(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6751771号
(P6751771)
(45)発行日　令和2年9月9日(2020.9.9)　(24)登録日　令和2年8月19日(2020.8.19)

(51)Int.Cl.　　F I
G06F 21/62 (2013.01)　　G06F 21/62　318
G06F 16/21 (2019.01)　　G06F 16/21

請求項の数 25　(全 32 頁)

(21)出願番号　特願2018-554013(P2018-554013)
(86)(22)出願日　平成29年4月14日(2017.4.14)
(65)公表番号　特表2019-519833(P2019-519833A)
(43)公表日　令和1年7月11日(2019.7.11)
(86)国際出願番号　PCT/US2017/027791
(87)国際公開番号　WO2017/181131
(87)国際公開日　平成29年10月19日(2017.10.19)
審査請求日　令和2年4月14日(2020.4.14)
(31)優先権主張番号　15/099,533
(32)優先日　平成28年4月14日(2016.4.14)
(33)優先権主張国・地域又は機関
米国(US)

早期審査対象出願

(73)特許権者　506332063
セールスフォース　ドット　コム　インコーポレイティッド
アメリカ合衆国　カリフォルニア州　９４１０５，サン　フランシスコ，　ミッション　ストリート　４１５，　サード　フロアー
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介

最終頁に続く

(54)【発明の名称】解析データセットのための細粒セキュリティ

(57)【特許請求の範囲】
【請求項１】
１つまたはそれ以上のセキュアな、プライマリデータベースソースから、バッチベースでデータフィールドを抽出するステップと、
前記フィールドに対してフィールドレベルセキュリティを割り当てるステップであり、
ユーザが選択可能なインヘリタンスを用いて前記フィールドの第１サブセットを特定する段階であり、前記フィールドの前記第１サブセットの各フィールドに対する前記フィールドレベルセキュリティは、少なくとも部分的に、前記１つまたはそれ以上のセキュアな、プライマリデータベースソースから抽出された前記フィールドの前記第１サブセットと関連する１つまたはそれ以上のソースフィールドから受け継ぐセキュリティに基づいて決定される、段階と、
ピン留め可能なインヘリタンスを用いて前記フィールドの第２サブセットを特定する段階であり、前記フィールドの前記第２サブセットの各フィールドに対する前記フィールドレベルセキュリティは、参照フィールドに対する前記フィールドの前記第２サブセットのためのフィールドレベルセキュリティのユーザがピン留めするインヘリタンスに少なくとも部分的に基づいて決定され、前記参照フィールドは、前記１つまたはそれ以上のセキュアな、プライマリデータベースソースにおける１つまたはそれ以上の属性にバインドされ、かつ、前記フィールドの前記第２サブセットとは異なっている、段階と、
コンパイルされたフィールドを獲得するために、前記割り当てられたフィールドレベルセキュリティを用いて前記フィールドをコンパイルする段階であり、前記コンパイルさ

れたフィールドは、グラフィカルユーザインターフェイス（ＧＵＩ）における表示のためにダッシュボードによるリアルタイムのクエリをサポートする、段階と、
を含む、ステップと、
前記コンパイルされたフィールドを１つまたはそれ以上の分析的な、読取り専用データベースに保管するステップであり、前記１つまたはそれ以上の分析的な、読取り専用データベースは、前記１つまたはそれ以上のセキュアな、プライマリデータベースソースとは異なる、ステップと、
ユーザから、クエリ結果に対するリクエストを受信するステップと、
前記ＧＵＩに表示するために、少なくとも部分的に前記割り当てられたフィールドセキュリティに基づいて、かつ、前記ユーザのフィールドセキュリティの許可を対象として、前記リアルタイムのクエリをサポートする前記コンパイルされたフィールドから前記クエリ結果を生成するステップと、
を含む、方法。
【請求項２】
前記方法は、さらに、
セキュアでないデータセットとして追加的なフィールドを受信するステップと、
前記受信した追加的なフィールドのための前記追加的なフィールドレベルセキュリティに係るユーザが選択可能な明示的なスペックを、前記１つまたはそれ以上のセキュアな、プライマリデータベースソースにおける追加的な参照フィールドに対する前記受信した追加的なフィールドのための前記追加的なフィールドレベルセキュリティに係るピン留め可能なインヘリタンスと結合することによって、前記受信したフィールドに対して追加的なフィールドレベルセキュリティを割り当てるステップであり、前記追加的な参照フィールドは、前記受信した追加的なフィールドおよび前記抽出されたフィールドとは異なる、ステップと、
を含む、請求項１に記載の方法。
【請求項３】
前記フィールドに対してフィールドレベルセキュリティを割り当てる前記ステップは、さらに、
前記フィールドレベルセキュリティに係る明示的なスペックを用いて、前記１つまたはそれ以上のセキュアな、プライマリデータベースソースからのフィールドレベルセキュリティのインヘリタンスをオーバーライドすることによって、前記フィールドレベルセキュリティを割り当てるステップ、を含む、
請求項１に記載の方法。
【請求項４】
前記リアルタイムのクエリをサポートする前記ステップは、
前記１つまたはそれ以上の分析的な、読取り専用データベースが、２０００万以上のレコードを検索し、かつ、選択されたレコードから総統計をまとめるときに、２秒以下の応答時間を実現するステップ、
を含む、請求項１に記載の方法。
【請求項５】
前記方法は、さらに、
前記１つまたはそれ以上のセキュアな、プライマリデータベースソースにおける、２つまたはそれ以上のフィールドにおけるデータから新たなフィールドを計算するステップと、
前記２つまたはそれ以上のフィールドにおけるフィールドレベルセキュリティ設定の組み合わせに基づいて、前記新たなフィールドにおけるフィールドレベルセキュリティを計算するステップと、
を含む、請求項１に記載の方法。
【請求項６】
前記方法は、さらに、

前記１つまたはそれ以上のセキュアな、プライマリデータベースソースにおける、２つまたはそれ以上のオブジェクトからのデータを結合するステップと、
前記２つまたはそれ以上のオブジェクトにおけるフィールドレベルセキュリティ設定の組み合わせに基づいて、前記結合されたデータにおいて１つまたはそれ以上のデータフィールドにおけるフィールドレベルセキュリティを計算するステップと、
を含む、請求項１に記載の方法。
【請求項７】
前記方法は、さらに、
ピン留めのための基礎として、前記１つまたはそれ以上のセキュアな、プライマリデータベースソースにおけるユーザが選択した参照フィールドをフラグ付けするステップと、
前記フラグ付けされた参照フィールドを列挙し、かつ、前記参照フィールドに対して前記フィールドの第２サブセットのピン留めをユーザができるようにする、ユーザインターフェイスを表示させるステップと、
を含む、請求項１に記載の方法。
【請求項８】
データの前記フィールドを抽出するためのスペックは、前記ユーザがフィールドレベルアクセスを有さないフィールドとして認識されたユーザ入力のストリングを含むアドバンスサーチを含み、
前記方法は、さらに、
前記認識されたストリングを認識されないものとして取り扱うステップ、を含む、
請求項１に記載の方法。
【請求項９】
前記方法は、さらに、
現在の値を更新するためのクエリの以前に、限られた時間について、前記フィールドに対する前記フィールドレベルセキュリティの現在の値をキャッシュするステップ、を含む、
請求項１に記載の方法。
【請求項１０】
１つまたはそれ以上のプロセッサおよび前記プロセッサに接続されたメモリを有する少なくとも１つのサーバを含むシステムであって、前記メモリは、コンピュータインストラクションを含み、前記プロセッサにおいて実行されると、前記システムは、
１つまたはそれ以上のセキュアな、プライマリデータベースソースから、バッチベースでデータフィールドを抽出し、
前記フィールドに対してフィールドレベルセキュリティを割り当て、前記割り当てることは、
ユーザが選択可能なインヘリタンスを用いて前記フィールドの第１サブセットを特定することであり、前記フィールドの前記第１サブセットの各フィールドに対する前記フィールドレベルセキュリティは、少なくとも部分的に、前記１つまたはそれ以上のセキュアな、プライマリデータベースソースから抽出された前記フィールドの前記第１サブセットと関連する１つまたはそれ以上のソースフィールドから受け継ぐセキュリティに基づいて決定されること、および、
ピン留め可能なインヘリタンスを用いて前記フィールドの第２サブセットを特定することであり、前記フィールドの前記第２サブセットの各フィールドに対する前記フィールドレベルセキュリティは、参照フィールドに対する前記フィールドの前記第２サブセットのためのフィールドレベルセキュリティのユーザがピン留めするインヘリタンスに少なくとも部分的に基づいて決定され、前記参照フィールドは、前記１つまたはそれ以上のセキュアな、プライマリデータベースソースにおける１つまたはそれ以上の属性にバインドされ、かつ、前記フィールドの前記第２サブセットとは異なっていること、
を含み、
コンパイルされたフィールドを獲得するために、前記割り当てられたフィールドレベル

セキュリティを用いて前記フィールドをコンパイルし、前記コンパイルされたフィールドは、グラフィカルユーザインターフェイス（ＧＵＩ）における表示のためにダッシュボードによるリアルタイムのクエリをサポートし、
前記コンパイルされたフィールドを１つまたはそれ以上の分析的な、読取り専用データベースに保管し、前記１つまたはそれ以上の分析的な、読取り専用データベースは、前記１つまたはそれ以上のセキュアな、プライマリデータベースソースとは異なっており、
ユーザから、クエリ結果に対するリクエストを受信し、
前記ＧＵＩに表示するために、少なくとも部分的に前記割り当てられたフィールドセキュリティに基づいて、かつ、前記ユーザのフィールドセキュリティの許可を対象として、前記リアルタイムのクエリをサポートする前記コンパイルされたフィールドから前記クエリ結果を生成する、
システム。
【請求項１１】
前記メモリは、さらに、コンピュータインストラクションを含み、前記プロセッサにおいて実行されると、前記システムは、
セキュアでないデータセットとして追加的なフィールドを受信し、
前記受信した追加的なフィールドのための前記追加的なフィールドレベルセキュリティに係るユーザが選択可能な明示的なスペックを、前記１つまたはそれ以上のセキュアな、プライマリデータベースソースにおける追加的な参照フィールドに対する前記受信した追加的なフィールドのための前記追加的なフィールドレベルセキュリティに係るピン留め可能なインヘリタンスと結合することによって、前記受信したフィールドに対して追加的なフィールドレベルセキュリティを割り当て、前記追加的な参照フィールドは、前記受信した追加的なフィールドおよび前記抽出されたフィールドとは異なっている、
請求項１０に記載のシステム。
【請求項１２】
前記フィールドに対してフィールドレベルセキュリティを割り当てることは、さらに、
前記フィールドレベルセキュリティに係る明示的なスペックを用いて、前記１つまたはそれ以上のセキュアな、プライマリデータベースソースからのフィールドレベルセキュリティのインヘリタンスをオーバーライドすることによって、前記フィールドレベルセキュリティを割り当てること、を含む、
請求項１０に記載のシステム。
【請求項１３】
前記１つまたはそれ以上の分析的な、読取り専用データベースが、２０００万以上のレコードを検索し、かつ、選択されたレコードから総統計をまとめるときに、２秒以下の応答時間を実現する、
請求項１０に記載のシステム。
【請求項１４】
前記メモリは、さらに、コンピュータインストラクションを含み、前記プロセッサにおいて実行されると、前記システムは、
前記１つまたはそれ以上のセキュアな、プライマリデータベースソースにおける、２つまたはそれ以上のフィールドにおけるデータから新たなフィールドを計算し、かつ、
前記２つまたはそれ以上のフィールドにおけるフィールドレベルセキュリティ設定の組み合わせに基づいて、前記新たなフィールドにおけるフィールドレベルセキュリティを計算する、
請求項１０に記載のシステム。
【請求項１５】
前記メモリは、さらに、コンピュータインストラクションを含み、前記プロセッサにおいて実行されると、前記システムは、
前記１つまたはそれ以上のセキュアな、プライマリデータベースソースにおける、２つまたはそれ以上のオブジェクトからのデータを結合し、

