【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成27年7月23日(2015.7.23)

【公表番号】特表2014-518416(P2014-518416A)
【公表日】平成26年7月28日(2014.7.28)
【年通号数】公開・登録公報2014-040
【出願番号】特願2014-515869(P2014-515869)
【国際特許分類】
Ｇ０６Ｆ　21/10　(2013.01)
Ｇ０６Ｑ　30/06　(2012.01)
Ｇ０６Ｑ　50/10　(2012.01)
【ＦＩ】
Ｇ０６Ｆ　21/22　１１０Ｃ
Ｇ０６Ｑ　30/06　１１０Ｅ
Ｇ０６Ｑ　50/10　１４０

【手続補正書】
【提出日】平成27年6月2日(2015.6.2)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
複数のプライベートデータセットを含むデータリポジトリであって、前記プライベートデータセットの各々は、データマーケットでの購入のために利用可能であり、前記複数のプライベートデータセットのうちの１つのプライベートデータセットは、第１のデータグループを含む一組のデータグループを含み、前記データグループの各々は、別々の暗号化キーを使用して暗号化され、前記第１のデータグループのデータは、前記第１のデータグループのための暗号化キーで暗号化され、前記データリポジトリは、前記第１のデータグループを第１のテーブルに格納し、前記第１のテーブルはデータの第１の部分を含み、前記データリポジトリはデータの得られる部分を第２のテーブルに格納し、データの前記得られる部分は、データの前記第１の部分から、データの前記第１の部分をデータの第２の部分と組み合わせることにより得られ、データの前記第２の部分は、前記第１のデータグループの外の場所からアクセスされ、データの前記第１の部分は、前記暗号化キーを用いて暗号化され、データの前記得られる部分がデータの前記第１の部分から得られることによる、データの前記得られる部分への不正アクセスを防ぐよう、データの前記得られる部分も前記暗号化キーを用いて暗号化される、データリポジトリと、
前記データマーケットでの購入のために利用可能なプライベートデータセットへのアクセスをコントロールするためのデータキュレーションシステムであって、前記データキュレーションシステムはサブスクライバーデータベースを含み、前記サブスクライバーデータベースは、サブスクライバーのサブスクライバープロファイルと、前記第１のデータグループの所有者のデータ所有者プロファイルとを含み、前記サブスクライバーデータベースは、前記サブスクライバーに前記暗号化キーへのアクセス権を付与する第１の資格を更に含み、前記暗号化キーは、前記サブスクライバーが、前記第１のデータグループの暗号化を解除し、データの前記得られる部分の暗号化を解除する際の使用を可能とする、データキュレーションシステムと
を含むシステム。

【請求項２】
請求項１に記載のシステムであって、前記データキュレーションシステムは、前記第１の資格に従い、前記第１のデータグループへのアクセスを管理する、システム。
【請求項３】
請求項２に記載のシステムであって、前記第１の資格は、前記第１のデータグループへの限定された数のアクセスを定め、前記データキュレーションシステムは、前記第１のデータグループへのアクセスを前記限定された数に制限する、システム。
【請求項４】
請求項１に記載のシステムであって、前記第１のテーブルも前記サブスクライバーのサブスクライバーデータを含む、システム。
【請求項５】
請求項４に記載のシステムであって、前記第１のデータグループの暗号化されていないフォーマットと前記第１のデータグループの暗号化されたフォーマットとが同じフォーマットであるように暗号化を保持するフォーマットを用いて、前記第１のデータグループは暗号化される、システム。
【請求項６】
請求項５に記載のシステムであって、前記サブスクライバーデータは前記暗号化されていないフォーマットである、システム
【請求項７】
請求項１に記載のシステムであって、前記第２のテーブルは、データ来歴を有する、システム。
【請求項８】
請求項１に記載のシステムであって、
前記第１のデータグループへの前記データマーケットを介した前記第１の資格を用いたアクセスを識別し、前記アクセスに基づいて課金イベントを生成する課金システム
をさらに含むシステム。
【請求項９】
請求項８に記載のシステムであって、前記課金イベントは、前記暗号化キーが要求されたときに生成される、システム。
【請求項１０】
データマーケットでの購入のために利用可能な複数のデータセットを提示するステップであって、前記データセットの各々は、データ所有者により所有され、データストアに格納され、前記データマーケットは、前記データセットの各々を使用する資格が与えられるための条件を提示し、第１のデータセットは第１のテーブルに格納された第１のデータグループを含み、データの得られる部分は第２のテーブルに格納され、前記第１のデータグループはデータの第１の部分を含み、データの前記得られる部分は、データの前記第１の部分から、データの前記第１の部分をデータの第２の部分と組み合わせることにより得られ、データの前記第２の部分は前記第１のデータセットの外の場所からのものであり、前記第１のテーブルの部分は前記第１のデータセットのための暗号化キーを用いて暗号化された、データの前記第１の部分を含み、データの前記得られる部分がデータの前記第１の部分から得られることによる、データの前記得られる部分への不正アクセスを防ぐように、前記第２のテーブルの部分は、前記第１のデータセットのための前記暗号化キーを用いて暗号化されたデータの前記得られる部分を含む、ステップと、
データユーザと前記データ所有者との間の第１の資格を確立するステップであって、前記第１の資格は、前記データユーザが前記第１のデータセットにアクセスすることを可能にし、前記第１の資格は、前記第１のデータセットを使用する資格が与えられるための提示された前記条件を満たす前記データユーザに基づく、ステップと、
データの前記第１の部分とデータの前記得られる部分のうちの一方の前記データユーザからの要求を受信するステップであって、前記要求は、前記第１の資格への参照を含む、ステップと、

