ベクトル１４２によって表されている物理的文書１０２を取引検証プロセスの一部として提供した実体が、要求された取引を完了することを認められていると判定することができる。そのような実装形態では、取引検証モジュール１７０は、通知ユニット１８０に、取引が認められており、許可されるべきであることを示す通知１８２を生成するよう命令することができる。そのような事例では、第１の企業取引検証サーバ１２０は、取引が許可されるべきであることを示す状態Ｂでユーザデバイスのディスプレイに表示するための通知を、要求元ユーザデバイス１１０に送ることができる。

【００５７】

図１の例では、画像１１５を取り込み、かつ画像１１５を第１の取引の取引検証の一部として第１の企業取引検証サーバ１２０に送る同じユーザデバイスが、通知１８２も受け取る。しかしながら、本開示はそのように限定される必要はない。代わりに、いくつかの実装形態では、第１の企業検証サーバ１２０は通知１８２を別のコンピュータに送ることができる。そのような事例では、別のコンピュータのユーザは、ある事例では通知１８２によって表され得る取引検証プロセスの決定を、取引検証中に物理的文書１０２を提示したユーザに伝達することができる。

【００５８】

段階Ａでユーザによって試みられた第１の取引の取引検証中に、善良行為者リスト１７２、悪質行為者リスト１７４、またはその両方を考慮してアクティベーションデータ１６０を分析した後、取引検証モジュール１７０は、取引が認められているか否かに関して取引検証モジュール１７０によって行われた判定に基づいて、協調検証システム（ＣＴＶＳ）更新モジュール１９０にデータを提供することができる。図１の例では、第１の取引は認められていなかったので、取引検証モジュール１７０は、ＣＴＶＳ更新モジュール１９０に、入力ベクトル１４２によって表されている物理的文書１０２を第１の取引の取引検証プロセスの一部として提供した第１の取引の実体が、第１の取引を完了することを認められていないことを示すデータを提供することができる。取引検証モジュール１７０は、ＣＴＶＳ更新モジュール１９０に、第１の取引データ、取引検証モジュール１７０の決定を示すデータ、またはその両方の組み合わせを構造化した１つまたは複数のフィールドを含む第１のデータ構造１９２を生成するよう命令することができる。

【００５９】

第１の取引データは、物理的文書１０２の画像１１５の抽出画像部分１１５ａに基づいて生成されたアクティベーションデータ１６０を含むことができる。いくつかの実装形態では、この第１の取引データはまた、取引の時刻、取引の日付、取引の場所、段階Ａで実体によって購入もしくはリースのために求められた商品もしくはサービスのタイプ（例えば、ウィジェット）、段階Ａで実体によって購入もしくはリースのために求められた商品もしくはサービスの数（例えば、１００個のウィジェット）、段階Ａで取引実体が関連付けられている組織（例えば、会社「Ｘ」）、または第１の取引に関連する任意の他の取引メタデータなどの、状態Ａで試みられた取引に関連する取引メタデータも含むことができる。第１の企業取引検証サーバ１２０は、協調ネットワーク２１２を使用して協調検証システム２２０に第１のデータ構造１９２を送ることができる。協調ネットワーク２１２は、有線ネットワーク、無線ネットワーク、またはそれらの任意の組み合わせを含む任意のタイプの通信ネットワークを含むことができる。同様に、協調ネットワーク２１２は、光ネットワーク、イーサネットネットワーク、ＷｉＦｉネットワーク、セルラーネットワーク、ブルートゥースネットワーク、インターネット、またはそれらの任意の組み合わせのうちの１つまたは複

数を含む。よって第1のデータ構造192は、第1の取引と関連付けられた悪質行為者を記述するデータを表す。

【００６０】

第1のデータ構造192は、協調検証システム220によって受け取りかつ処理することができる。例えば、協調検証システム220を、BA（「悪質行為者」）リスト更新モジュール230に入力することができる。悪質行為者リスト更新モジュール230は、第1のデータ構造192を受け取り、第1のデータ構造に含まれる情報に基づいて協調的BA（「悪質行為者」）リスト240を更新する。いくつかの実装形態では、これは、第1の企業取引検証サーバ120によって生成された、識別テンプレートと呼ばれ得るアクティベーションデータ160を、協調的悪質行為者リスト240に記憶することを含み得る。

【００６１】

他の実装形態では、悪質行為者リスト更新モジュール230は、取引メタデータを記憶されたアクティベーションデータ160と関連付けて記憶するように協調的悪質行為者リスト230を更新することができる。すなわち、悪質行為者リスト更新モジュール230は、対応するアクティベーションデータ160のセットによってインデックス付けされた、段階Aで試みられた取引などの拒否された取引と関連付けられたメタデータを含む取引レコードを生成することができる。取引の時刻、取引の日付、取引の場所、段階Aで実体によって購入もしくはリースのために求められた商品もしくはサービスのタイプ（例えば、ウィジェット）、段階Aで実体によって購入もしくはリースのために求められた商品もしくはサービスの数（例えば、100個のウィジェット）、段階Aで取引実体が関連付けられている組織（例えば、会社「X」）、または第1の取引に関連する任意の他の取引メタデータなどの、取引と関連付けられた、取引メタデータ。そのような取引メタデータを、段階Aの取引の当事者であった実体による後続の将来の不正取引を検出するために、協調検証システム220または第2の企業取引検証システム320などの他の企業取引検証システムによってマイニングすることができる。いくつかの実装形態では、アクティベーションデータ160と取引メタデータの両方を協調的悪質行為者リスト240に記憶することができる。

【００６２】

さらに別の実装形態では、悪質行為者リスト更新モジュール230は、協調的悪質行為者リスト240を更新する前に、第1の企業取引検証サーバ120によって拒否された第1の取引の取引価値を決定することができる。そのような事例では、悪質行為者リスト240は、悪質行為者更新モジュール230が、拒否された第1の取引の取引価値が所定の閾値を満たすと判定した場合にのみ、協調的悪質行為者リスト240を更新し得る。いくつかの実装形態では、取引価値は、取引のドル価値であり得る。この例では、取引価値は、例えば、購入されたウィジェットの個数にウィジェットのコストを掛けることによって決定することができる。他の実装形態では、取引価値を他の方法で決定することができ、事業に対する取引の影響を表す値などの重み値や異なる値を有し得る。特定のドル価値を有する取引は、事業のサイズ、事業のビジネスモデルなどに基づいてより大きい影響を有し得るか、またはより小さい影響を有し得るので、そのような影響値は特に有利であり得る。あるいは、取引価値が所定の閾値を満たさないと判定された場合には、悪質行為者更新モジュール230は、協調的悪質行為者リスト240を更新しないと決定してもよい。

【００６３】

異なる企業取引検証システム間での悪質行為者の情報共有を可能にする本開示の利点は、アクティベーションデータ160を、ユーザ識別可能情報の代わりに、悪質行為者リストに記憶することによって、またはアクティベーションデータを使用して、アクティベーションデータ160に対応する悪質行為者によって試みられた取引に関連する取引メタデータにインデックス付けすることによって、またはその両方の組み合わせによって達成される。協調検証システム220において悪質行為者を表すためにアクティベーション160を使用することにより、悪質行為者の身元が不可逆的な方法で完全に難読化され、悪質行為者の身元が協調的悪質行為者リスト240によって共有および記憶されることが可能に

なる。

【００６４】

他の企業取引検証システムによって識別された後続の不正取引を使用して、協調的悪質行為者リスト内のアクティベーションデータ160のセットと関連付けられ、アクティベーションデータ160のセットによってインデックス付けされた取引メタデータレコードを更新することができる。例えば、悪質行為者リスト更新モジュール230によってアクティベーションデータ160および取引メタデータを有する第1のデータ構造192が受け取られると、悪質行為者リスト更新モジュール230は、まず、検索を実行して、以前に受け取られ、協調的悪質行為者リスト240によって記憶された、アクティベーションデータ160のセットに対する所定の類似度閾値内に入る以前のアクティベーションデータのセットなどの別の識別テンプレートが存在するかどうかを判定することができる。存在する場合、悪質行為者リスト更新モジュール230は、所定の類似度レベルでアクティベーションデータ160と一致する以前に記憶されたアクティベーションデータに関連付けて取引メタデータを記憶するよう、協調的悪質行為者リスト240を更新することができる。

【００６５】

あるいは、第1のデータ構造192の新しく受け取られたアクティベーションデータ160に対応する識別テンプレートが協調的悪質行為者リスト240にまだ存在しない場合には、悪質行為者リスト更新モジュール230は、取引メタデータあり（またはなし）で協調的悪質行為者リスト240に新しいエントリを作成することができる。このようにして、複数の企業にまたがって悪質行為者によって試みられた以前の取引を集約することができる。次いで、後で、例えば、悪質行為者が異なる企業で別の不正行為を働こうと試みるときに、異なる企業は、協調検証システム220を参照することができ、協調検証システムは、BA（「悪質行為者」）リスト検索モジュール260を使用して、関連する識別テンプレートを求めて協調的悪質行為者リスト240を検索する、悪質行為者によって現在求められている不正取引と同様の取引を記述する取引メタデータを求めて協調的悪質行為者リスト240をマイニングする、それらの組み合わせなどを行うことができる。

【００６６】

協調的悪質行為者リスト240を維持するために、取引識別（ID）ライフサイクルマネージャ250を使用することができる。取引IDライフサイクルマネージャ250は、協調的悪質行為者リスト240内のレコードと関連付けて記憶されているタイムスタンプなどの記憶された時間記憶データの持続時間を監視することができる。例えば、いくつかの実装形態では、協調的悪質行為者リスト240に記憶された識別テンプレート、協調的悪質行為者リスト240内の識別テンプレートによってインデックス付けされた取引メタデータ、またはその両方などの拒否された取引に関連するデータは、所定の時間量にわたってのみ協調的悪質行為者リスト240によって記憶されたままであることが許可され得る。そのような実装形態では、取引IDライフサイクルマネージャモジュール250または悪質行為者リスト維持モジュールなどの他のモジュールを使用して、協調的悪質行為者リスト240に記憶された識別テンプレート、協調的悪質行為者リスト240に記憶された取引メタデータ、またはその両方の作成日と関連付けられたタイムスタンプを監視し、それぞれのタイムスタンプが、識別テンプレートが協調的悪質行為者リスト240によって記憶されることが認められている所定の時間量を満たしているかまたは超えている作成日を示す、悪質行為者リスト内の各識別テンプレートまたは他のデータを、削除することができる。