前記２つまたはそれ以上のオブジェクトにおけるフィールドレベルセキュリティ設定の組み合わせに基づいて、前記結合されたデータにおいて１つまたはそれ以上のデータフィールドにおけるフィールドレベルセキュリティを計算する、
請求項１０に記載のシステム。
【請求項１６】
前記メモリは、さらに、コンピュータインストラクションを含み、前記プロセッサにおいて実行されると、前記システムは、
ピン留めのための基礎として、前記１つまたはそれ以上のセキュアな、プライマリデータベースソースにおけるユーザが選択した参照フィールドをフラグ付けし、かつ、
前記フラグ付けされた参照フィールドを列挙し、かつ、前記参照フィールドに対して前記フィールドの第２サブセットのピン留めをユーザができるようにする、ユーザインターフェイスを表示させる、
請求項１０に記載のシステム。
【請求項１７】
データの前記フィールドを抽出するためのスペックは、前記ユーザがフィールドレベルアクセスを有さないフィールドとして認識されたユーザ入力のストリングを含むアドバンスサーチを含み、
前記メモリは、さらに、コンピュータインストラクションを含み、前記プロセッサにおいて実行されると、前記システムは、
前記認識されたストリングを認識されないものとして取り扱う、
請求項１０に記載のシステム。
【請求項１８】
前記メモリは、さらに、コンピュータインストラクションを含み、前記プロセッサにおいて実行されると、前記システムは、
現在の値を更新するためのクエリの以前に、限られた時間について、前記フィールドに対する前記フィールドレベルセキュリティの現在の値をキャッシュする、
請求項１０に記載のシステム。
【請求項１９】
実行可能なインストラクションを含む１つまたはそれ以上の非一時的な有形のコンピュータで読取り可能な記憶媒体であって、コンピュータ装置および１つまたはそれ以上のサーバによって実行されると、
１つまたはそれ以上のセキュアな、プライマリデータベースソースから、バッチベースでデータフィールドを抽出し、
前記フィールドに対してフィールドレベルセキュリティを割り当て、前記割り当てることは、
ユーザが選択可能なインヘリタンスを用いて前記フィールドの第１サブセットを特定することであり、前記フィールドの前記第１サブセットの各フィールドに対する前記フィールドレベルセキュリティは、少なくとも部分的に、前記１つまたはそれ以上のセキュアな、プライマリデータベースソースから抽出された前記フィールドの前記第１サブセットと関連する１つまたはそれ以上のソースフィールドから受け継ぐセキュリティに基づいて決定されること、および、
ピン留め可能なインヘリタンスを用いて前記フィールドの第２サブセットを特定することであり、前記フィールドの前記第２サブセットの各フィールドに対する前記フィールドレベルセキュリティは、参照フィールドに対する前記フィールドの前記第２サブセットのためのフィールドレベルセキュリティのユーザがピン留めするインヘリタンスに少なくとも部分的に基づいて決定され、前記参照フィールドは、前記１つまたはそれ以上のセキュアな、プライマリデータベースソースにおける１つまたはそれ以上の属性にバインドされ、かつ、前記フィールドの前記第２サブセットとは異なっていること、
を含み、
コンパイルされたフィールドを獲得するために、前記割り当てられたフィールドレベル

セキュリティを用いて前記フィールドをコンパイルし、前記コンパイルされたフィールドは、グラフィカルユーザインターフェイス（ＧＵＩ）における表示のためにダッシュボードによるリアルタイムのクエリをサポートし、
前記コンパイルされたフィールドを１つまたはそれ以上の分析的な、読取り専用データベースに保管し、前記１つまたはそれ以上の分析的な、読取り専用データベースは、前記１つまたはそれ以上のセキュアな、プライマリデータベースソースとは異なっており、
ユーザから、クエリ結果に対するリクエストを受信し、
前記ＧＵＩに表示するために、少なくとも部分的に前記割り当てられたフィールドセキュリティに基づいて、かつ、前記ユーザのフィールドセキュリティの許可を対象として、前記リアルタイムのクエリをサポートする前記コンパイルされたフィールドから前記クエリ結果を生成する、
コンピュータで読取り可能な記憶媒体。
【請求項２０】
前記インストラクションは、さらに、前記コンピュータ装置および前記１つまたはそれ以上のサーバによって実行されると、
セキュアでないデータセットとして追加的なフィールドを受信し、
前記受信した追加的なフィールドのための前記追加的なフィールドレベルセキュリティに係るユーザが選択可能な明示的なスペックを、前記１つまたはそれ以上のセキュアな、プライマリデータベースソースにおける追加的な参照フィールドに対する前記受信した追加的なフィールドのための前記追加的なフィールドレベルセキュリティに係るピン留め可能なインヘリタンスと結合することによって、前記受信したフィールドに対して追加的なフィールドレベルセキュリティを割り当て、前記追加的な参照フィールドは、前記受信した追加的なフィールドおよび前記抽出されたフィールドとは異なっている、
請求項１９に記載のコンピュータで読取り可能な記憶媒体。
【請求項２１】
前記フィールドに対してフィールドレベルセキュリティを割り当てることは、さらに、
前記フィールドレベルセキュリティに係る明示的なスペックを用いて、前記１つまたはそれ以上のセキュアな、プライマリデータベースソースからのフィールドレベルセキュリティのインヘリタンスをオーバーライドすることによって、前記フィールドレベルセキュリティを割り当てること、を含む、
請求項１９に記載のコンピュータで読取り可能な記憶媒体。
【請求項２２】
前記１つまたはそれ以上の分析的な、読取り専用データベースが、２０００万以上のレコードを検索し、かつ、選択されたレコードから総統計をまとめるときに、２秒以下の応答時間を実現する、
請求項１９に記載のコンピュータで読取り可能な記憶媒体。
【請求項２３】
前記インストラクションは、さらに、前記コンピュータ装置および前記１つまたはそれ以上のサーバによって実行されると、
前記１つまたはそれ以上のセキュアな、プライマリデータベースソースにおける、２つまたはそれ以上のフィールドにおけるデータから新たなフィールドを計算し、かつ、
前記２つまたはそれ以上のフィールドにおけるフィールドレベルセキュリティ設定の組み合わせに基づいて、前記新たなフィールドにおけるフィールドレベルセキュリティを計算する、
請求項１９に記載のコンピュータで読取り可能な記憶媒体。
【請求項２４】
前記インストラクションは、さらに、前記コンピュータ装置および前記１つまたはそれ以上のサーバによって実行されると、
前記１つまたはそれ以上のセキュアな、プライマリデータベースソースにおける、２つまたはそれ以上のオブジェクトからのデータを結合し、

前記２つまたはそれ以上のオブジェクトにおけるフィールドレベルセキュリティ設定の組み合わせに基づいて、前記結合されたデータにおいて１つまたはそれ以上のデータフィールドにおけるフィールドレベルセキュリティを計算する、
請求項１９に記載のコンピュータで読取り可能な記憶媒体。
【請求項２５】
前記インストラクションは、さらに、前記コンピュータ装置および前記１つまたはそれ以上のサーバによって実行されると、
ピン留めのための基礎として、前記１つまたはそれ以上のセキュアな、プライマリデータベースソースにおけるユーザが選択した参照フィールドをフラグ付けし、かつ、
前記フラグ付けされた参照フィールドを列挙し、かつ、前記参照フィールドに対して前記フィールドの第２サブセットのピン留めをユーザができるようにする、ユーザインターフェイスを表示させる、
請求項１９に記載のコンピュータで読取り可能な記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、超高速な、アドホックデータ探索、および、統合され、異種混合のデータセットにおけるファセットナビゲーション（faceted navigation）の技術分野に関する。
【０００２】
本特許出願は、２０１６年４月１４日付の米国特許出願第１５／０９９５３３号、タイトル”ＦＩＮＥ ＧＡＩＮ ＳＥＣＵＲＩＴＹ ＦＯＲ ＡＮＡＬＹＴＩＣ ＤＡＴＡ ＳＥＴＳ”（文書管理番号ＳＡＬＥ１１４７－１／１６９９ＵＳ）に基づく優先権を主張するものである。本関連出願は、全ての目的のためにここにおいて参照として包含されている。
【０００３】
本特許出願は、２０１４年１０月１０日付の米国特許出願第１４／５１２２３０号、タイトル”ＲＯＷ－ＬＥＶＥＬ ＳＥＣＵＲＩＴＹ ＩＮＴＥＧＲＡＴＩＯＮ ＯＦ ＡＮＡＬＹＴＩＣＡＬ ＤＡＴＡ ＳＴＯＲＥ ＷＩＴＨ ＣＬＯＵＤ ＡＲＣＨＩＴＥＣＴＵＲＥ”（文書管理番号ＳＡＬＥ１０９６－１／１４５１ＵＳ）に関連する。この特許出願において説明されるように、このような読取り専用データベースにおけるインデックス付きフィールドは、ディメンション（dimension）と呼ばれ、そして、数量フィールドはメジャー（measures）と呼ばれ得る。より詳細な説明は、関連する特許出願において見出され、優先権を主張する出願にも組み込まれているように、全ての目的のためにここにおいて参照として包含されている。
【背景技術】
【０００４】
背景技術セクションにおいて説明される技術的事項（subject matter）は、単に背景技術セクションにおいて言及した結果として先行技術であると仮定されるべきではない。同様に、背景技術セクションにおいて、または、背景技術セクションの技術的事項に関連して言及された問題は、先行技術において以前に認識されていたものと仮定されるべきではない。背景技術セクションにおける技術的事項は、単に異なるアプローチを表すに過ぎないものであり、請求される発明の実施にも対応し得るものである。
【０００５】
ビジネスでは、情報を得たビジネス上の決定を下すために、分析されている大量のデータセットについて、クエリ（query）し、かつ、クエリ結果をリアルタイムに検討する能力が必要である。分析データセット（analytics dataset）は、アドホッククエリ分析（ad-hoc query analysis）のために最適化されたフィールドの具体化された（materialized）されたコレクションを含んでいる。あらゆるクエリについて１秒以内（sub-second）のクエリ応答を可能にするためである。データセットの分野に対するセキュリティは、ビジネスにとって非常に重要である。

【０００６】
ビジネスの顧客は、いくつかのオブジェクトについて数百のカスタムデータフィールドを含む、内部コンテンツ管理システム（CRM）と、他のエンタープライズシステムを含む、外部エンティティとの両方からのデータセットに対してデータセキュリティを必要とする。CRMデータセキュリティは、セールス、サービスマーケティング、ソーシャルネットワーキングコミュニティ、分析、カスタマイズされたアプリケーション、および、モノのインターネット（Internet of Things、IoT）を含む、エンタープライズビジネスに係る多くの広範なカテゴリにおいて極めて重要である。データセキュリティは、また、外部ソースからのデータに対しても重要である。分析プラットフォーム（analytics platform）へ直接的にアップロードされたカンマ区切り値（comma separated value、CSV）ファイルを介して受信できるものである。加えて、ビジネスには、既存のデータセットを組み合わせることによって作成されたデータセットに対して効果的なデータセキュリティが必要である。

【０００７】
セキュリティ要求は、大量のデータについてビジネス分析を「ライブで（”live”）」提供するシステムのために、データと機能へのユーザクセスをコントロールし、かつ、制限する機能に対する必要性を駆り立てている。データセキュリティは、ユーザがログインできる時期、場所、方法といった組織レベルの機能（organization-level features）、各オブジェクトのレコードについてユーザが実行できるアクション（例えば、作成、読取り編集、削除）を決定するオブジェクトレベルの許可（object-level permissions）、および、デフォルト設定、共有ルール、等を通してアクセスを許可するレコードレベルの許可（record-level permissions）を含み得る。加えて、レポート、視覚化デザイン、電子メールテンプレート、および文書を含む企業の様々なデータを保護するためにフォルダ構成（folder organization）を使用することができ、フォルダアクセス（folder access）をパブリックに設定することができ、または、ロールベース（role-based）でアクセスを提供することもできる。データのフィールドレベルの許可は、１回の実施においてオブジェクトのレコードに対してユーザが閲覧および編集できるフィールドを指定する（例えば、閲覧可能かつ読取り専用を指定する）。

【０００８】
ダッシュボードとして表示される単一の視覚化レンズまたはレンズ群を介して、異なるセキュリティプロファイルを持つユーザに対して分析結果を展開することが望ましい場合には、データフィールドレベルセキュリティ（FLS）が必要とされるか、または、そうでなければ、各ユーザまたはユーザプロファイルの権限（permissions）に応じて様々なフィールド数を有するデータセットのコピーを作成する必要があるか、いずれかである。このことは、レンズのコピーを作成し、かつ、データセットを変更し、そして、次いで、ユーザがセキュリティ権限（security permissions）を持つデータセットおよびレンズに対するユーザクセスをコントロールするようにアプリケーション共有を構成するシステムを要求する。複数の同様なデータセットを作成する第２のオプションは、すぐにメンテナンスとセキュリティの問題となり、そして、著しいシステムパフォーマンスの影響を生じさせ得るものである。代替的に、フィールドレベルのセキュリティを使用する第１のオプションにより、異なるセキュリティプロファイルを持つ複数のユーザにわたり単一のレポートを共有することができ、一方で、ユーザはアクセスが許可されたデータフィールドだけを閲覧することが確保されている。