前記第１の資格を評価して、前記データユーザが、データの前記第１の部分とデータの前記得られる部分とのうちの前記一方へのアクセスを有することを判定するステップと、
前記暗号化キーを用いて前記第１のデータセットの暗号化を解除するステップと
を含む方法。
【請求項１１】
請求項１０に記載の方法であって、
前記第１のデータセットの暗号化を解除するために、前記データユーザに前記暗号化キーを返すステップ
をさらに含む方法。
【請求項１２】
請求項１０に記載の方法であって、
前記データユーザが前記第１のデータセットを要求したことを検出し、課金システムに前記要求のログを作成するステップ
をさらに含む方法。
【請求項１３】
請求項１０に記載の方法であって、
消費者から前記第１のデータセットの来歴を要求するステップであって、前記消費者は、前記データユーザにより提供される前記第１のデータセットのユーザである、ステップと、
前記第１のデータセットの認証トークンを返すステップと
をさらに含む方法。
【請求項１４】
請求項１３に記載の方法であって、前記認証トークンは前記第１のデータセットのための公開キーである、方法。
【請求項１５】
請求項１４に記載の方法であって、前記消費者は、前記消費者と前記データユーザとの間の第２の資格を有し、前記第２の資格は、前記消費者が、前記複数のデータセットのうちの第２の異なるサブセットにアクセスすることを可能にする、方法。
【請求項１６】
請求項１５に記載の方法であって、前記第２の異なるサブセットは前記データストアに格納された、方法。
【請求項１７】
複数のプライベートデータセットを含むデータリポジトリであって、前記プライベートデータセットの各々は、データマーケットでの購入のために利用可能であり、前記複数のプライベートデータセットのうちの１つのプライベートデータセットは、第１のデータグループを含む一組のデータグループを含み、前記データリポジトリは、前記第１のデータグループを第１のテーブルに格納し、前記第１のデータグループはデータの第１の部分を含み、前記データリポジトリはデータの得られる部分を第２のテーブルに格納し、データの前記得られる部分は、データの前記第１の部分から、データの前記第１の部分をデータの第２の部分と組み合わせることにより得られ、データの前記第２の部分は、前記プライベートデータセットの外でアクセスされ、前記第１のテーブルの部分は、前記プライベートデータセットのための暗号化キーを用いて暗号化されたデータの前記第１の部分を含み、データの前記得られる部分がデータの前記第１の部分から得られることによる、データの前記得られる部分への不正アクセスを防ぐよう、前記第２のテーブルの部分は、前記暗号化キーを用いて暗号化された、データの前記得られる部分を含む、データリポジトリと、
別々のデータ所有者により所有された前記プライベートデータセットの各々と、
前記プライベートデータセットのうちの前記１つのプライベートデータセットのための前記暗号化キーを含む、各プライベートデータセットのための別々の暗号化キーを含む暗号化キーリポジトリと、