【００６７】

識別テンプレート、取引メタデータ、またはその両方などの協調的悪質行為者リスト240によって記憶されたデータのデータ管理を規定するライフサイクルルールは、記憶された協調検証システム全体にわたって均一とすることができる。例えば、いくつかの実装形態では、協調的悪質行為者リスト240内のデータは、90日間の均一なライフサイクルを有することができる。いくつかの実装形態では、この均一な期間は、経済的規制、消費者保護、州法、連邦法、またはそれらの組み合わせに基づくものであり得る。他の実装形態では、協調的悪質行為者リスト240によって記憶されたデータの管理を規定するルー

ルを不均一とすることができる。例えば、第1の組の識別テンプレート、取引メタデータ、またはそれらの組み合わせは、第1の期間にわたって協調的悪質行為者リスト240に記憶することができ、第2の組の識別テンプレート、取引メタデータ、またはそれらの組み合わせは、第2の期間にわたって協調的悪質行為者リストに記憶することができ、第2の期間は第1の期間と異なる。

【００６８】

いくつかの実装形態では、これらの不均一の期間は、それぞれのデータセットと関連付けられたカスタムライフサイクルルールを使用して確立することができる。いくつかの実装形態では、それぞれのデータセットのカスタムライフサイクルルールを、協調検証システム220にデータを提供した企業によって決定し、割り当てることができる。例えば、第1の企業は、協調的悪質行為者リスト240が、悪質行為者の識別テンプレート、取引メタデータ、またはその両方を30日間にわたって記憶すると規定し得るが、第2の企業は、協調的悪質行為者リスト240が、悪質行為者の識別テンプレート、取引メタデータ、またはその両方を、90日間などの法律によって許可された法的制限までにわたって記憶すると規定し得る。他の実装形態では、不均一の期間は、データ自体の属性に基づいて設定することができ、データによって提供される企業から潜在的に独立していることが可能である。例えば、識別テンプレート、取引メタデータ、またはその両方が、識別テンプレート、取引メタデータ、またはその両方を分類またはルール判定するために使用することができる追加のデータと共に送られてもよい。

【００６９】

協調的悪質行為者リスト240が、悪質行為者の識別テンプレートとしてアクティベーションデータ160を含むように更新された後、段階Bにおける第1の取引が拒否された実体は、段階Cで別の取引の当事者になろうと試みる。例えば、第1の企業からの100個のウィジェットの購入を拒否された後、会社「X」と関連付けられているとされる悪質行為を行う実体は、次に、第2の企業から100個のウィジェットを購入しようと試みる可能性がある。図1の例では、実体の第1の取引は、第1の企業取引サーバ120の悪質行為者リスト174に記憶された身元テンプレートが、所定の類似度レベルの範囲内で、取引検証プロセス中に機械学習モデル150が第1の取引の実体によって提示された物理的文書102の画像115の少なくとも一部分を表す入力ベクトル142を処理したことに基づいて機械学習モデル150によって生成されたアクティベーションデータ160と一致したため、第1の企業によって拒否された。そのような悪質行為者リストのデータは、段階Aの第1の取引の当事者であった実体が悪質行為者であることを第1の企業が既に知っていたため、第1の企業によって記憶されている可能性がある。

【００７０】

悪質行為を行う実体の第1の企業（例えば、ABC社）との以前の対話に基づき、悪質行為を行う実体は、段階Cで異なる第2の企業（例えば、Mom and Pop's Widgets）で不正取引の別の試みを行おうと考える可能性がある。悪質行為を行う実体の考えは、ウィジェット提供者のABC Inc.などの第1の企業は悪質行為を行う実体の悪巧みに気付いているが、第2のウィジェット提供者のMom and Pop's Widgetsなどの第2の企業は、そのような悪巧みに気付いていないかもしれないというものであり得る。結果として、悪質行為を行う実体は、Mom and Pop's Widgetsなどの第2の企業で同じ（または類似の）不正行為を行おうと試みる可能性がある。

【００７１】

図1の例は、商品、すなわちウィジェットの購入を含む取引を説明している。しかしながら、本開示はそのような取引に限定される必要はない。むしろ、本開示は、ローン申請やクレジット申請などの取引中の金融サービスの申請者のスクリーニング、セルラーサービスやインターネットサービスやケーブルサービスなどの電気通信サービスの申請者のスクリーニング、セキュリティ端末における申請者のスクリーニング、または任意の他のタイプの申請者/実体のスクリーニングを含むがこれらに限定されない、実体認証/検証が行われる実体間の任意の取引または対話の実行中における取引検証/実体認証に使用する

ことができる。したがって、第1の企業および第2の企業は、銀行、金融機関、航空会社、政府機関、電気通信サービスプロバイダ、電気通信デバイスプロバイダ、小売業者、または任意の他の組織を含むがこれらに限定されない、任意の数の企業を含むことができる。

【００７２】

段階Cで、第2の企業の実体は、ユーザデバイス310のカメラ305を使用して、物理的文書102の画像315を取り込み得る。ユーザデバイス310は、取り込まれた画像を表すデータを第2の企業取引検証システム320に送ることができる。ユーザデバイス310は、ネットワーク312を使用して第2の企業取引検証システム320と通信することができる。ネットワーク312は、LAN、WAN、セルラーネットワーク、インターネット、またはそれらの組み合わせなどの1つまたは複数の有線ネットワークまたは無線ネットワークを含むことができる。

【００７３】

第2の企業取引検証システム320は、図1に示される第1の取引検証システム100Aと同様の第2の取引検証システム100Bを含むことができる。すなわち、第2の取引検証システム100Bは、第1の取引検証システム100Aに関して説明されたモジュール、モデル、およびデータベースの各々を含み、第1の取引検証システム100Aに関して説明されたのと同じ動作のすべてを実行することができる。例えば、第2の企業取引検証システム320は、画像315から抽出された画像の一部分315aを表すアクティベーションデータのセットなどの難読化された識別テンプレートを生成することができる。図1の例では、第2の企業取引検証システムは、第2の企業取引検証システム320が、悪質行為者リスト374に記憶された、段階Aおよび段階Bで取引が拒否された悪質行為を行う実体の物理的文書102に所定の誤差閾値内で対応する識別テンプレートを有していない場合でも、協調検証システム220を使用して不正取引を拒否することができる。

【００７４】

図1の例では、第2の企業取引検証システムは、第2の取引検証システム100Bを使用して画像315を取得し、第2の抽出画像部分315aを取得し、取引検証システムがGA（「善良行為者」）リスト372およびBA（「悪質行為者」）リスト374を検索するために使用できる第2のアクティベーションデータのセットを生成することができる。第2の取引検証システム100Bは、善良行為者リスト372内または悪質行為者リスト374内のどの識別テンプレートも、所定の類似度レベルの範囲内で第2のアクティベーションデータのセットと一致しないと判定する可能性がある。したがって、第2の取引検証システム100Bは、第2の取引検証システム100Bの取引検証モジュールを使用して、協調検証システム220が段階Cで試みられた取引をスクリーニングするよう求める要求392を生成することができる。要求392は、物理的文書102表す第2のアクティベーションデータのセットと取引メタデータとを有する第2のデータ構造を含むことができる。

【００７５】

要求392の第2のデータ構造は、第2のアクティベーションデータのセットと第2の取引メタデータとを表すデータを構造化した1つまたは複数のフィールドを含むことができる。第2のアクティベーションデータは、抽出画像部分315aの機械学習モデルの処理に基づく機械学習モデルの隠れ層の出力である。この第2のアクティベーションデータは、第1の取引検証システム100Aに関して説明されたアクティベーションデータ160と同じ方法で生成される。要求392の第2のデータ構造の第2の取引メタデータは、データ構造192と同じかまたは同様のタイプの取引メタデータを含むことができる。例えば、第2の取引メタデータは、取引の時刻、取引の日付、取引の場所、段階Aで実体によって購入もしくはリースのために求められたウィジェットもしくはサービスのタイプ、段階Aで実体によって購入もしくはリースのために求められたウィジェットの個数、段階Aで実体によって求められたサービスのパラメータ、または第1の取引に関連する任意の他の取引メタデータなどの、状態Cで試みられた取引に関連するメタデータを含むことができる。

【００７６】

協調検証システム220は、第2のデータ構造392を受け取ることができる。協調検証システム220は、悪質行為者リスト検索モジュール260を使用して、要求392の第2のデータ構造内に含まれるデータに基づいて協調的悪質行為者リスト240に記憶されたデータをマイニングすることができる。協調的悪質行為者リスト240をマイニングすることは、いくつかの異なる動作のうちの1つまたは複数を含むことができる。例えば、いくつかの実装形態では、協調的悪質行為者リスト240をマイニングすることは、第2のデータ構造392から取得された第2のアクティベーションデータのセットが、所定の類似度レベルの範囲内で、協調的悪質行為者リスト240上のエントリと一致するかどうかを判定することを含むことができる。

【００７７】

例として、協調検証システム220内の悪質行為者リスト検索モジュール260は、要求392の第2のデータ構造を入力として受け取り、要求329の第2のデータ構造に含まれていた第2のアクティベーションデータを抽出することができる。悪質行為者リスト検索モジュール260は、検索パラメータとして第2のアクティベーションデータのセットを含む検索クエリ392aを生成し、協調的悪質行為者リスト294に対して検索クエリ392aを実行することができる。クエリ392aを実行することは、例えば、第2のアクティベーションデータのセットと協調的悪質行為者リスト240に記憶された識別テンプレートの各々との間でベクトル比較を実行することを含むことができる。検索クエリ392aに応答して、検索結果394のセットを悪質行為者リスト検索モジュールによって取得することができる。検索結果394は、識別テンプレートのうちの1つまたは複数が、所定の類似度レベルの範囲内で第2のアクティベーションデータのセットと一致したか否かを示すことができる。協調的悪質行為者リスト240内のどの識別テンプレートも、所定の類似度レベルの範囲内で第2のアクティベーションデータのセットと一致しなかった場合には、悪質行為者リスト検索モジュール260は、第2のアクティベーションデータのセットが協調的悪質行為者リスト240上のどの識別テンプレートとも一致しなかったことを示す応答メッセージを生成することができる。あるいは、協調的悪質行為者リスト240内の識別テンプレートが、所定の類似度レベルの範囲内で第2のアクティベーションデータのセットと一致すると判定された場合には、悪質行為者リスト検索モジュール260は、検索結果394に基づいて、所定の類似度レベルの範囲内で第2のアクティベーションデータのセットと一致する識別テンプレートが協調的悪質行為者リスト240内で見つかったことを示す応答メッセージ394aを生成することができる。いずれの場合も、応答メッセージは、ネットワーク212を介して第2の企業検証サーバ320に返送することができる。