【０００９】
一つの使用例において、給与のような機密フィールドに対するアクセスは、従業員、人事（HR）管理者、および経営幹部に限定される必要があり、そして、他の全てのユーザに対して読取りアクセスを禁止する必要がある。FLSを使用して、HR管理者プロファイルを持つレポート作成者は、従業員の給与を含むレポートを作成でき、そして、レポート作成者は、HR以外の管理者がそのフィールドまたはデータを閲覧しないことの完全な保証を伴って、レポートを全てのHRユーザと確信をもって共有することができる。

【００１０】
別の使用例において、個人の健康データは、健康保険可搬性および説明責任法（Health Insurance Portability and Accountability Act、HIPAA）のプライバシールールに準拠するように保護される必要がある。この例において、患者データの重要情報閲覧者（医者および医師のアシスタントといった人）は、彼らが診断記述および処方情報を含むデータフィールドを閲覧することができることを指定するプロファイルを有している。－医療施設の事業所内の会計係は見る必要がないであろうフィールドである。
【００１１】
開示される技術は、統合された、異種混合のデータセットにおけるデータフィールドレベルのセキュリティを特定すること、および、実施することに関する。
【発明の概要】
【００１２】
例示的で非限定的な実施の様々な態様について基本的または一般的な理解を可能にするのに役立つように、ここにおいて簡略化された概要が提供される。実装形態は、より詳細な説明および添付の図面に続いている。しかしながら、この概要は、広範囲にわたるまたは包括的な概要として意図されたものではない。代わりに、この概要の唯一の目的は、以下に続く様々な実装のより詳細な説明に対する前置きとして、いくつかの例示的で非限定的な実装形態に関連するいくつかの概念を簡略化した形で提示することである。
【００１３】
開示されるシステムおよび方法は、フィールドレベルセキュリティを、バッチベース（batch basis）でプライマリソースから抽出され、かつ、分析の、読取り専用データベースの中へコンパイルされたデータフィールドに対して割り当てるために使用可能である。本方法は、抽出されたフィールドを生成するソースフィールドからのフィールドレベルセキュリティに係るユーザ選択可能なインヘリタンスを組み合わせることによって割り当てることを含み、抽出されたフィールドに対するフィールドレベルセキュリティのインヘリタンス（inheritance）をデータベースソースにおける参照フィールドに対してピン留めする（pinning）ことを伴うものであり、ここで、参照フィールドは抽出されたフィールドとは異なるものである。
【００１４】
開示される方法は、また、セキュアでないデータセットとして追加フィールドを受信すること、および、追加フィールドに対してフィールドレベルセキュリティを割り当てることも含んでいる。追加フィールドは、受信したフィールドのためのフィールドレベルセキュリティのユーザ選択可能な明示的なスペック（specification）を、受信したフィールドのためのフィールドレベルセキュリティのインヘリタンスをデータベースソースにおける参照フィールドにピン留めすることと結合することによって受信されるものである。
【００１５】
開示される技術の他の態様および利点は、以降の図面、詳細な説明、および請求項を検討することによって理解することができる。
【図面の簡単な説明】
【００１６】
添付される図面は、説明目的のものであり、そして、この開示に係る１つまたはそれ以上の実装形態のための可能な構造およびプロセスオペレーションの実施例を提供するためだけに役立つものである。これらの図面は、この開示の精神および範囲から逸脱することなく、当業者によってなされ得る形態および詳細におけるいかなる変更も決して限定するものではない。技術的事項のより完全な理解は、以下の図面と併せて考慮するときに、詳細な説明および請求項を参照することによって導き出すことができる。ここで、図面の全体を通じて同様な参照番号は同様な要素を示している。
【図１】図１は、フィールドレベルセキュリティを伴う一つの例示的なビジネス情報および分析アーキテクチャ環境を示している。
【図２】図２は、一つの分析クラウド環境のためのデータソースの例についてブロック図

を示している。
【図３】図３は、２つの結合され、かつ、変換されたデータセットの組み合わせについて一つの例示的なフィールドレベルセキュリティ属性を示している。
【図４】図４は、リモート要求（remote request）のために交換されたメッセージを伴う一つの例示的なブロック図を示している。
【図５】図５は、複数のレンズを用いたダッシュボードの一つの例を示している（従来技術）。
【図６】図６は、セキュアなデータベースからのデータのフィールドに対してデータのセキュリティを実装するためのフローについて一つの概要を示している。
【図７】図７は、分析データセットについて細粒セキュリティを実施することができる一つの例示的なマルチテナントコンピュータ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】
【００１７】
以下の詳細な説明は、図面を参照して行われる。実施例は、開示される技術を、その範囲を限定することなく説明するために記載されるものであり、特許請求の範囲は請求項によって規定される。当業者であれば、以下の説明について様々な均等な変形を認識するだろう。
【００１８】
洞察データ分析（insight data analysis）は、データ視覚化（data visualizations）に係るデータ探索、ダッシュボード構築、および宣言的表現（declarative representation）をサポートしている。探索およびリプレイ探索の最中には、データフィルタリング、グループ化、およびプレゼンテーションフォーマットにおける変更がアニメーション化され、変更がデータ値をどのように再配分するかを示している。単独で又は組み合わせにおいて、これらの機能は、データ分析およびプレゼンテーションの成功に貢献することができる。
【００１９】
単一パネルのデータ探索およびリプレイの最中には、新しいデータの視覚化がそれらがデザインされるようにアニメーション化される。データセグメントについてドリルダウン（drill down）することは、例えば、元のデータセグメントを選択された再グループ化に従って細分化させ、そして、アニメーション化された細分化の成長および再構成を通じて、より細かい（granular）データの視覚化へと視覚的に進歩させる。このことは、分析者が、データを理解し、そして、続いて、プロセス並びに数字に興味がある同僚に対して重要なデータセグメントを説明するのに役立つ。
【００２０】
分析データセットについて細粒セキュリティ（fine grain security）のための開示される方法は、異なるセキュリティプロファイルを持つユーザ間で共有されるべきデータをレポートする単一のダッシュボードの使用をサポートし、一方で、ユーザは彼らがアクセスを許可されたフィールドだけを閲覧することを確保している。
【００２１】
開示される実装形態に従ったシステム、装置、および方法の例は、「販売機会（”sales opportunity”）」のコンテクストにおいて説明されている。リード（leads）、見込み（prospects）、およびアカウント（accounts）といった、販売コンタクト（sales contacts）の例は、コンテクストを追加し、かつ、開示される実装形態の理解を援助するためだけに使用されている。他のインスタンスにおいて、多数の要素を伴うデータは、医療システム診断および検査結果、保険請求、カスタマーサービスコールルーティング、等、または、かなりの数の特徴を有するであろう任意のデータを含んでよい。他のアプリケーションも可能であるので、以下の例は、範囲、コンテクスト、または設定のいずれにおいても最終的または限定的なものとして理解されるべきではない。当業者には、従って、「販売機会」のコンテクストの中または外側で実施が行われ得ることが、明らかであろう。
【００２２】

フィールドレベルセキュリティ環境

図１は、フィールドレベルセキュリティ環境100における分析データセットについて細粒セキュリティを実施するための一つの環境を示しており、分析読取り専用データストア（data store）102、セキュアなCRMデータストア104、外部データストア142、および、マルチテナントCRMコンピューティングサービス106を含んでいる。マルチテナントCRMコンピューティングサービス106における、FLSフィルタ116は、フィールドレベルセキュリティロールおよびクエリ要求者の権限に基づいて、大きなデータセットをフィルタする。

【００２３】

分析読取り専用データストア102は、読取り専用データセットを含んでいる。分析される大量のデータセットについて、探索し、かつ、リアルタイムで探索結果を閲覧するために使用可能な、複数のユーザのフィールドレベルセキュリティ属性を有するものである。セキュアなCRMデータストア104は、一つの例において、マルチテナントCRMコンピューティングサービス106からバッチベースで抽出されたデータセットを含んでいる。抽出されたフィールドに対するフィールドレベルセキュリティは、抽出されたフィールドを生成するソースフィールドからのフィールドレベルセキュリティに係るユーザ選択可能なインヘリタンスを組み合わせることによって割り当てることができる。抽出されたフィールドに対するフィールドレベルセキュリティのインヘリタンスをデータベースソースにおける参照フィールドに対してピン留めすることを伴うものであり、ここで、参照フィールドは抽出されたフィールドとは異なるものである。大規模なデータリポジトリから取得された（抽出された）データは、関連するフィールドレベルセキュリティと共に、分析読取り専用データストア102へとコンパイルすることができ、そして、「生の（”raw”）」データセットを作成するために使用することができる、－分析のための読取り専用データ構造であり、増大、変換、平坦化、等がなされ、かつ、ビジネスエンティティのための顧客が視認可能（customer-visible）なデータセットとして発行され得るものである。

【００２４】

外部データストア142は、企業のコンテンツ管理システムの一部ではないソースからのデータを含み得る。外部システムの例は、これらに限定されるわけではないが、SAP™、ORACLE E-BUSINESS™、PEOPLESOFT™、NETSUITE™、およびWORKDAY™を含んでいる。このデータには、顧客の購入履歴、人口統計学的特性（demographics）、関係性、およびプリファレンスを含み得る。一つの例において、データは、スプレッドシート形式で提供される、競合他社についての販売クオータ（quotas）を表すコンマ区切り値（CSV）として表現することができる。フィールドレベルセキュリティは、スプレッドシートのデータ表現の中に含まれ得るものであり、または、管理者によりユーザ選択可能なものであり得る。外部データストア142は、また、外部ソースから受信したデータも含み得るものであり、そのフィールドレベルセキュリティは、フィールドに対するフィールドレベルセキュリティに係るユーザ選択可能な明示的なスペックを組み合わせることによって、追加的に受信されたフィールドに対して割り当てられる。データは、他の形式においても受信され得る、－これらに限定されるわけではないが、その他のデリミタ区切り（delimiter-separated）フォーマット、ビットマップ画像、異なるタイプのマルチメディアのためのOggフォーマットコンテナ、および、独占的（proprietary）なファイルフォーマットを含んでいる。

【００２５】

図１に示される環境は、異種混合（heterogeneous）のデータソース及び関連する探索を取り扱う分析サーバ162、および、複数のソースからのフィールドレベルセキュリティメタデータを管理するための内部FLSエンジン156を伴う分析FLSエンジン146、－承継され、ピン留めされ、かつ、ユーザ選択可能なFLSを含んでいるもの、を有する。加えて、ネットワーク145は、ここにおいて説明されるデータストア、サーバ、およびエンジン間で通信するものである。

【００２６】

環境においては、また、GUIクライアントエンジン166も示されている。ライブビジネス

分析レンズとダッシュボードを鑑賞するため、および、「ライブ（”live”）」分析データのニュアンス（nuances）を探索するために新規かつ更新されたクエリ要求を受け入れるためのレンズおよびダッシュボードビルダ178を伴う視覚化ディスプレイエンジン176を含むものである。これらの要求は、サービスのために分析サーバ162に対してルート（routed）され得る。レンズおよびダッシュボードビルダ178は、ダッシュボードをデザインして、リアルタイムなデータ探索結果として複数のレンズを表示している。つまり、アナリストは、複数のクエリ結果のセットのための表示チャートを単一のダッシュボード上に配置することができる。グローバルフィルタへの変更がダッシュボード上の任意の表示チャートに影響を与える場合、ダッシュボード上の残りの表示チャートは、変更を反映するために更新される。正確なライブクエリー結果が、クエリ結果を要求しているユーザのフィールドレベルセキュリティ権限に従って、ダッシュボード上のディスプレイレンズのセットにわたり生成され、かつ、表示される。GUIクライアントエンジン166は、－モバイルアプリケーション165またはユーザコンピューティングデバイス164のユーザについて、分析クエリ要求および分析サーバ162への応答のフローを管理する。

【００２７】

所望のセキュリティプロファイル属性を有するフィールドを有する参照テーブルを作成することができ、そして、分析テーブルにおけるフィールドを参照テーブルにおけるフィールドに対してピン留めすることができる。つまり、フィールドに対するフィールドレベルセキュリティは、データストアにおいて既存の列（columns）と属性にバインドして、テーブルにおける参照フィールドから継承（inherit）することができる。

【００２８】

GUIクライアントエンジン166は、また、分析読取り専用データストア102におけるフィールドに対してセキュリティメタデータオプションを選択し、かつ、構成するための管理者により使用可能であるユーザ選択可能なFLSインターフェイス186も含んでいる。

【００２９】

マルチテナントCRMコンピューティングサービス106は、ワークステーション、サーバ、コンピューティングクラスタ、ブレードサーバ、サーバファーム、または、あらゆる他のデータ処理システムまたはコンピューティングデバイスを含む、様々なタイプのものであり得る。そして、ネットワーク145は、相互に通信するデバイスの任意のネットワークまたはネットワークの組み合わせであり得る。例えば、マルチテナントCRMコンピューティングサービス106は、LAN（ローカルエリアネットワーク）、WAN（ワイドエリアネットワーク）、電話ネットワーク（公衆交換電話網（PSTN）、セッションイニシエーションプロトコル（SIP）、3G、4G　LTE）、無線ネットワーク、ポイントツーポイントネットワーク、スターネットワーク、トークンリングネットワーク、ハブネットワーク、WiMAX、Wi-Fi、ブルートゥース（登録商標）のようなピアツーピア接続、近距離無線通信（NFC）、Z-Wave、ZigBee、または、インターネットを含む、データネットワークの他の適切な構成、のうち１つ又は任意の組み合わせを使用して実施され得る。他の実装形態においては、イントラネット、エクストラネット、仮想プライベートネットワーク（VPN）、非TCP/IPベースのネットワーク、任意のLANまたはWAN等といった、他のネットワークが使用され得る。

【００３０】

分析読取り専用データストア102、セキュアなCRMデータストア104、外部データストア142、および、マルチテナントCRMコンピューティングサービス106は、汎用分散メモリキャッシュシステムを使用して実施され得る。いくつかの実装形態において、データ構造は、１つまたはそれ以上のテナントからの情報を共通データベースイメージのテーブルの中へ保管することができ、オンデマンドデータベースサービス（ODDS）を形成する。マルチテナントデータベースシステム（MTDS）といった、多くの方法で実施され得るものである。データベースイメージは、１つまたはそれ以上のデータベースオブジェクトを含み得る。他の実装形態において、データベースは、リレーショナルデータベース管理システム（RDBMS）、オブジェクト指向データベース管理システム（OODBMS）、分散ファイルシステム

（DFS）、スキーマなし（no-schema）データベース、または、あらゆる他のデータ記憶システム又はコンピューティングデバイス、であり得る。分析読取り専用データベースでは、２０００万件を超えるレコードを検索し、かつ、選択されたレコードから集計統計をコンパイルするときに、２秒未満の応答時間を実施することができる。

【００３１】

いくつかの実装形態において、ユーザコンピューティングデバイス164は、パーソナルコンピュータ、ラップトップコンピュータ、タブレットコンピュータ、スマートフォンまたは他のモバイルコンピューティングデバイス、パーソナルデジタルアシスタント（PDA）、デジタルイメージキャプチャデバイス、等であり得る。いくつかの実装形態において、ユーザモバイルデバイス165は、タブレットコンピュータ、スマートフォンまたは他のモバイルコンピューティングデバイス、パーソナルデジタルアシスタント（PDA）、デジタルイメージキャプチャデバイス、等であり得る。

【００３２】

視覚化ディスプレイエンジン176およびユーザ選択可能なFLSインターフェイス186は、ブラウザにおいて又はアプリケーションとして動作している、多数の形態のうち１つをとることができる。ユーザインターフェイス、ダッシュボードインターフェイス、エンゲージメントコンソール、および、モバイルインターフェイス、タブレットインターフェイス、サマリインターフェイス、またはウェアラブルインターフェイスといった、他のインターフェイスを含んでいるものである。いくつかの実装形態においては、オンプレミス（on-premise）環境におけるWebベースまたはクラウドベースのサーバ上でホストされ得る。一つの実装形態において、視覚化ディスプレイエンジン176およびユーザ選択可能なFLSインターフェイス186は、コンピューティングデバイス上で動作しているブラウザからアクセスされ得る。ブラウザは、CHROME™、INTERNET EXPLORER™、FIREFOX™、SAFARI™、OPERA™、等であり得る。他の実装形態において、視覚化ディスプレイエンジン176およびユーザ選択可能なFLSインターフェイス186は、コンピュータデスクトップアプリケーション上のエンゲージメントコンソール（engagement console）として動作し得る。

【００３３】

他の実装形態において、フィールドレベルセキュリティ環境100は、上記に列挙されたものと同じ要素またはコンポーネントを有さなくてよく、かつ／あるいは、上記に列挙されたものの代わりに、または、加えて、Webサーバおよびテンプレートデータベースといった要素またはコンポーネントを有してよい。異なる要素またはコンポーネントを単一のソフトウェアモジュールへと組み合わせることができ、そして、複数のソフトウェアモジュールを同じハードウェア上で実行することができる。データセキュリティは、一つのシステムについてデータフローにおける複数のレベルにおいて考慮される。次に、一つの実施例が説明される。

【００３４】

図２は、データフロー図の一つの例を示しており、これらに限定されるわけではないが、CRMデータ242および外部データ292を含んでいる。分析クラウド245について、アプリケーション254は、CRMデータ242および外部データ292からのデータを組み込むデータセット264を含んでいる。データセット264は、レンズ265として示される（rendered）。ダッシュボード266は、ユーザ268に対してCRMデータ242および外部データ292に基づく分析を配信するために、複数のレンズ265を表示することができる。

【００３５】

一つのユースケース（use case）において、企業のための管理者は、会社のCRMデータ242へのアクセスをコントロールする。データセット所有者は、データセット264に係るレコードに対するアクセスをコントロールする。アプリケーションの所有者、管理者、および十分な許可を有するユーザ（例えば、アプリケーションに対するアクセスを認められたマネージャ）は、アプリケーションの中のデータセット264、レンズ265、およびダッシュボード266に対するアクセスをコントロールする。フィールドレベルセキュリティを介して細粒セキュリティを提供するための開示される方法は、ユーザ268は、彼らが許可を有

するデータだけを見ることを確保することができる。構築時にCRMリレーショナルデータベースから切り離された抽出データセットに対してセキュリティを適合させることができる。

【００３６】

セキュリティは、また、異なるインフラストラクチャおよびセキュリティモデルの下で動作している、外部ソースから抽出され、そして、抽出されたCRMデータと組み合されたデータを取り扱うように適合させることもできる。一つの例示的なユースケースにおいて、大企業は、競合するボート（boat）ブランドについて月毎にボートのセールスを調査しており、一方で、調査データがチーフインテリジェンスオフィサ（CIO）であるシニアITリーダー、マーケティングリーダー、およびサプライチェーンリーダーを対象とするデータ統合企業から引き出された最近のローン（load）を分析していてよい。つまり、複数の外部ソースからの異種混合のデータを、彼らのプロファイルが必要とされるフィールドレベルセキュリティをカバーするユーザのために、ダッシュボード上に含めることができる。

【００３７】

いくつかのユースケースについては、複数のデータセットが結合され、かつ、変換されることを必要とし、そして、データが結合された２つまたはそれ以上のオブジェクトにおけるフィールドレベルのセキュリティ設定の組み合わせに基づいて、結果フィールド（resultant field）についてフィールドレベルセキュリティを計算することができる。

【００３８】

以下の検討は、ビジネスの難局を明らかにすることができる「ライブ（”live”）」データ分析の配信を促進するためのデータセットの結合および変換の使用の動機を与える。様々なタイプのオンデマンドトランザクションデータ管理システムを分析データストアと統合することができ、データアナリストに対してトランザクションデータ管理システムを検索するためのアドホックを提供する。このことは、数値、メトリック、および測定値を使用する分析アプリケーションの迅速な構築を促進することができ、トランザクションデータ管理システムに保管されたトランザクションデータからビジネスインテリジェンス（business intelligence）を推進し、かつ、組織の意思決定を支援する。トランザクションデータは、組織のオペレーションをサポートするデータオブジェクトを参照するものであり、そして、営業、サービス、銀行業務、受注管理、製造、医療記録、購買、課金、等といった、異なる分野における主要なビジネスプロセスを自動化するアプリケーションシステムの中に含まれている。トランザクションデータのいくつかの例は、企業データ（例えば、注文入力、サプライチェーン、出荷、請求書）、販売データ（口座、リード、機会）、医療データ（診断、処方箋、請求）、等を含んでいる。

【００３９】

抽出（extraction）は、一つの実装形態に従って、トランザクションデータストアからトランザクションデータを取得するタスクを参照するものである。このことは、データベースまたはスプレッドシートからフラットファイルをダウンロードするのと同様に単純であってよく、または、外部システムとの関係をセットアップし、次いで、ターゲットシステムに対するデータの転送をコントロールするのと同様に複雑なものであってよい。ロード（loading）は、キャプチャされたデータが、ウェアハウスまたはマート（mart）といった、新しいデータストアの中に置かれるフェイズである。いくつかの実装形態において、ロードは、構造化照会言語（SQL）におけるIMPORTおよびOracleユーティリティにおけるLOADといった、カスタムプログラミングコマンドによって遂行される。いくつかの実装形態においては、複数のアプリケーションプログラミングインターフェイス（API）を使用することができ、トランザクションデータを専用のデータストアの中へロードする抽出コネクタと一緒に、複数のトランザクションデータソースとインターフェイスする。

【００４０】

変換（transformation）は、抽出またはロードされたデータに対して一連のルールまたはファンクションを適用する段階（stage）を参照し、一般的に、抽出またはロードされ

たデータを、分析を導き出すのに役立つフォーマットに変換するためのものである。変換のいくつかの実施例は、ロードする所定の列だけの選択、コード値の変換、フリーフォーム値の符号化、新たな計算値の導出、ソート、複数ソースからのデータの結合、集計、非正規化、データの転置またはピボット（pivoting）、一つの列の複数列への分離、および、データの検証、を含んでいる。

【００４１】

一つの実装形態において、補強変換（augment transformation）は、２つのデータセットからのデータを結合して、それら両方にわたる検索をできるようにする。例えば、「ユーザデータセット（”user dataset”）」を「アカウントデータセット（”account dataset”）」を用いて補強することにより、データアナリストは、アカウントの所有者と作成者の名前を含む、全てのアカウントの詳細を表示するクエリを生成することができる。補強変換は、２つの入力データセットからのデータに基づいて新たなデータセットを作成する。各入力データセットは、左または右のデータセットとして識別され得る。新たなデータセットは、左データセットの全ての列を含み、かつ、右データセットからは指定された列だけが追加されている。補強変換は、左の、外部結合を実行し、ここで、新たな結合は、左データセットから全ての行（rows）と、右データセットから一致した行だけを含んでいる。別の実装形態において、２つ以上のデータセットに及ぶクエリを可能にすることができる。このことは、一度に２つのデータセットを補強することによって達成することができる。例えば、３つのデータセットを補強するためには、最初の２つのデータセットを補強してから、結果として生じるデータセットを第３のデータセットを用いて補強することができる。

【００４２】

いくつかの実装形態においては、補強変換の結合条件を指定することができ、右データセットにおける行を左データセットにおけるものと一致させる方法を決定する。以下の実施例は、単一列の結合条件を示している。単一列のキーに基づいて以下のデータセットを補強するために、「オポチュニティ（”Opportunity”）」が左データセットとして割り当てられ、そして、「アカウント（”Account”）」が右データセットとして割り当てられる。また、”OpptyAcct”が、それらの間の関係として指定される。

オポチュニティデータセット（”Opportunity dataset”）	アカウントデータセット（”Account dataset”）
ID	*ID
Opportunity_Name	Account_Name
Amount	Annual_Revenue
Stage	Billing_Address
Closed_Date	
*Account_ID	

【００４３】

全てのアカウント列に対して”OpptyAcct”プリフィクスが追加され、そして、データセットが”Opportunity.Account_ID = Account.ID”として定義されたキーに基づいて結合される。２つの入力データセットを補強した後で、結果として得られるデータセット

は、以下の列を含んでいる。

オポチュニティーアカウントエッジマート（”Opportunity-Account　EdgeMart”）
ID
Opportunity_Name
Amount
Stage
Closed_Date
Account_ID
OpptyAcct.Account_Name
OpptyAcct.Annual_Revenue
OpptyAcct.Billing_Address

【００４４】
他の実装形態においては、異なる重量級の変換（heavy-weight　transformation）を適用することができる。アカウント上でロールベースのアクセスを作成するためのフラット化変換、データセットにおいて一次元列をインデックス付けするためのインデックス変換、データセットにおいてデータに基づいて大文字小文字を区別するフルテキストインデックスを生成するエヌグラム（Ngram）変換、クエリに利用できるようにするためにデータセットを登録する登録変換、および、データオブジェクトのフィールドからデータを抽出する抽出変換を、を含むものである。
【００４５】
いくつかの実装形態においては、分析データセットのための細粒セキュリティは、プライマリデータベースソースにおける２つまたはそれ以上のオブジェクトからのデータを結合すること、および、２つまたはそれ以上のオブジェクトにおけるフィールドレベルセキュリティ設定の組み合わせに基づいて、結合されたデータにおける１つまたはそれ以上のフィールドのフィールドレベルセキュリティを計算すること、を含んでいる。
【００４６】
図３は、２つのオブジェクトの結合に係る一つの例示的な実装形態300を示している。補強エンジン345は、２つのオブジェクト、データセットＡ　324とデータセットＢ　328、を結合することができる。いくつかの実装形態において、新たなフィールドは、プライマリデータベースソースにおける２つまたはそれ以上のフィールドのデータから計算することができ、そして、その２つまたはそれ以上のオブジェクトにおけるフィールドレベルセキュリティ設定の組み合わせに基づいて、新たなフィールドの中のフィールドレベルセキュリティを計算している。
【００４７】
変換エンジン355は、結合の結果を変更することができる。一つの実装形態において、結合および変換後の、結果として生じるフィールドに対するフィールドレベルセキュリテ