【００７８】

図1の例では、段階Cの取引の当事者である実体と関連付けられた識別テンプレートは、第1の企業取引検証サーバ120によって協調的悪質行為者リストに既に記憶されていたため、悪質行為者リスト検索モジュール260は、第2のアクティベーションデータのセットと一致する識別テンプレートを見つける。したがって、この事例では、応答メッセージ394aは、一致が見つかったことを示し、この応答メッセージは、第2の企業検索取引検証システム320に返送される。第2の取引検証システム100Bの通知モジュールは、応答メッセージ394aに基づいて通知382を生成することができ、通知382は、実体の物理的文書102を表すアクティベーションデータのセットと一致する識別テンプレートが協調的悪質行為者リスト内で見つかったため、段階Cで取引の当事者である人物によって求められた取引が拒否されるべきであることを示す。通知382をユーザデバイス310に送って、取引が拒否されることを示す通知を出力390させることができる。この出力は、例えば、取引が拒否されることを示す「取引は拒否された」などのオーディオメッセージ、第1の取引が拒否されることを示すテキスト、グラフィック、もしくは両方を表示する視覚メッセージ、第1の取引が拒否されることを示す、ユーザデバイス310を振動させるなどの触覚フィードバック、またはそれらの任意の組み合わせを含むことができる。その結果、たとえ第2の企業取引検証サーバ320が、それ自体のローカル悪質行為者リストまたは善良行為者リストに基づいて、段階Cで悪質行為者を検出して取引を拒否することがで

きなかったとしても、第2の企業取引サーバ320は、協調検証システムによって維持され、悪質行為者が検出される際に第1の企業取引検証サーバ120などの1つまたは複数の他の企業によって日常的に更新される協調的悪質行為者リスト240を参照した結果として、物理的文書102を用いて悪質行為者によって段階Cで試みられた取引を拒否することができる。

【００７９】

しかしながら、本開示は、協調的悪質行為者リスト240が所定の類似度レベルの範囲内で第2のアクティベーションデータのセットと一致する識別テンプレートを含むかどうかを判定することに限定される必要はない。代わりに、いくつかの実装形態では、協調的悪質行為者リスト240をマイニングすることは、第2のデータ構造392から取得された第2の取引メタデータが、類似度閾値レベルの範囲内で、協調的悪質行為者リスト240内の1つまたは複数の以前の取引レコードと一致するかどうかを判定することを含むことができる。

【００８０】

例えば、いくつかの実装形態では、悪質行為者リスト検索モジュール260は、協調的悪質行為者リスト240をマイニングして、以前に識別された悪質行為者の他の取引からの取引メタデータを記憶した取引レコードを含むかどうかを判定することができる。例えば、いくつかの実装形態では、段階Cでの取引は、会社「X」のための100個のウィジェットを購入する要求であり得る。そのようなシナリオでは、第2のデータ構造392は、100個のウィジェットの購入注文、購入会社「X」、またはそれらの組み合わせなどの第2の取引メタデータを含むことができる。悪質行為者リスト検索モジュール260は、100個のウィジェット、「X」、またはそれらの組み合わせなどの第2の取引メタデータからクエリパラメータを抽出することができる。悪質行為者リスト検索モジュール260は、「100個のウィジェット」および「X」というクエリパラメータを含むクエリ392aを生成し、協調的悪質行為者リスト240に対してクエリ392aを実行することができる。悪質行為者リスト検索モジュール260は、検索結果394のセットを取得することができる。検索結果394のセットは、クエリ392aを満たす1つまたは複数の取引レコードがあるかどうかを示すことができる。いくつかの実装形態では、検索結果394は、検索クエリ392aを満たす取引レコードが識別されなかったというデータ指示を含み得る。

【００８１】

他の実装形態では、検索結果394は、識別された用語のうちの1つまたは複数を含むものとして識別された1つまたは複数の取引レコードを含むことができる。例えば、悪質行為者リスト検索モジュール260は、100個のウィジェットの購入注文、会社「X」のウィジェットを購入する要求、またはそれらの組み合わせを含んでいた協調的悪質行為者リスト240内の1つまたは複数の取引レコードを識別し得る。そのような事例では、悪質行為者リスト検索モジュールは、協調ネットワーク212を介してセクション取引検証サーバ320に送るための通知394aを生成することができる。通知394aを受け取ると、第2の取引検証システム100Bの通知モジュールは、通知394aを分析し、通知394aの内容に基づいて段階Cで試みられた取引が承認されるべきか拒否されるべきかを判定し、ユーザデバイス310によって処理された場合にユーザデバイス310に、段階Cで試みられた取引が承認されるべきか拒否されるべきかを示す警告または他のメッセージを表示させる通知382を生成することができる。いくつかの実装形態では、通知394aは、協調検証システム220によって、段階Cで試みられた取引を記述する1つまたは複数の現在の取引レコードに類似すると判定された、1つまたは複数の識別された取引レコードを記述するデータを含むことができる。他の実装形態では、通知394aは、単に、段階Cで試みられた取引が承認されるべきか拒否されるべきかを記述するデータだけを含むことができる。

【００８２】

例えば、いくつかの実装形態では、通知382は、段階Cで試みられた取引の拒否を、例えば、段階Cで試みられた取引と、取引レコードを協調的悪質行為者リスト240に記憶させるそもそもの原因となった、別の企業（例えば、第1の企業）での悪質行為者による以

前に試みられた取引との類似度に基づいてトリガすることができる。他の実装形態では、通知382は、取引の承認または拒否が行われる前に、取引のさらなる検討、および段階Cで取引を試みた実体とのさらなる相談をトリガし得る。例えば、おそらくは、その実体に、会社「X」が存在し、100個のウィジェットの購入をカバーするリソース（例えば、銀行口座の現金、十分なクレジットラインなど）を有することを示すために、納税申告情報などのさらなる情報を提供するよう要求することができる。別の例として、さらなる検討および相談は、通知382の処理に基づくユーザデバイス310による、クレジットカード支払いの代わりに現金または為替支払いなどの異なる形の支払いを要求するプロンプトを含み得る。

【００８３】

例示のように、拒否された取引に関連するメタデータを表すデータを含む取引レコードの記憶は、様々な利点を含む。特に、協調的悪質行為者リスト240に記憶された取引レコードは、異なる企業にまたがる悪質行為者による取引を、悪質行為者が各取引で提示する物理的文書102を変更した場合でさえも検出する方法となり得る。異なる取引間での物理的身分証明書の共通表現の代わりに、システム100は、異なる企業間での取引の類似度の評価および検出を実行することができる。この方法論は、一部は、悪質行為者が、異なる企業にまたがって試みる不正取引において傾向に従う可能性が高いという前提に基づくものとすることができる。そのような傾向は、求められたウィジェットまたはサービスのタイプ、求められたウィジェットまたはサービスのブランド、求められたウィジェットまたはサービスの数、支払い方法、デバイスの購入元の会社名、またはそれらの任意の組み合わせにおける類似性を有し得る。よって、これらの形態の取引メタデータの各々を、悪質行為者によって試みられた不正取引を識別するために評価することができる。これらの取引レコードは識別テンプレートを使用してインデックス付けされるため、取引レコードは完全に匿名であり、リバースエンジニアリングすることはできない。

【００８４】

ある事例では、「識別テンプレート」という用語は、物理的文書102などの物理的文書の表現を記述するために使用される。加えて、「アクティベーションデータ」または「アクティベーションベクトル」という用語は、機械学習モデル150の隠れ層の出力を記述するために使用される。しかしながら、いくつかの実装形態では、「識別テンプレート」、「アクティベーションデータ」、または「アクティベーションベクトル」の間にいかなる差異も存在しない場合があることに留意されたい。そのような実装形態では、隠れ層154bによって出力されるアクティベーションデータはアクティベーションデータ160であり、そのアクティベーションデータ160のベクトル表現を識別テンプレートとして使用することができる。他の実装形態では、異なるデータ処理システムにおけるそれぞれの使用を容易にするために、アクティベーションデータ160と、アクティベーションデータ160に対応するアクティベーションベクトルと、アクティベーションデータ160に対応する識別テンプレートとの間に比較的小さなフォーマットの差異が生じる場合がある。例えば、アクティベーションデータを記憶のために識別テンプレートにするときに、アクティベーションベクトルにヘッダフィールドなどのデータフィールドが追加される場合がある。いずれにせよ、同義的にアクティベーションベクトルまたは実行時識別テンプレートと呼ぶことができる新たに生成されたアクティベーションデータ160と、記憶された識別テンプレートとの間の比較が、本明細書に記載されるように訓練された機械学習モデル150の隠れ層154bによって出力されたアクティベーションデータを評価することによって行われる。

【００８５】

図2は、取引をスクリーニングするために協調取引検証システムを使用して取引を検証するためのプロセス200の一例のフローチャートである。プロセス200は、1つまたは複数の電子システム、例えば図1のシステム100によって実行され得る。

【００８６】

システム100は、取引の当事者を識別する物理的文書の少なくとも一部分を表す第1の

データを、第1の企業取引検証システムにより受け取ることによってプロセス200の実行を開始することができる（210）。いくつかの実装形態では、取得された第1のデータは、取引の当事者を識別する物理的文書の少なくとも部分を表す入力ベクトルを含むことができる。入力データベクトルは、スマートフォンなどのユーザデバイスによって生成され、ユーザデバイスによってサーバに送られた取引の当事者を識別する物理的文書の画像の少なくとも一部分に基づいて生成することができる。画像は、LAN、WAN、セルラーネットワーク、インターネット、またはそれらの組み合わせなどの1つまたは複数の有線ネットワークまたは無線ネットワークを介して受け取ることができる。取り込まれた画像は、取引の当事者を識別する物理的文書の全部または一部分を描写することができる。

【００８７】

いくつかの実装形態では、取得された第1のデータは、物理的文書から抽出された複数の局面を表すことができる。例えば、取得された第1のデータは、文書の一部分、文書上の顔画像、または物理的文書によって描写された様々な経歴、テキスト、もしくはコードベースのデータ（例えば、バーコード、クイックレスポンス（QR）コードなど）といった他のデータを含むことができる。