ィは、データセットＡ　324およびデータセットＢ　328のフィールドレベルセキュリティ設定に基づいている。結果データセット365は、フィールドXを含み、派生フィールド（derived　field）を構成するフィールドのセキュリティ344、346を集めることによって設定されたセキュリティレベルを伴っている。一つの実施例において、フィールドAは列１に依存するFLSを有し、フィールドBは列２に依存するFLSを有し、そして、フィールドCはフィールドAおよびフィールドBから派生し－両方に依存し、かつ、両方に縛られ、列１と列２の両方に依存する、フィールド視認性（field　visibility）を伴うものである。実施例を続けると、管理者は、このデフォルト設定をオーバーライド（override）するように許可され得るものであり、フィールドC　FLSを列１に対して、または列２に対して、もしくは、完全に異なる列（列３）に対して手動で結合することができる。列のリスト（１、２、または「その他（”other”）」を表示することは、フィールドCについて我々が有する系統情報（lineage　information）に基づくものであろう。

【００４８】

オーバーライドオプションは、集計統計（aggregate　statistics）が根底にある詳細よりも広く分散されている場合に有用である。ロールアップ（roll-ups）は、それらがまとめるフィールドのセキュリティ制限を継承することができないだろう。フィールドに対する特別な派生セキュリティ（derived　security）は、JOINオペレーションから生成できる。計算されたフィールドに対する特別な派生セキュリティは、コンポーネントのうち１つよりもセキュリティに相当するものであり得る。

【００４９】

図４における一つの例示的なブロック図は、ユーザのためにフィールドレベルセキュリティ要求をカスタマイズした一つの実装形態を表示しており、－環境における機能ブロック間での要求と応答を示している。GUIクライアントエンジン166は、要求を送信する（例えば、レンズのリスト、データセットのリスト、外部データに対するリモートクエリ）。要求を受信すると、分析サーバ162は、新しいクエリが必要であるか否かを判断する。そして、必要である場合に、マルチテナントCRMコンピューティングサービス106に対してリモートリクエスト424を送信する。分析FLSエンジン146における内部FLSエンジン156に対して要求を送信するものであり、－要求しているユーザ（requesting　user）に対するFLS要求434のリクエストである。ユーザのための複合FLS444がFLSフィルタ116に戻される場合には、次いで、FLSフィルタされた（FLS-filtered）応答454が生成され、そして、GUIクライアントエンジン166を介してユーザに対してクエリ結果を表示するために機能する分析サーバ162に対して送信される。

【００５０】

いくつかの実装形態について、クエリにおけるフィールドに対してFLSを指定することができる。一つのユースケースにおいて、分析サーバ要求は、興味のオブジェクトを含み、そうしたオブジェクトのフィールド系統と一緒である。分析サーバは、認可されたFLSに基づいて、要求しているユーザについて許可されるフィールドを含むオブジェクトを用いて応答することができる。クエリとレスポンスは、属性値（attribute-value）のペアから成るデータオブジェクトを送信するJSONまたは別のフォーマットを使用して配信され得る。フィールド系列の一つの例は、以下のように表すことができる。

```
”field3.relation1.relation2.field”
        ”<entity1>”：［
                ”<field1>”、
                ”<field2>”、
                ”<field3.relation1.relation2.field>”
、
                ・・・］
        ”<entity2>”：［
                ”<field1>”、
                ”<field2>”、
```

”<field3.relation1.relation2.field>”
、
・・・]

【００５１】
ユーザが選択可能なFLSインターフェイス186は、抽出されたフィールドについてフィールドレベルセキュリティを明示的に指定するために、管理者のためのスクリーンインターフェイスを提供することができる。指定されたFLSは、管理者によって、抽出されたフィールドについてフィールドレベルセキュリティのインヘリタンスをオーバーライドすることができる。

【００５２】
ユーザが必要なフィールドレベルセキュリティプロファイルを有さないフィールドを求める（call for）、レンズまたは複数のレンズのダッシュボード、をユーザが要求する場合に、GUIは、その要求は完了できないことをユーザに対して伝えるメッセージを配信することができる。いくつかの実装形態について、レンズをレンダリングするために必要な任意のフィールドがユーザによって視認できない場合、レンズは供給されず、そして、「レンズは見ることができない（”lens not visible”）」と伝えるUIを表示することができる。この結果は、利用可能なレンズのリストの表示をユーザが要求している場合、そして、また、レンズクエリを実行するようにユーザが要求した場合にも起こり得るものである。同様に、ユーザがセキュリティ権限を欠く１つまたはそれ以上のレンズをユーザが有する場合に、ダッシュボードは、いくつかの実装形態において、レンズを隠すことができ、そして、他の事例においてはレンズがユーザから隠されていることを伝えるメッセージを表示することができる。

【００５３】
いくつかのユースケースにおいては、ユーザが要求されるFLSプロファイルを欠いている場合に、ユーザがセキュリティ権限を欠くフィールドをプロジェクトのために利用可能なフィールドから取り除くことができ、そして、実行可能なクエリを作成するためにフィールドのサブセットを使用するこができる。このシナリオにおいては、視覚化の成功が制限され得る。

【００５４】
別の実装形態においては、分析サーバ162に対するFLSフィルタされた応答の中にユーザのクエリを完了するために必要とされるフィールドのリストを含めることができ、そして、許容可能なフィールドのリターンリストに基づいてレンズおよびダッシュボードに対するクエリをフィルタすることができる。分析サーバ162は、保管されている視覚化、すなわちレンズおよびダッシュボード、におけるクエリを満足するために必要とされるフィールドを検査することができる。GUI166に対して提供されるレンズおよびダッシュボードのリストは、次いで、分析サーバ162によってフィルタすることができる。このことは、エラーを起こし、かつ、「レンズは見ることができない」メッセージの表示を生じさせるレンズおよびダッシュボードを、ユーザが閲覧しようとする試みを防止する。上級ユーザが、フィールドレベルセキュリティのアクセスを有さないフィールド名をタイプ入力しようと試みる状況について、システムはフィールド名の認識に応答（acknowledge）しない。開示される技術は、ユーザがフィールドレベルアクセスを有さないフィールドとして認識されるユーザ入力ストリングを含む高度な検索を含むデータフィールドを抽出すること、および、その認識されたストリングを認識されないものとして取り扱うことのためのスペックを含んでいる。

【００５５】
図５（従来技術）は、複数のレンズを伴うダッシュボードの一つの実施例として示されている。この視覚化において、ダッシュボードを閲覧しているユーザは、「アカウント名（”Account Name”）」フィールドに対するアクセスを許可されていない。ダッシュボードは、このフィールドに依存する２つのウィジェットを含んでいる。右端のフィルタセレクター「アカウントセレクタ（”account selector”）」525および右下の円グラフ56

8である。２つの表示オプションは、これら２つのコンポーネントをフィルタしてダッシュボードから取り除くこと、または、ダッシュボードをレンダリングして、これらの２つのレンズの代わりにエラーメッセージを表示することである。第３の選択肢として、ユーザがダッシュボードを閲覧することを全く防止することができる。

【００５６】

いくつかの実装形態においては、データセットが作成され、かつ、キャッシュされ、そして、ユーザのセッションは、そのセッションのデータセットが作成されたときに存在したFLS情報を使用することができる。このユースケースについては、ユーザがセッションを開始したときに有しているフィールドレベルセキュリティの制限が、セッション全体を通じて継続される。

【００５７】

セキュリティ分析のための抽出／構築サイクル間で生じるFLSの変化に応答するために、多数のオプションが利用可能である。キャッシュ時間がゼロ、つまりキャッシングが全く無いときは、セキュリティのドリフト（drift）が無く、完全なセキュリティの忠実度（security fidelity）が達成される。いくつかの実装形態において、分析読取り専用データベースにおけるフィールドに対するフィールドレベルセキュリティの現在値のキャッシュは、現在の値に対するアップデートをクエリする以前の、５－１０分のうちの限られた時間について有効である。

【００５８】

システムフロー

図６は、分析データセットについて細粒セキュリティを実施している一つの実装形態に係るフローチャート600を示している。フローチャート600は、例えば、情報を受信または検索し、情報を処理し、結果を保管し、かつ、結果を送信するように構成された１つまたはそれ以上のプロセッサによって、少なくとも部分的にデータベースシステムを用いて実施され得る。他の実装形態は、異なる順序で、かつ／あるいは、図６に示されるものとは異なる、より少ないか又は追加のステップを用いて、ステップを実行することができる。以下に説明される動作は、より多くのステップへと細分され、または、より少ないステップへと組み合わされ、説明される本方法を異なるステップの数量または配置を使用して実行することができる。

【００５９】

動作610において、FLSエンジン116は、セキュアな（secured）プライマリデータベースソースからデータのフィールドをバッチベースで抽出する。

【００６０】

動作620において、分析FLSエンジン146は、フィールドを分析読取り専用データストア102へとコンパイルする。

【００６１】

動作630において、内部FLSエンジン156は、抽出されたフィールドに対してフィールドレベルセキュリティを割り当て、そして、複数のソースからのフィールドレベルセキュリティメタデーター継承され（inherited）、ピン留めされ、かつ、ユーザ選択されたFLSを含むもの、を管理することができる。

【００６２】

動作640において、分析FLSエンジン146は、抽出されたフィールドを生成するソースフィールドからのフィールドレベルセキュリティのユーザ選択可能なインヘリタンスを組み合わせる。抽出されたフィールドに対するフィールドレベルセキュリティのインヘリタンスをデータベースソースにおける参照フィールドにピン留めすることを用いるものである。

【００６３】

マルチテナント統合

図７は、図１のフィールドレベルセキュリティ環境100との統合に適した一つの例示的なマルチテナントシステム700のブロック図を示している。一般的に、図７で示されるマ

ルチテナントシステム700は、複数のテナント間で共有される共通データベース732からのデータ722に基づいて、仮想アプリケーション716および718を動的に作成し、かつ、サポートするサーバ704を含む。共通データベースは、代替的に、ここにおいては「マルチテナントデータベース（”multi-tenant database”）」として参照されるものである。GUIクライアントを含む、仮想アプリケーション716および718によって生成されるデータおよびサービスは、ネットワーク745を介して、任意の数のクライアントデバイス748または758に対して、必要に応じて提供される。

【００６４】

ここにおいて使用されるように、「テナント（”tenant”）」または「組織（”organization”）」は、マルチテナントデータベース732の中でデータの共通サブセットに対するアクセスを共有する一人またはそれ以上のユーザのグループを参照するものである。この点に関して、各テナントは、それぞれのテナントに対して、関連付けられ、割り当てられ、または、そうでなければ所属している、一人またはそれ以上のユーザを含んでいる。別の言葉で言えば、マルチテナントシステム700の中の各ユーザそれぞれが、マルチテナントシステム700によってサポートされる複数のテナントのうち特定のテナントに対して、関連付けられ、割り当てられ、または、そうでなければ所属している。テナントは、ユーザ、ユーザの部署、業務または法律上の組織、及び／又は、マルチテナントシステム700の中でユーザの特定のセットについてデータを維持するあらゆる他のエンティティ、を表してよい。複数のテナントがサーバ704およびデータベース732に対するアクセスを共有することができるが、各テナントに対してサーバ704から提供される特定のデータおよびサービスは、他のテナントに対して提供されるものからセキュアに隔離することができる。マルチテナントアーキテクチャにより、従って、ユーザの異なるセットは、他のテナントに属しているか、または、そうでなければ関連付けられている任意のデータ722を必ずしも共有することなく、機能性およびハードウェアリソースを共有することができる。

【００６５】

マルチテナントデータベース732は、任意の数のテナントと関連するデータ722を保管し、かつ、管理することができる、あらゆる種類のリポジトリ（repository）または他のデータストレージシステムである。データベース732は、あらゆるタイプの従来のデータベースサーバハードウェアを使用して実施することができる。様々な実装形態において、データベース732は、処理（processing）ハードウェアをサーバ704と共有している。他の実装形態において、データベース732は、ここにおいて説明される様々な機能を実行するためにサーバ704と通信する別個の物理的及び／又は仮想データベースサーバのハードウェアを使用して実施される。マルチテナントデータベース732は、ここにおいては、代替的にオンデマンドデータベースとして参照されてよい。この点で、マルチテナントデータベース732は、アプリケーションプラットフォーム717、セキュアに分離されたテナント１のメタデータ712およびテナント２のメタデータ714を伴うもの、によって生成されるオンデマンド仮想アプリケーション716または718に対して、実行時に（at run-time）データを提供する（または、提供するように利用可能である）。

【００６６】

実際に、データ722は、アプリケーションプラットフォーム717をサポートするために任意的な方法でオーガナイズされ、かつ、フォーマットされてよい。様々な実装形態において、従来のデータ関連性は、インデックス付け、一意性、エンティティ間の関係性、及び／又は、必要に応じて従来のデータベース構成の他の態様を確立する任意の数のピボットテーブル713を使用して確立される。

【００６７】

サーバ704は、仮想アプリケーションを生成するための動的アプリケーションプラットフォーム717を集合的に提供する、１つまたはそれ以上の現実及び／又は仮想コンピューティングシステムを使用して実施される。例えば、サーバ704は、相互に関連して動作している現実及び／又は仮想サーバのクラスタを使用して実施することができ、典型的には、従来のネットワーク通信、クラスタ管理、ロードバランシング、および、必要に応じて

他の機能に関連している。サーバ704は、プロセッサ736、メモリ738、入力／出力機能734、等といった、あらゆる種類の従来の処理ハードウェアを用いて動作する。入力／出力734は、一般的に、ネットワーク（例えば、ネットワーク745、または、他のローカルエリア、ワイドエリア、もしくは他のネットワーク）、マスストレージ、ディスプレイ装置、データ入力装置、及び／又は、同様のものに対するインターフェイスを表す。ユーザインターフェイス入力装置734は、キーボード、マウス、トラックボール、タッチパッド、またはグラフィックタブレットといったポインティングデバイス、スキャナ、ディスプレイに組み込まれているタッチスクリーン、音声認識システムとマイクロホンといった音声入力装置、および、他のタイプの入力装置を含む。一般的に、用語「入力装置（”input device”）」の使用は、コンピュータシステム717の中へ情報を入力する可能なタイプの装置および方法を含むように意図されている。

【００６８】

ユーザインターフェイス出力装置は、ディスプレイサブシステム、プリンタ、ファックス装置、または、オーディオ出力装置といった非視覚的ディスプレイを含み得る。ディスプレイサブシステムは、ブラウン管（CRT）、液晶ディスプレイ（LCD）といったフラットパネル装置、プロジェクション装置、または、可視画像を作成するためのいくらかの他のメカニズムを含み得る。ディスプレイサブシステムは、また、オーディオ出力装置といった非視覚的ディスプレイを提供することもできる。一般的に、用語「出力装置（”output device”）」の使用は、プロセッサ736からユーザ、もしくは、別のマシンまたはコンピュータシステムに対して情報を出力するための全ての可能なタイプの装置および方法を含むように意図されている。

【００６９】

プロセッサ736は、任意の適切な処理システムを使用して実装され得る。１つまたはそれ以上のプロセッサ、コントローラ、マイクロプロセッサ、マイクロコントローラ、処理コア、及び／又は、任意の数の分散または統合されたシステムにわたり広がっている他のコンピューティングリソース、任意の数の「クラウドベース（”cloud-based”）」または他の仮想システムを含んでいるもの、といったものである。メモリ738は、プロセッサ736上における実行のためのプログラミングインストラクションを保管することができる任意の非一時的な短期または長期のストレージ、または、他のコンピュータで読取り可能な媒体を表しており、あらゆる種類のランダムアクセスメモリ（RAM）、読取り専用メモリ（ROM）、フラッシュメモリ、磁気または光学マスストレージ、及び／又は、同様なものを含んでいる。コンピュータで実行可能なプログラミングインストラクションは、サーバ704及び／又はプロセッサ736によって読み取られ、かつ、実行されるときに、サーバ704及び／又はプロセッサ736に、アプリケーションプラットフォーム717及び／又は仮想アプリケーション716および718を作成させ、生成させ、または、そうでなければ促進させ、そして、ここにおいて説明される１つまたはそれ以上の追加的なタスク、オペレーション、ファンクション、及び／又は、プロセスを実行させる。メモリ738は、そうしたコンピュータで読取り可能な媒体の一つの適切な実装形態を表しており、そして、代替的または追加的に、サーバ704は、例えば、ポータブルハードドライブ、USBフラッシュドライブ、光ディスク、等の、ポータブルまたはモバイルコンポーネント、もしくはアプリケーションプラットフォームとして実現される外部のコンピュータで読取り可能な媒体を受け取り、かつ、協業し得ることに留意すべきである。

【００７０】

アプリケーションプラットフォーム717は、クライアントデバイス748および758に対してデータ及び／又はサービスを提供する仮想アプリケーション716および718を生成する、あらゆる種類のソフトウェアアプリケーションまたは他のデータ処理エンジンである。典型的な実装形態において、アプリケーションプラットフォーム717は、あらゆる種類の従来的又は専有的なオペレーティングシステム728を使用して、処理ハードウェアの処理リソース、通信インターフェイス、および他の機能に対するアクセスを獲得する。仮想アプリケーション716および718は、典型的には、クライアントデバイス748および758から受信

した入力に応じて実行時に生成される。

【００７１】

引き続き図７を参照すると、サーバ704によって提供されるデータおよびサービスは、ネットワーク745上におけるあらゆる種類のパーソナルコンピュータ、携帯電話、タブレット、または、他のネットワーク対応クライアントデバイス748または758を使用して取り出すことができる。一つの例示的な実装形態において、クライアントデバイス748または758は、マルチテナントデータベース732から取り出されたデータ及び／又は情報をグラフィカルに表示することができる、モニタ、スクリーン、または、別の従来的な電子ディスプレイといった、ディスプレイ装置を含んでいる。

【００７２】

いくつかの実装形態において、ネットワーク745は、ローカルエリアネットワーク（LAN）、ワイドエリアネットワーク（WAN）、WiMAX、Wi-Fi、電話ネットワーク、無線ネットワーク、ポイントツーポイントネットワーク、スターネットワーク、トークンリングネットワーク、ハブネットワーク、メッシュネットワーク、ブルートゥース（登録商標）、近距離通信（NFC）、Z-Wave、ZigBeeのようなピアツーピア接続、または、インターネットを含む、データネットワークの他の適切なコンフィグレーションのうち任意の一つまたは任意の組み合わせであり得る。

【００７３】

前述の説明は、本質的に単なる例示であり、そして、技術的事項またはアプリケーションの実装、または、そうした実装の使用を限定するように意図されたものではない。さらに、技術分野、背景、または詳細な説明において提示された任意の表現され、又は、暗示された理論によって拘束される意図は存在しない。ここにおいて使用されるように、用語「例示的（”exemplary”）」は、「一つの例、インスタンス、または説明として機能する」ことを意味するものである。ここにおいて例示的として記載されたあらゆる実装形態は、必ずしも他の実装形態よりも好ましく又は有利であるとして解釈されるべきものではなく、そして、ここにおいて記載される例示的な実装形態は、どのようにしても技術的事項の範囲または適用可能性を限定するように意図されたものではない。

【００７４】

開示される技術は、データベースシステム、マルチテナント環境、またはリレーショナルデータベース実装を含む、任意のコンピュータ実装システムのコンテクストにおいて実施することができる。ORACLE^{TM}互換データベース実装、IBM DB2 Enterprise Server互換リレーショナルデータベース実装、MySQL又はPostgreSQL互換リレーショナルデータベース実装、またはMicrosoft SQL Server互換リレーショナルデータベース実装、またはVampire^{TM}互換非リレーショナルデータベース実装といったNoSQL非リレーショナルデータベース実装、Apache Cassandra^{TM}互換非リレーショナルデータベース実装、BigTable互換非リレーショナルデータベース実装、もしくはHBase又はDynamoDB互換非リレーショナルデータベース実装、等である。

【００７５】

さらに、開示される技術は、相互に協働し、かつ、通信する２つまたはそれ以上の別個の異なるコンピュータ実装システムを使用して実装することができる。開示される技術は、多数の方法で実装することができる。方法は、プロセス、方法、装置、システム、デバイス、コンピュータで読取り可能なインストラクションまたはコンピュータプログラムコードを保管するコンピュータで読取り可能な記憶媒体といったコンピュータで読取り可能な媒体として、もしくは、中に組み込まれたコンピュータで読取り可能なプログラムコードを有するコンピュータで使用可能な媒体を含むコンピュータプログラム製品としてのものを含んでいる。

【００７６】

特定の実装形態

一つの実装形態において、開示される方法は、セキュアな、プライマリデータベースソースからバッチベースでデータフィールドを抽出すること、そして、フィールドを分析的

な、読取り専用データベースの中へコンパイルすること、および、抽出されたフィールドに対するフィールドレベルセキュリティをデータベースソースにおける参照フィールドに対してピン留めすることを伴い、抽出されたフィールドを生成するソースフィールドからのフィールドレベルセキュリティのユーザ選択可能なインヘリタンスを組み合わせることによって、抽出されたフィールドに対してフィールドレベルセキュリティを割り当てること、を含む。ここで、参照フィールドは、抽出されたフィールドとは異なるものである。開示される方法は、さらに、セキュアでないデータセットとして追加的なフィールドを受信すること、および、受信したフィールドに対するフィールドレベルセキュリティをデータベースソースにおける参照フィールドに対してピン留めすることを伴い、受信したフィールドに対するフィールドレベルセキュリティのユーザ選択可能な明示的スペックを結合することによって受信された、追加的なフィールドに対してフィールドレベルセキュリティを割り当てること、を含む。ここで、参照フィールドは、抽出されたフィールドとは異なるものである。

【００７７】

開示される技術に係るこの方法および他の実装形態は、開示される追加的な方法に関連して説明される以下の特徴及び／又は複数の特徴のうちの１つまたはそれ以上を含み得る。簡潔のために、この出願において開示される特徴の組み合わせは、個々には列挙されず、そして、特徴の各基本セットと伴に繰り返されない。読者は、このセクションにおいて特定される特徴が、実装形態として特定される基本の特徴セットとどのように容易に組み合わされ得るのか理解するだろう。

【００７８】

いくつかの実装形態において、フィールドレベルセキュリティのユーザ選択可能な割り当ては、さらに、フィールドレベルセキュリティの明示的なスペックを用いて抽出されたフィールドからのフィールドレベルセキュリティのインヘリタンスをオーバーライドすることによって、フィールドレベルセキュリティを割り当てること、を含む。

【００７９】

分析的な、読取り専用データベースのための開示される方法の実施は、２０００万以上のレコードを検索し、かつ、選択されたレコードから総統計をまとめるときに、２秒以下の応答時間を実現する、

【００８０】

いくつかの実装形態について、分析データセットのための細粒セキュリティに係る開示される方法は、プライマリデータベースソースにおける２つまたはそれ以上のオブジェクトからのデータを結合すること、および、２つまたはそれ以上のオブジェクトにおけるフィールドレベルセキュリティ設定の組み合わせに基づいて、結合されたデータにおける１つまたはそれ以上のフィールドのフィールドレベルセキュリティを計算すること、を含む。

【００８１】

さらに他の実装形態において、本方法は、ピン留めのための基礎（basis）として、データベースソースにおけるユーザが選択した（user-selected）参照フィールドをフラグ付けすること、および、フラグ付けされた参照フィールドを列挙し、かつ、参照フィールドに対して抽出されたフィールドのピン留めをユーザができるようにする、ユーザインターフェイスの表示を行わせること、を含み得る。

【００８２】

開示される方法の実装形態は、さらに、ユーザがフィールドレベルアクセスを有さないフィールドとして認識されるユーザ入力ストリングを含む高度な検索を含むデータのフィールドを抽出すること、および、その認識されたストリングを認識されないものとして取り扱うことのためのスペックを含む。

【００８３】

開示される方法のいくつかの実装形態について、要求されるレンズが、フィールドレベルセキュリティ許可をユーザが有さないフィールドを使用する場合に、レンズは表示され

ない。いくつかの場合には、レンズは利用可能ではないというメッセージがディスプレイに表示される。ユーザが利用可能でないフィールドを求めるダッシュボードの取り扱いは、ユーザがフィールドレベルセキュリティ許可を有するダッシュボードのためのレンズのサブセットおよび残りのレンズが閲覧のために利用可能ではないことを伝えるメッセージを含み得る。ユーザが利用可能でないフィールドを求めるストリングによって指定される高度なクエリを含む実装形態においては、要求しているユーザがセキュリティ許可を有さない保護データは表示されない。