【００８８】

システム100は、プロセス200の実行を継続して、第1のデータの難読化を表す第2のデータを生成することができる（220）。いくつかの実装形態では、第2のデータは、機械学習モデルの隠れ層によって生成することができる。例えば、第1のデータの難読化は、機械学習モデルが段階210で取得された第1のデータを処理した結果として機械学習モジュールの隠れ層によって出力されたアクティベーションデータのセットを含むことができる。いくつかの実装形態では、機械学習モデルの隠れ層は、機械学習モデルが訓練されている偽造防止アーキテクチャの1つまたは複数のセキュリティ特徴の有無を検出するように訓練されている隠れセキュリティ特徴識別器層を含むことができる。

【００８９】

システム100は、プロセス200の実行を継続して、第1の企業取引検証システムにより、かつ第2のデータに基づいて、取引が拒否されるべきかどうかを判定することができる（230）。例えば、システム100は、取引が許可されるべき実体を表す他の取引の他の当事者についての1つまたは複数の物理的文書を表す以前に生成されたアクティベーションデータを記憶している善良行為者リスト、取引が拒否されるべき他の取引の他の当事者についての1つまたは複数の物理的文書を表す以前に生成されたアクティベーションデータを記憶している悪質行為者リスト、またはその両方の組み合わせを検索して、取得されたアクティベーションデータが、善良行為者リスト、悪質行為者リスト、またはその両方に記憶されたアクティベーションデータのインスタンスのいずれかの所定の誤差量内にあるかどうかを判定することによって、取引が拒否されるべきかどうかを判定することができる。

【００９０】

取引が拒否されるべきであると判定したことに基づき、システム100は、プロセス200の実行を継続して、所定の時間量にわたって第2のデータを含む1つまたは複数のデータレコードを含むように協調検証システムのデータベースを更新することができ、協調検証ネットワークは、協調検証システムのメンバーである他の企業における当事者による1つまたは複数の他の取引についての先制拒否を可能にする（240）。難読化された第2のデータ、取引メタデータ、またはそれらの組み合わせを表すデータを構造化した1つまたは複数のフィールドを含むデータ構造を、第1の企業取引検証システムによって協調検証システムに送ることができる。データ構造によって構造化されたデータの少なくとも一部分を、協調検証ネットワークによって記憶することができる。いくつかの実装形態では、データを、協調ネットワークによって協調的悪質行為者リストに記憶することができる。

【００９１】

同じ企業検証システムまたは異なる企業検証システムからの他の取引検証要求もまた、協調検証システムに送ることができる。他の取引検証要求からのデータは、以前の取引を

表す以前に記憶されたデータからのデータと比較され得る。協調検証システムによって記憶されたデータは、個人を特定できる情報を公開するのを防止するために上述した方法で難読化されており、しかも同時に、1人または複数人の悪質行為者による不正取引を働こうとする試みの可能性があるインスタンスを認識する能力を維持している。次いで、以前に実行された取引およびそれらの取引と関連付けられた当事者から記憶されたデータを使用して、協調検証システムのメンバーであるユーザまたは企業のうちの1者または複数に現在の認証および不正検出プロセスを通知することができる。

【００９２】

図3は、協調取引検証システム300の一例のコンテキスト図である。システム300は、カメラ105、ユーザデバイス110、画像115、第1の企業取引検証サーバ120、第1の取引検証システム100A、協調検証システム220、ネットワーク112、212、312、第2の企業取引検証システム320、第2の取引検証システム100B、カメラ305、およびユーザデバイス310など、図1のシステム100からの同じ特徴の多くを含む。実際、システム300は、システム300が、第1の企業取引検証サーバ120の取引履歴データベース176および協調検証システム220の悪質行為者リスト更新モジュール230と通信するユーザ端末412も含むことを除いて、システム100と同じである。システム300のそのような追加の特徴は、ユーザ412aなどのユーザが、取引レコードを検討し、悪質行為者によって求められた取引が第1の企業取引検証サーバ120によって承認された後のある時点で、悪質行為者に関連する識別テンプレート、取引メタデータ、またはその両方を協調的悪質行為者リスト240に追加することを可能にする。図3の例では、段階Aから段階Bまでおよび段階Cから段階Dまでのプロセスが示されている。

【００９３】

図3の例を参照すると、実体は、段階Aで取引を開始しようと試みることができる。取引の一部として、実体は、物理的文書102を提示することができる。検証当事者は、カメラ105ユーザデバイス110を使用して、物理的文書102の画像115を取り込むことができる。画像115は、物理的文書102の画像の少なくとも一部分を描写している抽出画像部分115a、および物理的文書102の画像115が取り込まれたときの周囲環境の一部分を描写している第2の部分115bを含むことができる。ユーザデバイス110は、ネットワーク112を使用して第1の取引検証サーバ120に画像115を送ることができる。ネットワーク112は、有線ネットワーク、無線ネットワーク、LAN、WAN、セルラーネットワーク、インターネット、またはそれらの任意の組み合わせを含むことができる。

【００９４】

第1の企業取引検証サーバ120は、図1を参照して説明されたプロセスを使用して、物理的文書102の画像115の取引検証を実行することができる。しかしながら、例示目的で、図3の例では、善良行為者リスト172または悪質行為者リスト174のいずれにおいても、アクティベーションデータ160と一致する識別テンプレートが見つからないと仮定する。したがって、図3のこの例では、通知ユニット180は、段階Aで要求された取引が拒否されないことを示す通知482を生成することができる。通知482は、段階Bでユーザデバイスに送ることができ、ユーザデバイス110によって処理された場合にユーザデバイス110に、取引が拒否されないことを示すデータを出力させる。例として、いくつかの実装形態では、ユーザデバイスは、「取引が承認された」ことを示すメッセージを出力することができる。そのようなメッセージはまた、音声データ、触覚フィードバックなどを使用して出力されてもよい。

【００９５】

通知482は、それ自体では解決の手がかりとならないが、第1の企業取引検証サーバ120が段階Aで要求された取引が定義されるべき理由を発見しなかったことを示す。この例では、ユーザデバイス110のユーザには、段階Aで要求された取引を拒否する他のどんな理由もなかった。その結果、第1の企業の代表者は、取引を許可することができる。この例のために、取引は、10年間にわたって返済可能な会社「Y」による50万ドルのローンを求める要求であったと仮定する。ここでは、50万ドルのローンを承認された取引の

当事者であった実体は、会社「Y」の銀行口座に50万ドルが預けられた状態で金融機関を去る。図3の例では、CTVS更新モジュール190は、段階Aおよび段階Bでの取引が承認されたため、協調検証システム220を更新しない。

【００９６】

しかしながら、段階Aおよび段階Bで発生した取引に関連する取引メタデータを取引履歴データベースに記憶することができる。取引履歴データベース176は、例えば、第1の企業によって行われたすべての販売、リース、ローン、物件への立入り許可、物件への立入り拒否などの取引レコードを含むことができる。この例では、取引履歴データベース176に、ローン金額:50万ドル、支払期間:10年、借り手:会社「Y」などの取引メタデータを記憶した取引レコードを記憶することができる。取引レコードには、段階Aと段階Bとの間の第1の取引検証サーバ120による取引のスクリーニング中に生成されたアクティベーションデータ160を使用してインデックス付けすることができる。取引履歴データベース176はまた、会社「Y」から受け取られたローン支払いを示すデータ、会社「Y」からローン支払いが受け取られなかったことを示すデータ、または会社「Y」に対するローンの状況を記述する他のデータを記憶するように更新することができる。

【００９７】

図3の例では、段階Bでの承認後のある時点で、取引の当事者であった実体（または他のユーザ）は50万ドルのローンの支払いを怠る。そのようなシナリオでは、第1の企業は、第1の企業が金銭的損失を被る立場に置かれる可能性が高い。

【００９８】

その実体（または他のユーザ）が会社「Y」の50万ドルのローンを停止した後のある時点で、ユーザ412aは、ユーザデバイス412を使用して取引履歴データベース176内の取引レコードを検討することができる。ユーザ412aは、会社「Y」のローンに対応する取引履歴内の50万ドルのローンに対する会社「Y」の支払いの不履行を検出することができる。そのようなシナリオでは、ユーザ412aは、ユーザデバイス412を使用して、協調検証システム220の悪質行為者リスト更新モジュール230に、取引レコードを協調的悪質行為者リスト240に追加するよう命令することができる。協調的悪質行為者リスト240へのそのような更新は、段階Aでの取引の当事者であった実体が、協調検証システム220と関連付けられた他の企業を、その実体が第1の企業を欺いたのと同じ方法で（例えば、ローンを支払わないことによって）欺くのを防ぐことができる。ユーザデバイス412からの命令は、協調ネットワーク212を使用して協調検証システム220に送ることができる。段階Aで要求された取引について記憶された取引レコードの一部であった識別テンプレート、取引メタデータ、またはその両方を、協調的悪質行為者リスト240に記憶することができる。

【００９９】

ユーザ412aがコンピュータを使用して悪質行為者リスト230を更新した後の時点で、その実体は段階Cで別の不正な取引を試みる可能性がある。例えば、ユーザ412aは、会社「Y」のための別の50万ドルのローンまたは異なるlローン金額の安全を確保しようと試みることができる。段階Cで、第2の企業の代表者は、ユーザデバイス310のカメラ305を使用して、物理的文書102の画像315を取り込み得る。ユーザデバイス310は、ネットワーク312を使用して第2の企業取引検証システム320と通信することができる。第2の企業取引検証システム320は、図1に示される第1の取引検証システム100Aと同様の第2の取引検証システム100Bを含むことができる。すなわち、第2の取引検証システム100Bは、第1の取引検証システム100Aに関して説明されたモジュール、モデル、およびデータベースの各々を含み、第1の取引検証システム100Aに関して説明されたのと同じ動作のすべてを実行することができる。例えば、第2の企業取引検証システム320は、画像315から抽出された画像の一部分315aを表すアクティベーションデータのセットなどの難読化された識別テンプレートを生成することができる。図1の例では、第2の企業取引検証システムは、第2の企業取引検証システム320が、段階Aおよび段階Bで取引が拒否された悪質行為を行う実体の物理的文書102に所定の誤差閾値内で対応する識別テン

プレートを有していない場合でも、協調検証システム220を使用して不正取引を拒否することができる。

【０１００】

図3の例では、第2の企業取引検証システム320は、第2の取引検証システム100Bを使用して画像315を取得し、第2の抽出画像部分315aを取得し、取引検証システムが善良行為者リスト372および悪質行為者リスト374を検索するために使用することができる第2のアクティベーションデータのセットを生成することができる。第2の取引検証システム100Bは、善良行為者リスト372内または悪質行為者リスト374内のどの識別テンプレートも、所定の類似度レベルの範囲内で第2のアクティベーションデータのセットと一致しないと判定する可能性がある。したがって、第2の取引検証システム100Bは、第2の取引検証システム100Bの取引検証モジュールを使用して、協調検証システム220に段階Cで試みられた取引をスクリーニングするよう求める要求392を生成することができる。要求392は、物理的文書102表す第2のアクティベーションデータのセットと取引メタデータとを有する第2のデータ構造を含むことができる。