【００８４】

さらに他の実装形態について、分析読取り専用データベースにおけるフィールドに対するユーザ権限のキャッシュは、限られた時間についてのものである。これらに限定されるわけではないが、ユーザ権限を更新する以前の、２－６分、３－８分、または４－１０分のうち一つを含んでいる。

【００８５】

開示される方法は、さらに、現在の値に対するアップデートをクエリする以前に、分析読取り専用データベースにおけるフィールドに対するフィールドレベルセキュリティの現在値を３－８分の限られた時間についてキャッシュすることを含み得る。他の実装形態において、本方法は、現在の値に対するアップデートをクエリする以前に、分析読取り専用データベースにおけるフィールドに対するフィールドレベルセキュリティの現在値を４－９分の限られた時間についてキャッシュすることを含み得る。もしくは、現在の値に対するアップデートをクエリする以前に、分析読取り専用データベースにおけるフィールドに対するフィールドレベルセキュリティの現在値を５－１０分の限られた時間についてキャッシュすることを含み得る。

【００８６】

他の実装形態は、インストラクションが刻まれた非一時的で有形なコンピュータで読取り可能な媒体を含み得る。インストラクションは、コンピュータデバイスおよび１つまたはそれ以上のサーバ上で実行されたときに、上記のプロセスのうち任意のものを実行する。

【００８７】

さらに別の実装形態は、１つまたはそれ以上のプロセッサ、および、プロセッサに接続されたメモリを有する少なくとも１つのサーバを含むコンピューティングシステムを含んでよく、プロセッサ上で実行されたとき、コンピューティングシステムに上記のプロセスのうち任意のものを実行させるコンピュータインストラクションを含んでいる。

【００８８】

開示される技術は、上に詳述された好ましい実装形態および実施例を参照して開示されているが、これらの実施例は、限定する意味ではなく、むしろ例示的であると意図されていることが理解されるべきである。当業者であれば、変更および組み合わせが容易になされることが期待される。変更および組み合わせは、本発明の精神および以降の請求項の範囲内のものである。

【００８９】

クローズ（Clauses）

１．セキュアな読取り専用データベースを構築するためのシステムが開示される。本システムは、

少なくとも１つのプライマリデータベースソースから、ディメンションおよびメジャーを含むデータフィールドをバッチで抽出するための抽出手段と、

抽出されたデータフィールドの中のディメンションに対する不変のインデックスを用いて、少なくとも１つの読取り専用データベースの中へ抽出されたデータフィールドをコンパイルするためのコンパイル手段と、

複数のコンパイルされたデータフィールドに対してデータフィールドレベルセキュリティのアクセスを割り当てるためのセキュリティ割り当て手段であり、セキュリティ手段は、セキュリティのインヘリタンスとセキュリティのピン留めとの間の選択のための選択手

段を含む、手段と、を含み、ここで、
セキュリティのインヘリタンスの選択により、セキュリティ割り当て手段は、プライマリデータベースソースにおいて抽出されたフィールドから、コンパイルされたデータフィールドに対して、インヘリタンスによってデータフィールドレベルセキュリティを割り当て、かつ、
セキュリティのピン留めの選択により、セキュリティ割り当て手段は、コンパイルされたデータフィールドに対する参照フィールドから、コンパイルされたデータフィールドに対するピン留めされた参照フィールドからのデータフィールドレベルセキュリティのインヘリタンスを用いて、セキュリティのピン留めによってデータフィールドレベルセキュリティを割り当て、
参照フィールドは、抽出されたフィールドとは異なるものであり、
読取り専用データベースの構築の最中に、割り当てられたデータフィールドレベルセキュリティをコンパイルされたデータフィールドと整合させるための構築手段と、
を含んでいる。
【００９０】
２．本システムは、さらに、
データフィールドレベルセキュリティの対象とならないセキュアでないデータセットから、さらに、追加的なデータフィールドを抽出するための抽出手段と、
明示的なセキュリティとセキュリティのピン留めとの間のさらなる選択のための選択手段を用いて、追加的なデータフィールドに対してフィールドレベルセキュリティをさらに割り当てるためのセキュリティ割り当て手段と、を含み、ここで、
明示的なセキュリティの選択により、セキュリティ割り当て手段は、追加的なデータフィールドについてフィールドレベルセキュリティの明示的なスペックによってデータフィールドレベルセキュリティを割り当て、かつ、
セキュリティのピン留めの選択により、セキュリティ割り当て手段は、コンパイルされたデータフィールドに対する参照テーブルにおける参照フィールドから、追加的なデータフィールドに対するピン留めされた参照フィールドからのデータフィールドレベルセキュリティのインヘリタンスを用いて、セキュリティのピン留めによってデータフィールドレベルセキュリティを割り当てる、
クローズ１に係るシステム。
【００９１】
３．選択手段は、さらに、明示的なセキュリティ間の選択を行い、かつ、
明示的なセキュリティの選択により、セキュリティ割り当て手段は、追加的なデータフィールドについてフィールドレベルセキュリティの明示的なスペックによってデータフィールドレベルセキュリティを割り当てる、
クローズ２に係るシステム。
【００９２】
４．２０００万以上のレコードを検索し、かつ、選択されたレコードから総統計をまとめるときに、読取り専用データベースは、２秒以下の応答時間を実現する、
クローズ１乃至３のいずれか一つに係るシステム。
【００９３】
５．本システムは、さらに、
プライマリデータベースソースにおいて２つまたはそれ以上のデータフィールドにおけるデータから新たなデータフィールドを計算するための新たなフィールド手段、を含み、かつ、
セキュリティ割り当て手段は、２つまたはそれ以上のデータフィールドにおけるデータフィールドレベルセキュリティ設定の組み合わせに基づいて、さらに、新たなデータフィールドにおけるデータフィールドレベルセキュリティを計算する、
クローズ１乃至４のいずれか一つに係るシステム。
【００９４】

６．本システムは、さらに、
プライマリデータベースソースにおける２つまたはそれ以上のオブジェクトからのデータを結合するためのオブジェクト結合手段、を含み、かつ、
セキュリティ割り当て手段は、２つまたはそれ以上のオブジェクトにおけるデータフィールドレベルセキュリティ設定の組み合わせに基づいて、さらに、結合されたデータにおいて１つまたはそれ以上のデータフィールドにおけるデータフィールドレベルセキュリティを計算する、
クローズ１乃至５のいずれか一つに係るシステム。
【００９５】
７．選択手段は、さらに、
プライマリデータベースソースにおけるデータフィールドのうち少なくとも１つをセキュリティのピン留めのための参照フィールドとしてフラグ付けを行い、かつ、
フラグ付けされた参照フィールドを列挙し、かつ、参照フィールドに対して抽出されたフィールドに係るセキュリティのピン留めをユーザが選択できるようにする、ユーザインターフェイスの表示を行う、
クローズ１乃至６のいずれか一つに係るシステム。
【００９６】
８．読取り専用データベースをセキュアにする方法が、さらに開示される。本方法は、
少なくとも１つのプライマリデータベースソースから、ディメンションおよびメジャーを含むデータフィールドを抽出するステップと、
抽出されたデータフィールドの中のディメンションに対する不変のインデックスを用いて、少なくとも１つの読取り専用データベースの中へ抽出されたデータフィールドをコンパイルするステップと、
セキュリティのインヘリタンスとセキュリティのピン留めとの間の選択を伴って、複数のコンパイルされたデータフィールドに対してデータフィールドレベルセキュリティのアクセスを割り当てるステップであり、ここで、
セキュリティのインヘリタンスの選択により、プライマリデータベースソースにおいて抽出されたフィールドから、コンパイルされたデータフィールドに対して、インヘリタンスによってデータフィールドレベルセキュリティを割り当て、かつ、
セキュリティのピン留めの選択により、コンパイルされたデータフィールドに対する参照フィールドから、コンパイルされたデータフィールドに対するピン留めされた参照フィールドからのデータフィールドレベルセキュリティのインヘリタンスを用いて、セキュリティのピン留めによってデータフィールドレベルセキュリティを割り当て、
参照フィールドは、抽出されたフィールドとは異なるものである、ステップと、
読取り専用データベースの構築の最中に、割り当てられたデータフィールドレベルセキュリティをコンパイルされたデータフィールドと整合させるステップと、
を含んでいる。
【００９７】
９．本方法は、さらに、
データフィールドレベルセキュリティの対象とならない少なくとも１つのセキュアでないデータセットから追加的なデータフィールドを抽出するステップと、
明示的なセキュリティとセキュリティのピン留めとの間のさらなる選択のために、追加的なデータフィールドに対してフィールドレベルセキュリティを割り当てるステップと、を含み、ここで、
明示的なセキュリティの選択により、追加的なデータフィールドについてフィールドレベルセキュリティの明示的なスペックによってデータフィールドレベルセキュリティを割り当て、かつ、
セキュリティのピン留めの選択により、コンパイルされたデータフィールドに対する参照テーブルにおける参照フィールドから、追加的なデータフィールドに対するピン留めされた参照フィールドからのデータフィールドレベルセキュリティのインヘリタンスを用

いて、セキュリティのピン留めによってデータフィールドレベルセキュリティを割り当てる、
クローズ８に係る方法。
【００９８】
１０．本方法は、さらに、明示的なセキュリティ間の選択を行うステップを含み、かつ、
明示的なセキュリティの選択により、追加的なデータフィールドについてフィールドレベルセキュリティの明示的なスペックによってデータフィールドレベルセキュリティを割り当てる、
クローズ９に係る方法。
【００９９】
１１．本方法は、さらに、
プライマリデータベースソースにおいて２つまたはそれ以上のデータフィールドにおけるデータから新たなデータフィールドを計算するステップと、
２つまたはそれ以上のデータフィールドにおけるデータフィールドレベルセキュリティ設定の組み合わせに基づいて、新たなデータフィールドにおけるデータフィールドレベルセキュリティを計算するステップと、含む、
クローズ８乃至１０のいずれか一つに係る方法。
【０１００】
１２．本方法は、さらに、
プライマリデータベースソースにおける２つまたはそれ以上のオブジェクトからのデータを結合するステップと、
２つまたはそれ以上のオブジェクトにおけるデータフィールドレベルセキュリティ設定の組み合わせに基づいて、結合されたデータにおいて１つまたはそれ以上のデータフィールドにおけるデータフィールドレベルセキュリティを計算するステップと、を含む、
クローズ８乃至１１のいずれか一つに係る方法。
【０１０１】
１３．本方法は、さらに、
プライマリデータベースソースにおけるデータフィールドのうち少なくとも１つをセキュリティのピン留めのための参照フィールドとしてフラグ付けするステップ、を含み、かつ、
フラグ付けされた参照フィールドを列挙し、かつ、参照フィールドに対して抽出されたフィールドに係るセキュリティのピン留めをユーザが選択できるようにする、ユーザインターフェイスの表示を行う、
クローズ８乃至１２のいずれか一つに係る方法。
【０１０２】
１４．読取り専用データベースをセキュアにするためのコンピュータプログラムインストラクションが刻まれた非一時的なコンピュータで読取り可能な記憶媒体であって、インストラクションがプロセッサ上で実行されると、
少なくとも１つのプライマリデータベースソースから、ディメンションおよびメジャーを含むデータフィールドをバッチで抽出するステップと、
抽出されたデータフィールドの中のディメンションに対する不変のインデックスを用いて、少なくとも１つの読取り専用データベースの中へ抽出されたデータフィールドをコンパイルするステップと、
セキュリティのインヘリタンスとセキュリティのピン留めとの間の選択を伴って、複数のコンパイルされたデータフィールドに対してデータフィールドレベルセキュリティのアクセスを割り当てるステップであり、ここで、
セキュリティのインヘリタンスの選択により、プライマリデータベースソースにおいて抽出されたフィールドから、コンパイルされたデータフィールドに対して、インヘリタンスによってデータフィールドレベルセキュリティを割り当て、かつ、
セキュリティのピン留めの選択により、コンパイルされたデータフィールドに対する

参照フィールドから、コンパイルされたデータフィールドに対するピン留めされた参照フィールドからのデータフィールドレベルセキュリティのインヘリタンスを用いて、セキュリティのピン留めによってデータフィールドレベルセキュリティを割り当て、
参照フィールドは、抽出されたフィールドとは異なるものである、ステップと、
読取り専用データベースの構築の最中に、割り当てられたデータフィールドレベルセキュリティをコンパイルされたデータフィールドと整合させるステップと、
を含む、方法を実行する。

【０１０３】

１５．上記方法は、さらに、
データフィールドレベルセキュリティの対象とならないセキュアでないデータセットから追加的なデータフィールドを抽出するステップと、
明示的なセキュリティとセキュリティのピン留めとの間のさらなる選択のために、追加的なデータフィールドに対してフィールドレベルセキュリティを割り当てるステップと、を含み、ここで、
明示的なセキュリティの選択により、追加的なデータフィールドについてフィールドレベルセキュリティの明示的なスペックによってデータフィールドレベルセキュリティを割り当て、かつ、
セキュリティのピン留めの選択により、コンパイルされたデータフィールドに対する参照テーブルにおける参照フィールドから、追加的なデータフィールドに対するピン留めされた参照フィールドからのデータフィールドレベルセキュリティのインヘリタンスを用いて、セキュリティのピン留めによってデータフィールドレベルセキュリティを割り当てる、
クローズ１４に係る非一時的なコンピュータで読取り可能な記憶媒体。

【０１０４】

１６．上記方法は、さらに、明示的なセキュリティ間の選択を選択するステップを含み、かつ、
明示的なセキュリティの選択により、追加的なデータフィールドについてフィールドレベルセキュリティの明示的なスペックによってデータフィールドレベルセキュリティを割り当てる、
クローズ１５に係る非一時的なコンピュータで読取り可能な記憶媒体。

【０１０５】

１７．上記方法は、さらに、
プライマリデータベースソースにおいて２つまたはそれ以上のデータフィールドにおけるデータから新たなデータフィールドを計算するステップと、
２つまたはそれ以上のデータフィールドにおけるデータフィールドレベルセキュリティ設定の組み合わせに基づいて、新たなデータフィールドにおけるデータフィールドレベルセキュリティを計算するステップと、含む、
クローズ１４乃至１６のいずれか一つに係る非一時的なコンピュータで読取り可能な記憶媒体。

【０１０６】

１８．上記方法は、さらに、
プライマリデータベースソースにおける２つまたはそれ以上のオブジェクトからのデータを結合するステップと、
２つまたはそれ以上のオブジェクトにおけるデータフィールドレベルセキュリティ設定の組み合わせに基づいて、結合されたデータにおいて１つまたはそれ以上のデータフィールドにおけるデータフィールドレベルセキュリティを計算するステップと、を含む、
クローズ１４乃至１７のいずれか一つに係る非一時的なコンピュータで読取り可能な記憶媒体。

【０１０７】

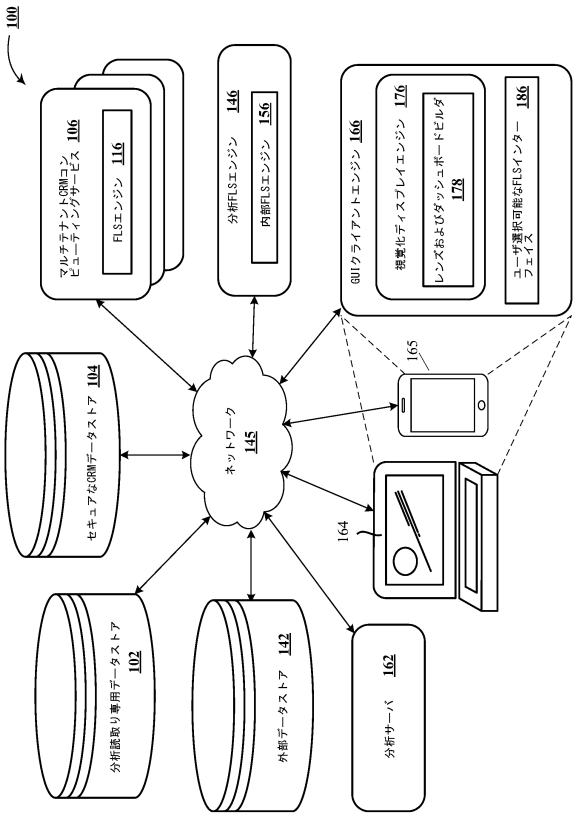
１９．上記方法は、さらに、

プライマリデータベースソースにおけるデータフィールドのうち少なくとも１つをセキュリティのピン留めのための参照フィールドとしてフラグ付けするステップ、を含み、かつ、

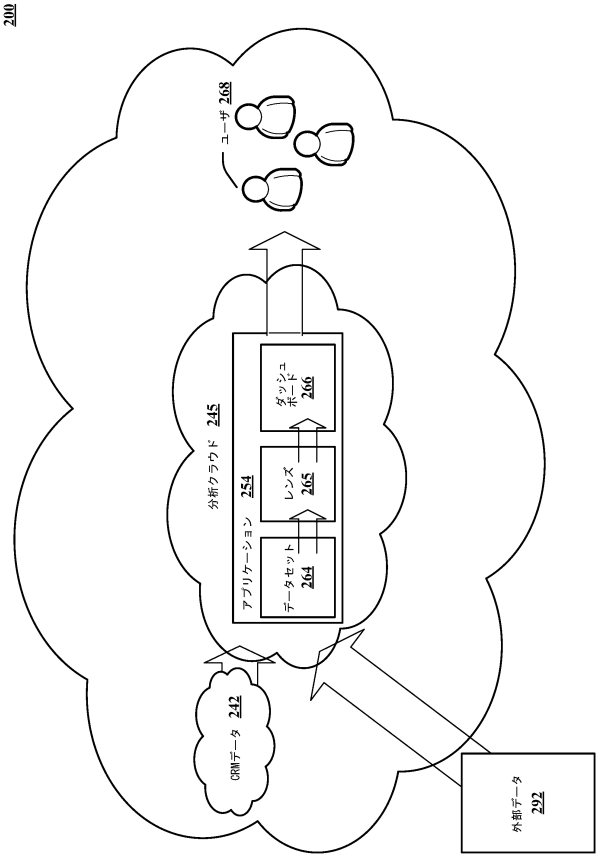
フラグ付けされた参照フィールドを列挙し、かつ、参照フィールドに対して抽出されたフィールドに係るセキュリティのピン留めをユーザが選択できるようにする、ユーザインターフェイスの表示を行う、

クローズ１４乃至１８のいずれか一つに係る非一時的なコンピュータで読取り可能な記憶媒体。

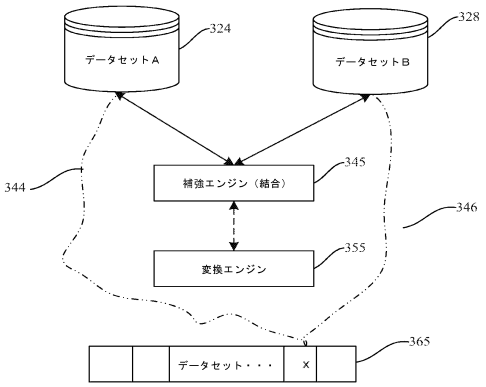
【図１】



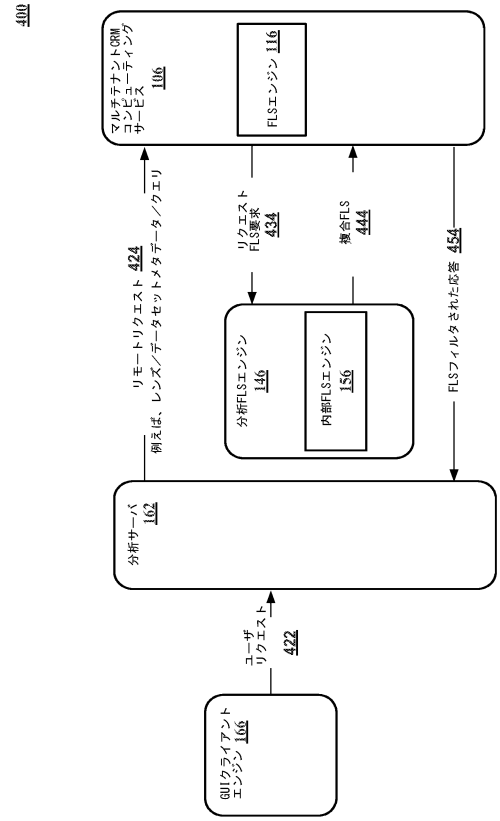
【図２】



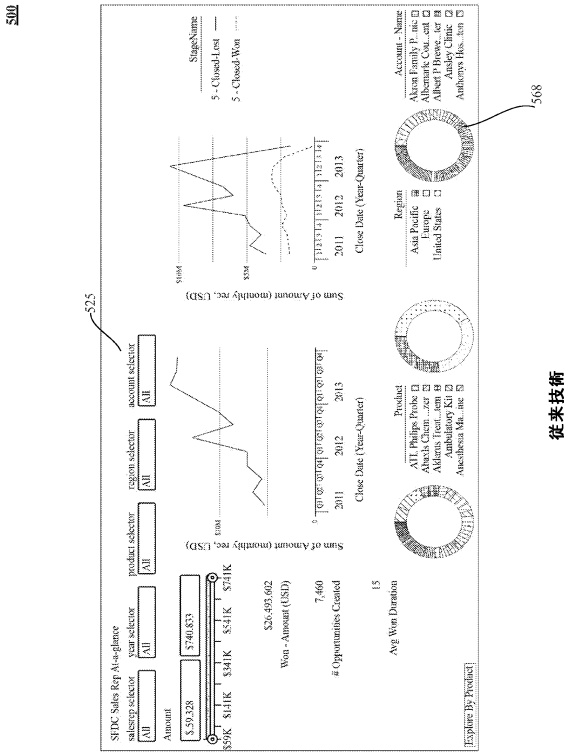
【図３】



【図４】

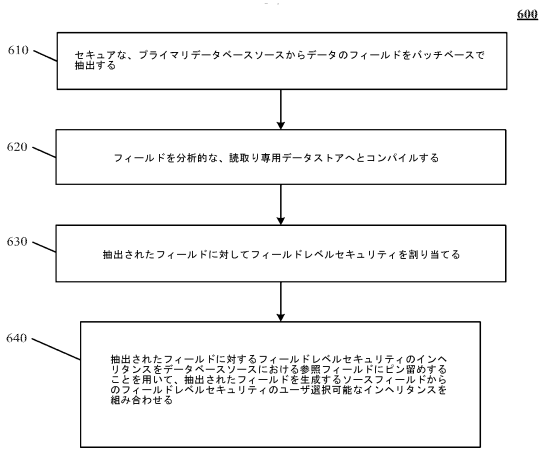


【図５】

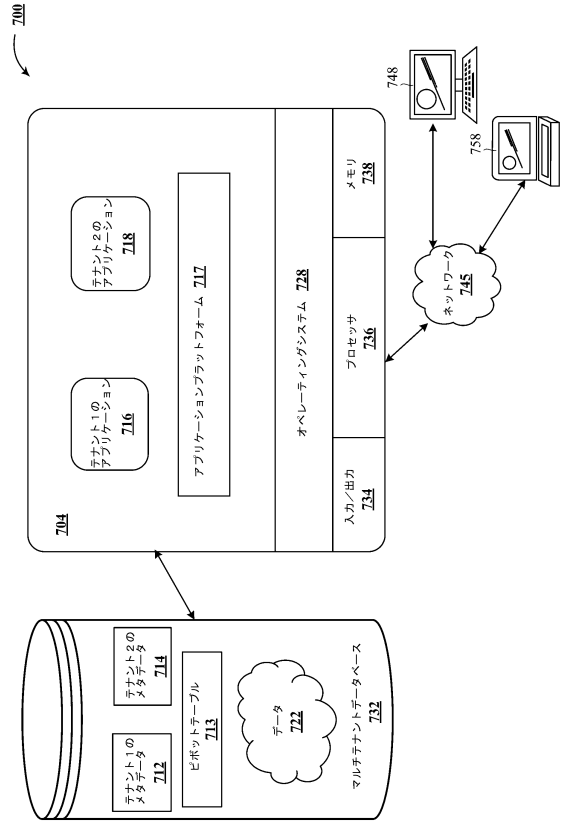


従来技術

【図６】



【図７】


700
704
テナント1の
アプリケーション
716
テナント2の
アプリケーション
718
アプリケーションプラットフォーム 717
オペレーティングシステム 728
入力/出力
734
プロセッサ
736
メモリ
738
748
758
ネットワーク
745
テナント1の
メタデータ
712
テナント2の
メタデータ
714
ピボットテーブル
713
データ
722
マルチテナントデータベース
732

フロントページの続き

(72)発明者　ティマーマン，ジャン　マイケル
カナダ国　ヴィ５ヴィ　３ジー９　ブリテッィシュ　コロンビア，ヴァンクーヴァー，オンタリオ　ストリート　４３６４
(72)発明者　シュナイダー，ドノヴァン
アメリカ合衆国　カリフォルニア州　９４１２７，サン　フランシスコ，アプトス　アヴェニュー　２５
(72)発明者　ギテルマン，アレックス
アメリカ合衆国　カリフォルニア州　９４７０７，バークリー，オックスフォード　ストリート　１１７５

審査官　平井　誠

(56)参考文献　米国特許出願公開第２００６／０２１８１５７（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６２
Ｇ０６Ｆ　１６／２１