【０１０１】

協調検証システム220は、要求392を受け取ることができる。協調検証システム220は、悪質行為者リスト検索モジュール260を使用して、第2のデータ構造要求392内に含まれるデータに基づいて協調的悪質行為者リスト240に記憶されたデータをマイニングすることができる。協調的悪質行為者リスト240をマイニングすることは、いくつかの異なる動作のうちの1つまたは複数を含むことができる。例えば、いくつかの実装形態では、協調的悪質行為者リスト240をマイニングすることは、第2のデータ構造392から取得された第2のアクティベーションデータのセットが、所定の類似度レベルの範囲内で、協調的悪質行為者リスト240上のエントリと一致するかどうかを判定することを含むことができる。あるいは、いくつかの実装形態では、協調的悪質行為者リスト240をマイニングすることは、第2のデータ構造392から取得された第2の取引メタデータが、類似度閾値レベルの範囲内で、協調的悪質行為者リスト240内の1つまたは複数の以前の取引レコードと一致するかどうかを判定することを含むことができる。

【０１０２】

この例では、選択されたマイニング技術にかかわらず、悪質行為者リスト検索モジュール260は、段階Cでの悪質行為者の以前の取引と関連付けられた協調的悪質行為者リスト240内の情報を識別することができる。例えば、悪質行為者リストモジュール260は、第2の取引検証システム100Bによって生成された第2のアクティベーションデータのセットを含むクエリ392aを生成することができる。そのような事例では、ユーザ412aがユーザデバイス412aを使用して協調的悪質行為者リスト240にアクティベーションデータ160を記憶したので、検索結果594は、第2のアクティベーションデータのセットが協調的悪質行為者リスト240内の識別テンプレートと一致することを示す。あるいは、悪質行為者リスト検索モジュール260は、段階Cで試みられた取引の取引メタデータに対応する取引レコードを求めて協調的悪質行為者リスト240を検索することもできる。そのような事例では、悪質行為者リスト検索モジュール260は、段階Cでの取引からの取引メタデータに基づくパラメータを含むクエリ392aを使用することができる。そのような事例では、クエリ392aのパラメータは、ローン金額「50万ドル」、支払期間「10年」、借り手「会社『Y』」を含むことができる。ここで、検索結果594は、会社「Y」が支払条件または返済条件を履行しないことによって不誠実な行為をした（例えば、以前のローン債務を怠った、商品に対するクレジットカード支払いを取り消したなどの）少なくとも1つの取引が識別されたことを示すことができる。

【０１０３】

検索結果に基づき、悪質行為者リスト検索モジュールは、協調ネットワーク212を介してセクション取引検証サーバ320に送るための通知594aを生成することができる。図3の例では、通知594aは、段階Cで試みられた取引が拒否されるべきであることを示すデータを含むことができる。通知594aを受け取ると、第2の取引検証システム100Bの

通知モジュールは、1つまたは複数の識別された取引レコードを記述するデータを含む通知582を生成することができる。通知582は、表示のためにユーザデバイス310に送ることができる。

【０１０４】

ある実装形態では、通知582は、段階Cで試みられた取引の拒否をトリガすることができる。拒否の理由は、例えば、段階Cで試みられた取引と、取引レコードを協調的悪質行為者リスト240に記憶させる原因となった、段階Cで取引を試みた悪質行為者によって以前に試みられたかまたは完了された取引との類似度に基づくものとすることができる。他の実装形態では、通知582は、取引の承認または拒否が行われる前に、取引のさらなる検討、および段階Cで取引を試みた実体とのさらなる相談をトリガし得る。例えば、おそらく、その実体に、手元の流動資産の限度額の証明などのさらなる情報を提供するように要求することができる。

【０１０５】

図3に示されるように、拒否された取引に関連するメタデータを含む取引レコードの記憶は、様々な利点を含む。特に、ユーザ412aがユーザデバイス412を使用して協調的悪質行為者リスト240を更新できるようにすることにより、たとえ悪質行為者が第1の企業において同様の不正取引を完了することに成功したとしても、悪質行為者による将来の不正取引が1つまたは複数の第2の企業において停止されることを可能にする機能が提供される。

【０１０６】

図4は、協調取引検証システムを使用して取引を検証するためのプロセスの一例のフローチャートである。プロセス400は、1つまたは複数の電子システム、例えば図3のシステム300によって実行され得る。

【０１０７】

システム300は、取引の当事者を識別する物理的文書の少なくとも一部分を表す第1のデータを、第1の企業取引検証システムにより受け取ることによってプロセス400の実行を開始することができる（410）。いくつかの実装形態では、取得された第1のデータは、取引の当事者を識別する物理的文書の少なくとも部分を表す入力ベクトルを含むことができる。入力データベクトルは、スマートフォンなどのユーザデバイスによって生成され、ユーザデバイスによってサーバに送られた取引の当事者を識別する物理的文書の画像の少なくとも一部分に基づいて生成することができる。画像は、LAN、WAN、セルラーネットワーク、インターネット、またはそれらの組み合わせなどの1つまたは複数の有線ネットワークまたは無線ネットワークを介して受け取ることができる。取り込まれた画像は、取引の当事者を識別する物理的文書の全部または一部分を描写することができる。

【０１０８】

いくつかの実装形態では、取得された第1のデータは、物理的文書から抽出された複数の局面を表すことができる。例えば、取得された第1のデータは、文書の一部分、文書上の顔画像、または物理的文書によって描写された様々な経歴、テキスト、もしくはコードベースのデータ（例えば、バーコード、クイックレスポンス（QR）コードなど）といった他のデータを含むことができる。

【０１０９】

システム300は、プロセス400の実行を継続して、第1のデータの難読化を表す第2のデータを生成することができる（420）。いくつかの実装形態では、第2のデータは、機械学習モデルの隠れ層によって生成することができる。例えば、第1のデータの難読化は、機械学習モデルが段階210で取得された第1のデータを処理した結果として機械学習モジュールの隠れ層によって出力されたアクティベーションデータのセットを含むことができる。いくつかの実装形態では、機械学習モデルの隠れ層は、機械学習モデルが訓練されている偽造防止アーキテクチャの1つまたは複数のセキュリティ特徴の有無を検出するように訓練されている隠れセキュリティ特徴識別器層を含むことができる。

【０１１０】

システム300は、プロセス400の実行を継続して、第2のデータを、所定の時間量にわたって第1の企業取引検証システムのデータベースに記憶することができる（430）。いくつかの実装形態では、図3の取引履歴データベース176などの取引履歴データベースを使用して第2のデータを記憶することができる。

【０１１１】

段階430で第2のデータを記憶した後に、システム300は、プロセス400の実行を継続して、第1の企業取引検証システムにより、取引が正規の取引ではないと判定することができる（440）。いくつかの実装形態では、取引が正規の取引ではないと判定することは、取引に関連するデータのさらなる検討を行うことを含む。例えば、図3では、人間412aは、段階Aに示される第1の取引に関連するデータのさらなる検討を行う。人間412aによって行われたさらなる検討により、第1の取引は信用できるものではなく、拒否されるべきであるという判定が得られる。

【０１１２】

取引が正規の取引ではないと判定したことに基づき、システム300は、プロセス400の実行を継続して、第2の所定の時間量にわたって第2のデータを含む1つまたは複数のデータレコードを含むように協調検証システムのデータベースを更新することができ、協調検証システムが、協調検証システムのメンバーである他の企業における当事者による1つまたは複数の他の取引についての先制拒否を可能にする（450）。例えば、段階Aに示される第1の取引に関連するデータは、さらなる検討の後に行われた判定に基づいて協調的悪質行為者リスト240に記憶される。この場合、さらなる検討は人間412aによって行われる。

【０１１３】

段階Cに示される第2の取引に関連するデータは、段階Aに示される第1の取引から協調的悪質行為者リスト240に記憶されたデータの要素と一致する。一致に基づき、第2の取引は拒否される。協調検証システム220は、第1の取引の当事者を第2の取引の当事者に関連付けることによって、第2の取引の拒否を可能にした。段階Aおよび段階Cの第1の取引および第2の取引の両方でそれぞれ使用された物理的文書102によって示されるように、2つの取引の当事者は同じであり、協調検証システム220は、第1の取引の当事者が人間412aによって行われたさらなる検討によって信用できるものではないとみなされたという事実に基づいて第2の取引を拒否することができる。これらの取引に関連するデータは難読化されているため、信用できない第2の取引が妨げられるだけでなく、個人を特定できる情報が公開されないため、プライバシー要件も満たされる。

【０１１４】

図5は、認証取引に使用するシステム構成要素のブロック図である。コンピューティングデバイス500は、ラップトップ、デスクトップ、ワークステーション、パーソナルデジタルアシスタント、サーバ、ブレードサーバ、メインフレーム、および他の適切なコンピュータなどの様々な形態のデジタルコンピュータを表すことが意図されている。コンピューティングデバイス550は、パーソナルデジタルアシスタント、セルラー電話、スマートフォン、および他の同様のコンピューティングデバイスなどの、様々な形態のモバイルデバイスを表すことが意図されている。加えて、コンピューティングデバイス500または550は、ユニバーサルシリアルバス（USB）フラッシュドライブも含むことができる。USBフラッシュドライブは、オペレーティングシステムおよび他のアプリケーションを記憶することができる。USBフラッシュドライブは、別のコンピューティングデバイスのUSBポートに挿入できる無線トランシーバやUSBコネクタなどの入力/出力構成要素を含むことができる。ここに示される構成要素、それらの接続および関係、ならびにそれらの機能は、例示を意図しているにすぎず、本出願において記載および/または特許請求される発明の実装形態の限定を意図するものではない。

【０１１５】

コンピューティングデバイス500は、プロセッサ502と、メモリ504と、記憶デバイス506と、メモリ504および高速拡張ポート510に接続する高速インターフェース508

と、低速バス514および記憶デバイス506に接続する低速インターフェース512とを含む。構成要素502、504、506、508、510および512の各々は、様々なバスを使用して相互接続され、共通のマザーボード上に、または必要に応じて他の方法で搭載することができる。プロセッサ502は、高速インターフェース508に結合されたディスプレイ516などの、外部入力/出力デバイス上にGUIのグラフィック情報を表示するためのメモリ504または記憶デバイス506に記憶された命令を含む、コンピューティングデバイス500内で実行するための命令を処理することができる。他の実装形態では、複数のプロセッサおよび/または複数のバスを、必要に応じて、複数のメモリおよび複数のタイプのメモリと共に使用することができる。また、各コンピューティングデバイスが、例えば、サーババンク、ブレードサーバのグループ、またはマルチプロセッサシステムとして、必要な動作の部分を提供する、複数のコンピューティングデバイス500を接続することもできる。

【０１１６】

メモリ504は、コンピューティングデバイス500内の情報を記憶する。一実装形態では、メモリ504は1つまたは複数の揮発性メモリユニットである。別の実装形態では、メモリ504は、1つまたは複数の不揮発性メモリユニットである。メモリ504は、磁気ディスクや光ディスクなどの、別の形態のコンピュータ可読媒体とすることもできる。

【０１１７】

記憶デバイス506は、コンピューティングデバイス500に大容量記憶を提供することができる。一実装形態では、記憶デバイス506は、フロッピーディスクデバイス、ハードディスクデバイス、光ディスクデバイス、もしくはテープデバイス、フラッシュメモリもしくは他の同様のソリッドステートメモリデバイス、または、ストレージエリアネットワークもしくは他の構成におけるデバイスを含むデバイスの配列などの、コンピュータ可読媒体とすることができるか、またはコンピュータ可読媒体を含むことができる。コンピュータプログラム製品を、情報キャリアにおいて有形的に具現化することができる。コンピュータプログラム製品はまた、実行された場合に上述のような1つまたは複数の方法を実行する命令を含むこともできる。情報キャリアは、メモリ504、記憶デバイス506、またはプロセッサ502上のメモリなどのコンピュータ可読媒体または機械可読媒体である。

【０１１８】

高速コントローラ508はコンピューティングデバイス500のための帯域幅集約型動作を管理し、低速コントローラ512は帯域幅集約性の低い動作を管理する。そのような機能の割り振りは例示にすぎない。一実装形態では、高速コントローラ508は、メモリ504と、例えば、グラフィックスプロセッサやアクセラレータを介して、ディスプレイ516と、様々な拡張カード（図示せず）を受け入れることができる高速拡張ポート510とに結合される。この実装形態では、低速コントローラ512は、記憶デバイス506と低速拡張ポート514とに接続される。低速拡張ポートは、様々な通信ポート、例えば、USB、ブルートゥース、イーサネット、無線イーサネットを含むことができ、キーボード、ポインティングデバイス、マイクロホン/スピーカ対、スキャナなどの1つもしくは複数の入力/出力デバイスに、または、例えばネットワークアダプタを介して、スイッチやルータなどのネットワーキングデバイスに結合することができる。コンピューティングデバイス500は、図に示されるように、いくつかの異なる形で実装することができる。例えば、コンピューティングデバイス500は、標準的なサーバ520として、または多くはそのようなサーバのグループとして実装することができる。コンピューティングデバイス500は、ラックサーバシステム524の一部として実装することもできる。加えて、コンピューティングデバイス500は、ラップトップコンピュータ522などのパーソナルコンピュータに実装することもできる。あるいは、コンピューティングデバイス500の構成要素を、デバイス550などのモバイルデバイス内の他の構成要素（図示せず）と組み合わせることもできる。そのようなデバイスの各々がコンピューティングデバイス500、550のうちの1つまたは複数を含むことができ、システム全体を、互いに通信し合う複数のコンピューティングデバイス500、550で構成することができる。

【０１１９】
コンピューティングデバイス５００は、図に示されるように、いくつかの異なる形で実装することができる。例えば、コンピューティングデバイス５００は、標準的なサーバ５２０として、または多くはそのようなサーバのグループとして実装することができる。コンピューティングデバイス５００は、ラックサーバシステム５２４の一部として実装することもできる。加えて、コンピューティングデバイス５００は、ラップトップコンピュータ５２２などのパーソナルコンピュータに実装することもできる。あるいは、コンピューティングデバイス５００の構成要素を、デバイス５５０などのモバイルデバイス内の他の構成要素（図示せず）と組み合わせることもできる。そのようなデバイスの各々がコンピューティングデバイス５００、５５０のうちの１つまたは複数を含むことができ、システム全体を、互いに通信し合う複数のコンピューティングデバイス５００、５５０で構成することができる。
【０１２０】
コンピューティングデバイス５５０は、構成要素の中でも特に、プロセッサ５５２と、メモリ５６４と、ディスプレイ５５４などの入力/出力デバイスと、通信インターフェース５６６と、トランシーバ５６８とを含む。デバイス５５０はまた、追加の記憶を提供するために、マイクロドライブや他のデバイスなどの記憶デバイスを備えることもできる。構成要素５５０、５５２、５６４、５５４、５６６および５６８の各々は、様々なバスを使用して相互接続され、構成要素のうちのいくつかを、共通のマザーボード上に、または必要に応じて他の方法で搭載することができる。
【０１２１】
プロセッサ５５２は、メモリ５６４に記憶された命令を含む、コンピューティングデバイス５５０内の命令を実行することができる。プロセッサは、別個の複数のアナログプロセッサおよびデジタルプロセッサを含むチップのチップセットとして実装することができる。加えて、プロセッサは、いくつかのアーキテクチャのいずれかを使用して実装することもできる。例えば、プロセッサ５１０は、ＣＩＳＣ（複合命令セットコンピュータ）プロセッサや、ＲＩＳＣ（縮小命令セットコンピュータ）プロセッサや、ＭＩＳＣ（最小命令セットコンピュータ）プロセッサとすることもできる。プロセッサは、例えば、ユーザインターフェースの制御、デバイス５５０によって実行されるアプリケーション、およびデバイス５５０による無線通信など、デバイス５５０の他の構成要素の調整を提供することができる。
【０１２２】
プロセッサ５５２は、制御インターフェース５５８およびディスプレイ５５４に結合された表示インターフェース５５６を介してユーザと通信することができる。ディスプレイ５５４は、例えば、ＴＦＴ（薄膜トランジスタ液晶ディスプレイ）ディスプレイ、ＯＬＥＤ（有機発光ダイオード）ディスプレイ、または他の適切な表示技術とすることができる。表示インターフェース５５６は、ユーザにグラフィック情報および他の情報を提示するようディスプレイ５５４を駆動するための適切な回路を含むことができる。制御インターフェース５５８は、ユーザからコマンドを受け取り、それらのコマンドをプロセッサ５５２に送るために変換することができる。加えて、デバイス５５０と他のデバイスとの近距離通信を可能にするように、プロセッサ５５２と通信する外部インターフェース５６２を設けることもできる。外部インターフェース５６２は、例えば、いくつかの実装形態では有線通信を提供することができ、または他の実装形態では無線通信を提供することができ、複数のインターフェースを使用することもできる。
【０１２３】
メモリ５６４は、コンピューティングデバイス５５０内の情報を記憶する。メモリ５６４は、１つもしくは複数のコンピュータ可読媒体、１つもしくは複数の揮発性メモリユニット、または１つもしくは複数の不揮発性メモリユニットのうちの１つまたは複数として実装することができる。拡張メモリ５７４を設け、拡張インターフェース５７２を介してデバイス５５０に接続することもでき、拡張インターフェース５７２は、例えば、ＳＩＭＭ（シングルインラインメモリモジュール）カードインターフェースを含むことができる。そのような拡張メモリ５７４は、デバイス５５０に追加の記憶空間を提供することができ、またはデ

バイス550のためのアプリケーションまたは他の情報を記憶することもできる。具体的には、拡張メモリ574は、上述のプロセスを実行または補足する命令を含むことができ、セキュア情報も含むことができる。よって、例えば、拡張メモリ574は、デバイス550のためのセキュリティモジュールとして設けることができ、デバイス550のセキュアな使用を可能にする命令でプログラムすることができる。加えて、セキュアアプリケーションを、識別情報をSIMMカード上にハッキングできない方法で配置するなど、追加情報と共にSIMMカードを介して提供することもできる。

【０１２４】

メモリは、後述するように、例えば、フラッシュメモリおよび/またはNVRAMを含むことができる。一実装形態では、コンピュータプログラム製品が、情報キャリアにおいて有形的に具現化される。コンピュータプログラム製品は、実行された場合に上述のような1つまたは複数の方法を実行する命令を含む。情報キャリアは、例えばトランシーバ568または外部インターフェース562を介して受け取りをすることができる、メモリ564、拡張メモリ574、またはプロセッサ552上のメモリなどのコンピュータ可読媒体または機械可読媒体である。

【０１２５】

デバイス550は、通信インターフェース566を介して無線で通信することができ、通信インターフェース566は必要に応じてデジタル信号処理回路を含むことができる。通信インターフェース566は、中でも特に、GSM音声通話、SMS、EMS、もしくはMMSメッセージング、CDMA、TDMA、PDC、WCDMA、CDMA2000、またはGPRSなどの様々なモードまたはプロトコルの下での通信を提供することができる。そのような通信は、例えば、無線周波数トランシーバ568を介して行うことができる。加えて、近距離通信を、例えば、ブルートゥース、Wi-Fi、または他のそのようなトランシーバ（図示せず）を使用して行うこともできる。加えて、GPS（全地球測位システム）レシーバモジュール570が、デバイス550に、デバイス550上で動作するアプリケーションによって必要に応じて使用され得る、追加的なナビゲーションおよび位置特定に関連した無線データを、提供することもできる。

【０１２６】

デバイス550はまた、オーディオコーデック560を使用して音声で通信することもでき、オーディオコーデック560は、ユーザから音声による情報を受け取り、それを使用可能なデジタル情報に変換することができる。オーディオコーデック560は、同様に、例えば、デバイス550のハンドセット内のスピーカなどを介して、ユーザに対して可聴音を生成することもできる。そのような音は、音声通話からの音を含むことができ、録音された音、例えば、音声メッセージ、音楽ファイルなどを含むことができ、デバイス550上で動作するアプリケーションによって生成された音も含むことができる。

【０１２７】

コンピューティングデバイス550は、図に示されるように、いくつかの異なる形で実装することができる。例えば、コンピューティングデバイス550は、セルラー電話580として実装することもできる。コンピューティングデバイス550は、スマートフォン582、パーソナルデジタルアシスタント、または他の同様のモバイルデバイスの一部として実装することもできる。

【０１２８】

本明細書に記載されるシステムおよび方法の様々な実装形態を、デジタル電子回路、集積回路、専用に設計されたASIC（特定用途向け集積回路）、コンピュータハードウェア、ファームウェア、ソフトウェア、および/またはそのような実装形態の組み合わせにおいて実現することができる。これら様々な実装形態は、記憶システム、少なくとも1つの入力デバイス、および少なくとも1つの出力デバイスからデータおよび命令を受け取り、記憶システム、少なくとも1つの入力デバイス、および少なくとも1つの出力デバイスにデータおよび命令を送るように結合された、専用または汎用とすることができる、少なくとも1つのプログラマブルプロセッサを含むプログラマブルシステム上で実行可能および

/または解釈可能な1つまたは複数のコンピュータプログラムにおける実装を含むことができる。

【０１２９】

これらのコンピュータプログラムは（プログラム、ソフトウェア、ソフトウェアアプリケーションまたはコードとも呼ばれ）、プログラマブルプロセッサのための機械命令を含み、高水準手続き型プログラミング言語および/またはオブジェクト指向プログラミング言語、および/またはアセンブリ言語/機械語で実装することができる。本明細書で使用される場合、「機械可読媒体」、「コンピュータ可読媒体」という用語は、機械命令を機械可読信号として受け取る機械可読媒体を含む、プログラマブルプロセッサに機械命令および/またはデータを提供するために使用される任意のコンピュータプログラム製品、装置および/またはデバイス、例えば、磁気ディスク、光ディスク、メモリ、プログラマブル論理デバイス（ＰＬＤ）を指す。「機械可読信号」という用語は、プログラマブルプロセッサに機械命令および/またはデータを提供するために使用される任意の信号を指す。

【０１３０】

ユーザとの対話を提供するために、本明細書に記載されるシステムおよび技術を、ユーザに情報を表示するための表示デバイス、例えばＣＲＴ（ブラウン管）やＬＣＤ（液晶ディスプレイ）モニタと、ユーザがコンピュータに入力を提供するためのキーボードおよびポインティングデバイス、例えばマウスやトラックボールとを有するコンピュータ上で実装することができる。他の種類のデバイスを使用してユーザとの対話を提供することもでき、例えば、ユーザに提供されるフィードバックは、任意の形の感覚的フィードバック、例えば、視覚フィードバック、聴覚フィードバック、または触覚フィードバックとすることができ、ユーザからの入力を、音響、音声、または触覚入力を含む、任意の形で受け取ることができる。

【０１３１】

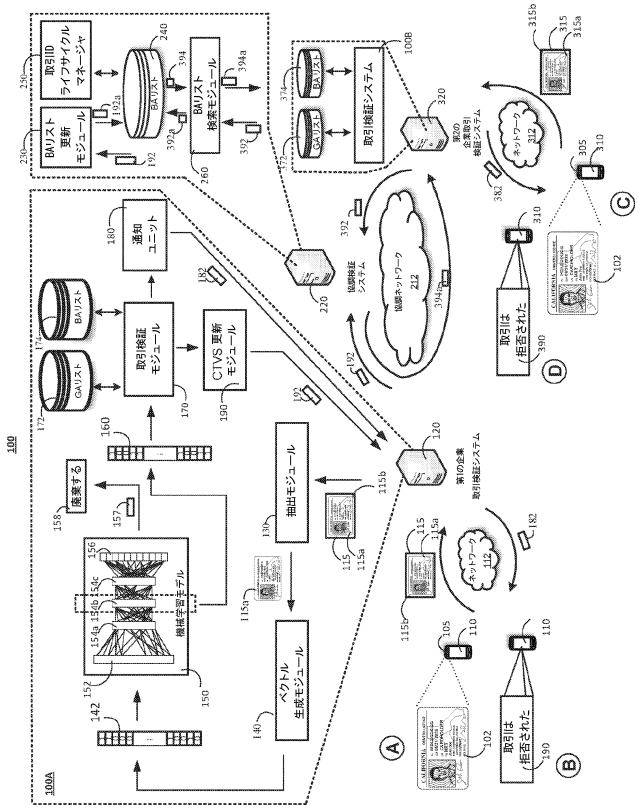
本明細書に記載されるシステムおよび技術を、例えばデータサーバとしてバックエンドコンポーネントを含むコンピューティングシステム、またはミドルウェアコンポーネント、例えばアプリケーションサーバを含むコンピューティングシステム、またはフロントエンドコンポーネント、例えば、ユーザが本明細書に記載されるシステムおよび技術の実装形態と対話するためのグラフィカルユーザインターフェースまたはウェブブラウザを有するクライアントコンピュータを含むコンピューティングシステム、またはそのようなバックエンドコンポーネント、ミドルウェアコンポーネントもしくはフロントエンドコンポーネントの任意の組み合わせにおいて実装することができる。システムの構成要素を、任意の形態または媒体のデジタルデータ通信、例えば、通信ネットワークによって相互接続することができる。通信ネットワークの例には、ローカルエリアネットワーク（「ＬＡＮ」）、広域ネットワーク（「ＷＡＮ」）、およびインターネットが含まれる。

【０１３２】

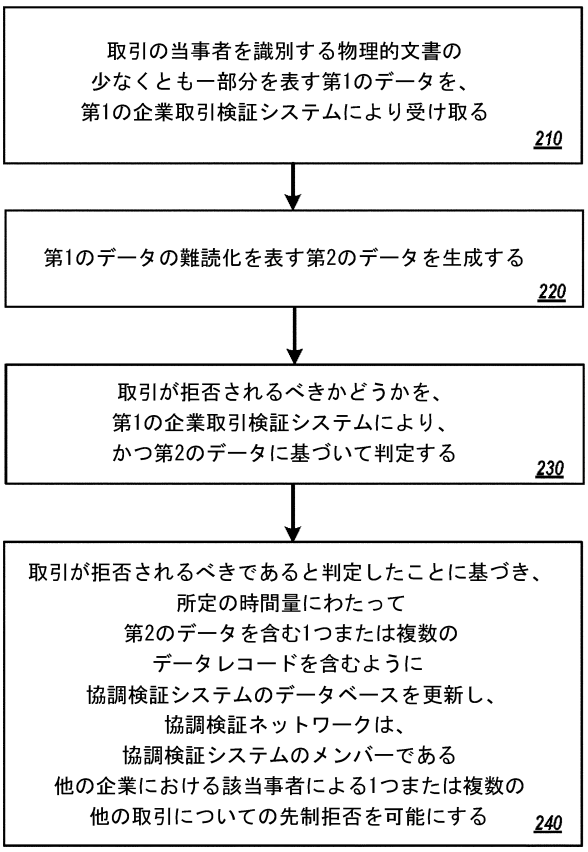
コンピューティングシステムは、クライアントとサーバとを含むことができる。クライアントとサーバとは、一般に、互いにリモートであり、通常は通信ネットワークを介して対話する。クライアントとサーバの関係は、それぞれのコンピュータ上で動作する、互いにクライアントサーバ関係を有するコンピュータプログラムによって生じる。

【図面】

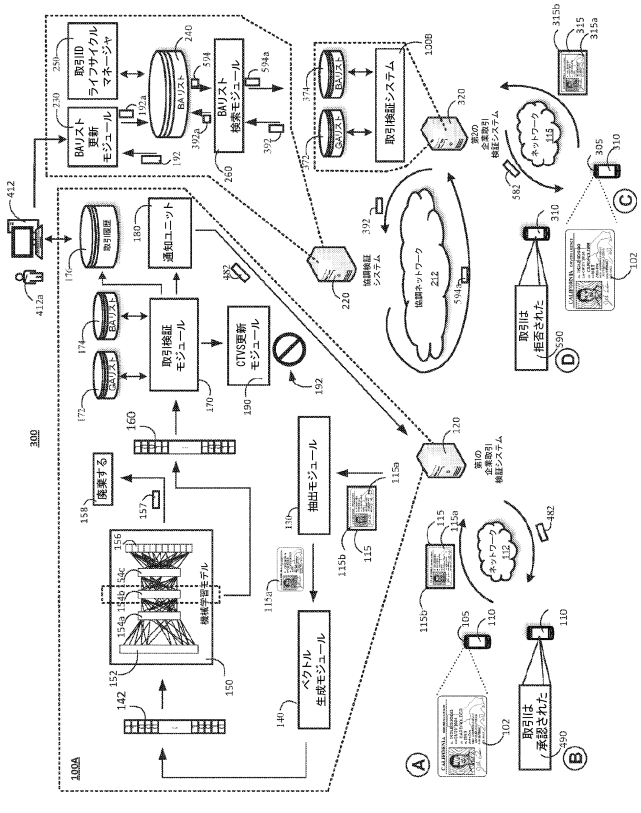
【図１】


取引ID ライフサイクル マネージャ
BAUXト 更新 モジュール
BAUXト 検索モジュール
取引検証システム
通知 ユニット
取引検証 モジュール
CTVS 更新 モジュール
抽出モジュール
ベクトル 生成モジュール
機械学習モデル
協調検証 システム
協調ネットワーク 212
ネットワーク 112
第10の企業 取引検証システム
取引は 拒否された
取引は 承認された
100
100A

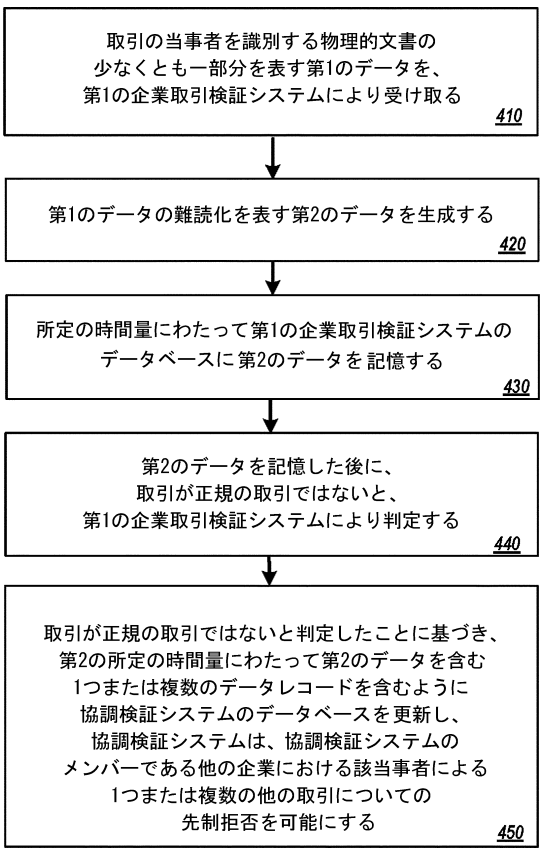
【図２】


取引の当事者を識別する物理的文書の
少なくとも一部分を表す第1のデータを、
第1の企業取引検証システムにより受け取る
210
第1のデータの難読化を表す第2のデータを生成する
220
取引が拒否されるべきかどうかを、
第1の企業取引検証システムにより、
かつ第2のデータに基づいて判定する
230
取引が拒否されるべきであると判定したことに基づき、
所定の時間量にわたって
第2のデータを含む1つまたは複数の
データレコードを含むように
協調検証システムのデータベースを更新し、
協調検証ネットワークは、
協調検証システムのメンバーである
他の企業における該当者による1つまたは複数の
他の取引についての先制拒否を可能にする
240

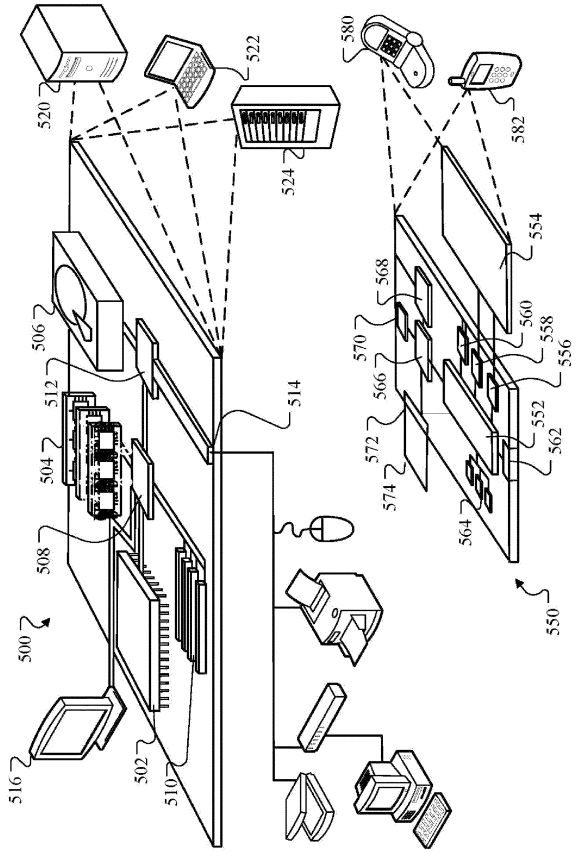
【図３】


取引ID ライフサイクル マネージャ
BAUXト 更新 モジュール
BAUXト 検索モジュール
取引検証システム
通知ユニット
取引検証 モジュール
CTVS更新 モジュール
抽出モジュール
ベクトル 生成モジュール
機械学習モデル
協調検証 システム
協調ネットワーク 212
ネットワーク 112
第10の企業 取引検証システム
取引は 拒否された
取引は 承認された
300
100A

【図４】


取引の当事者を識別する物理的文書の
少なくとも一部分を表す第1のデータを、
第1の企業取引検証システムにより受け取る
410
第1のデータの難読化を表す第2のデータを生成する
420
所定の時間量にわたって第1の企業取引検証システムの
データベースに第2のデータを記憶する
430
第2のデータを記憶した後に、
取引が正規の取引ではないと、
第1の企業取引検証システムにより判定する
440
取引が正規の取引ではないと判定したことに基づき、
第2の所定の時間量にわたって第2のデータを含む
1つまたは複数のデータレコードを含むように
協調検証システムのデータベースを更新し、
協調検証システムは、協調検証システムの
メンバーである他の企業における該当者による
1つまたは複数の他の取引についての
先制拒否を可能にする
450

【図５】


520
522
524
580
582
554
568
560
558
556
570
566
552
572
562
574
564
550
506
512
514
504
508
500
516
502
510

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 21/38551

A. CLASSIFICATION OF SUBJECT MATTER
IPC - G06Q 20/00 (2021.01)
CPC - G06Q 20/401, G06Q 20/382, G06Q 30/06, G06Q 20/04, G06Q 20/02, G06N 99/005, G06K 9/6256, G06K 9/6269, G06N 5/025, G06N 7/005, G06Q 10/10, G06Q 10/06, G06Q 30/0201, G06Q 30/02, G06Q 40/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
See Search History document

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
See Search History document

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2018/0181964 A1 (YOTI HOLDING LIMITED), 28 June 2018 (28.06.2018), entire document, especially Abstract; para [0045], [0154], [0251], [0438], [0695], [0968], [1018]	1-24
Y	US 2020/0145399 A1 (MORPHOTRUST USA, LLC), 07 May 2020 (07.05.2020), entire document, especially Abstract; para [0083], [0199], [0112], [0114], [0204], [0218]-[0219], [0308]	1-24
Y	US 10,242,283 B1 (CAPITAL ONE SERVICES, LLC), 26 March 2019 (26.03.2019), entire document, especially Abstract; col 13, ln 66 to col 14, ln 3	1-24

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 August 2021 (25.08.2021)	SEP 24 2021
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer Karl Rodriquez Telephone No. PCT Helpdesk: 571-272-4300

Form PCT/ISA/210 (second sheet) (July 2019)

フロントページの続き

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

（特許庁注：以下のものは登録商標）

１．ＱＲコード

２．ブルートゥース

３．ＷＣＤＭＡ

４．イーサネット

弁理士　佐藤 利光

(74)代理人　100188433

弁理士　梅村 幸輔

(74)代理人　100128048

弁理士　新見 浩一

(74)代理人　100129506

弁理士　小林 智彦

(74)代理人　100205707

弁理士　小寺 秀紀

(74)代理人　100114340

弁理士　大関 雅人

(74)代理人　100214396

弁理士　塩田 真紀

(74)代理人　100121072

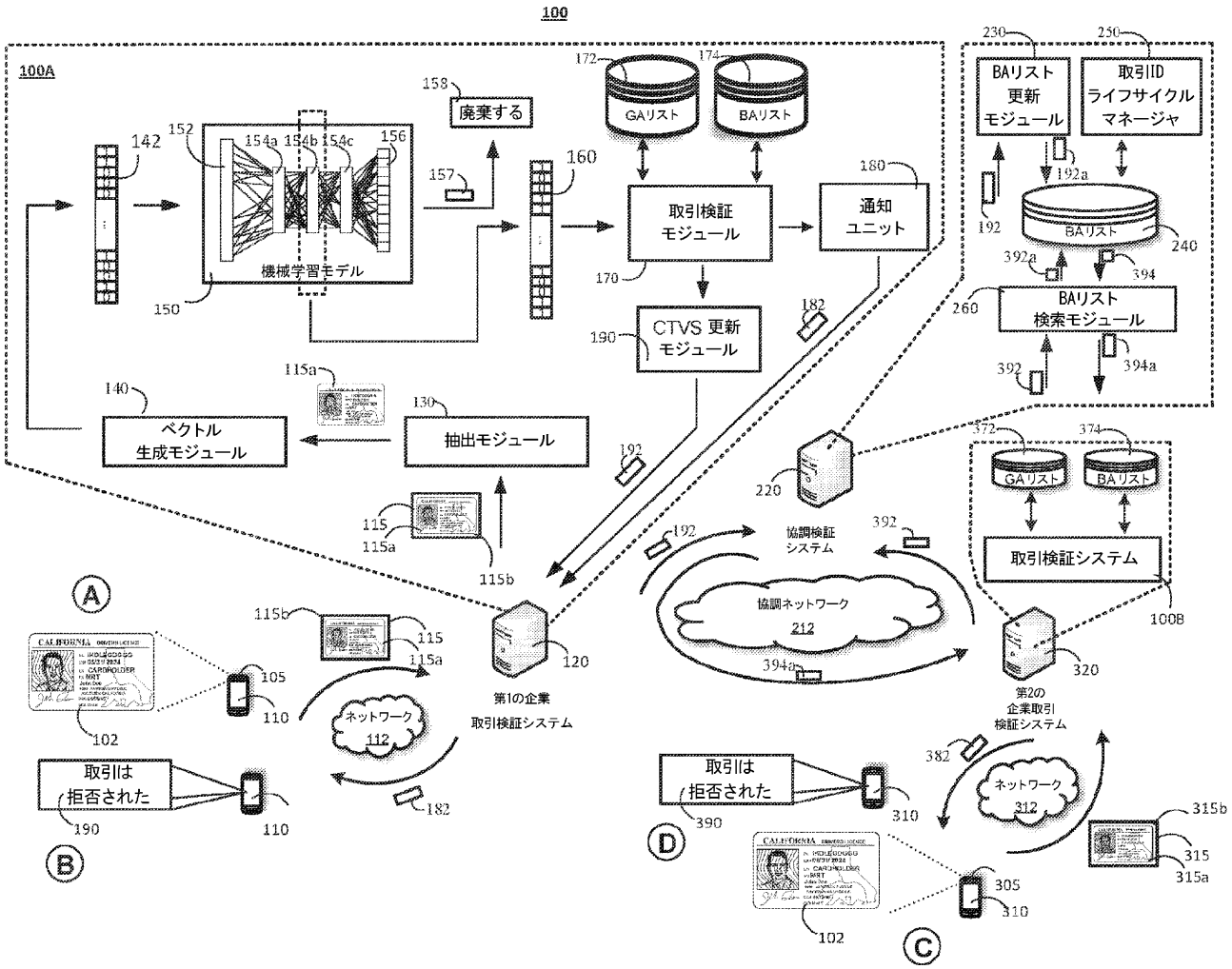
弁理士　川本 和弥

(72)発明者　フーバー ジュニア リチャード オースティン

アメリカ合衆国 ９８０３３ ワシントン州 カークランド カークランド アベニュー ８０５ スイート １０２

Ｆターム（参考）　5L049　BB00

【要約の続き】


100
100A
142
152
154a
154b
154c
156
機械学習モデル
150
158
廃棄する
157
160
172
GAリスト
174
BAリスト
取引検証
モジュール
180
通知
ユニット
170
CTVS 更新
モジュール
190
182
140
ベクトル
生成モジュール
115a
130
抽出モジュール
115
115b
192
230
BAリスト
更新
モジュール
250
取引ID
ライフサイクル
マネージャ
192a
240
392a
394
260
BAリスト
検索モジュール
392
394a
220
372
374
GAリスト
BAリスト
取引検証システム
100B
協調検証
システム
協調ネットワーク
212
394a
320
第2の
企業取引
検証システム
A
105
110
102
ネットワーク
112
第1の企業
取引検証システム
取引は
拒否された
190
B
382
310
390
D
315b
315
315a
305
C