前記データマーケットでの購入のために利用可能なデータへのアクセスをコントロールするためのデータキュレーションシステムであって、前記データキュレーションシステムは、
資格を含むサブスクライバーデータベースであって、前記資格は、サブスクライバーに、データ所有者により所有されるプライベートデータセットへのアクセス権を付与する、サブスクライバーデータベース
を含み、前記データキュレーションシステムは、
前記プライベートデータセットにアクセスする資格が与えられるための条件を満たすサブスクライバーに基づいて、プライベートデータセットにアクセスするための資格をサブスクライバーに付与し、
第１の資格と、データの前記第１の部分とデータの前記得られる部分とのうちの一方の要求とを含む第１の要求を第１のサブスクライバーから受け、
前記第１の資格を確認し、
プライベートデータセットのための前記暗号化キーを前記第１のサブスクライバーに返す、
データキュレーションシステムと
を含むシステム。
【請求項１８】
請求項１７に記載のシステムであって、
前記第１の要求を課金イベントとして検出する課金システム
をさらに含むシステム。
【請求項１９】
システムメモリ及びプロセッサを含むコンピュータシステムでの方法であって、
前記プロセッサが第１のデータセットにアクセスするステップであって、前記第１のデータセットは、前記第１のデータセットへのアクセスをコントロールするための第１のアクセス条件に関連付けられた、ステップと、
前記プロセッサが、前記第１のデータセットの別のバージョン又は前記第１のデータセットの得られるバージョンを含む得られるデータセットを、前記第１のデータセットを第２の別のデータセットと組み合わせることにより生成するステップであって、前記第２の別のデータセットは、前記第１のデータセットとは別に、前記第１のデータセットの外で維持され、前記第２の別のデータセットへのアクセスをコントロールするための第２のアクセス条件と関連付けられ、前記得られるデータセットは、前記第１のアクセス条件と前記第２のアクセス条件との双方に関連付けられた、ステップと
を含み、
前記得られるデータセットへの不正アクセスが、前記得られるデータセットを使用する資格を与える前に、前記第１のアクセス条件と前記第２のアクセス条件との双方が満たされることを要求することにより防がれる、方法。
【請求項２０】
請求項１９に記載の方法であって、前記得られるデータセットが前記第１のデータセットと同じ手法で管理できるよう、前記第１のデータセットと前記得られるデータセットとの双方を暗号化キーを用いて暗号化するステップをさらに含む方法。
【請求項２１】
請求項２０に記載の方法であって、前記第１のデータセット又は前記第２の別のデータセットへのアクセス権を、前記暗号化キーを返して前記第１のデータセット又は前記得られるデータセットの暗号化を解除することにより付与するステップをさらに含む方法。
【請求項２２】
請求項２１に記載の方法であって、前記第１のデータセット又は前記得られるデータセットへのアクセスを許可することと関連付けられた課金イベントを作成するステップをさらに含む方法。
【請求項２３】

請求項１９に記載の方法であって、前記得られるデータセットへのアクセスのための資格を確立するステップであって、前記資格は、前記第１のデータセットのデータ所有者とデータユーザとの間に確立された、ステップをさらに含む方法。
【請求項２４】
コンピュータシステムにある方法を実行させるコンピュータプログラムであって、前記方法は、
第１のデータセットにアクセスするステップであって、前記第１のデータセットは、前記第１のデータセットへのアクセスをコントロールするための第１のアクセス条件に関連付けられた、ステップと、
前記第１のデータセットの別のバージョン又は前記第１のデータセットの得られるバージョンを含む得られるデータセットを、前記第１のデータセットを第２の別のデータセットと組み合わせることにより生成するステップであって、前記第２の別のデータセットは、前記第１のデータセットとは別に、前記第１のデータセットの外で維持され、前記第２の別のデータセットへのアクセスをコントロールするための第２のアクセス条件と関連付けられ、前記得られるデータセットは、前記第１のアクセス条件と前記第２のアクセス条件との双方に関連付けられた、ステップと
を含み、
前記得られるデータセットへの不正アクセスが、前記得られるデータセットを使用する資格を与える前に、前記第１のアクセス条件と前記第２のアクセス条件との双方が満たされることを要求することにより防がれる、コンピュータプログラム。
【請求項２５】
請求項２４に記載のコンピュータプログラムであって、前記方法は、前記得られるデータセットが前記第１のデータセットと同じ手法で管理できるよう、前記第１のデータセットと前記得られるデータセットとの双方を暗号化キーを用いて暗号化するステップをさらに含む、コンピュータプログラム。
【請求項２６】
請求項２５に記載のコンピュータプログラムであって、前記方法は、前記第１のデータセット又は前記第２の別のデータセットへのアクセス権を、前記暗号化キーを返して前記第１のデータセット又は前記得られるデータセットの暗号化を解除することにより付与するステップをさらに含む、コンピュータプログラム。
【請求項２７】
請求項２４に記載の方法であって、前記方法は、前記得られるデータセットへのアクセスのための資格を確立するステップであって、前記資格は、前記第１のデータセットのデータ所有者とデータユーザとの間に確立された、ステップをさらに含む、コンピュータプログラム。
【請求項２８】
１以上のプロセッサと、
システムメモリと、
コンピュータ実行可能命令を格納した１以上のコンピュータ記憶装置と
を含むシステムであって、前記コンピュータ実行可能命令は前記システムをキュレーションシステムとして機能させ、前記キュレーションシステムは、
第１のデータセットにアクセスし、前記第１のデータセットは、前記第１のデータセットへのアクセスをコントロールするための第１のアクセス条件に関連付けられ、
前記第１のデータセットの別のバージョン又は前記第１のデータセットの得られるバージョンを含む得られるデータセットを、前記第１のデータセットを第２の別のデータセットと組み合わせることにより生成し、前記第２の別のデータセットは、前記第１のデータセットとは別に、前記第１のデータセットの外で維持され、前記第２の別のデータセットへのアクセスをコントロールするための第２のアクセス条件と関連付けられ、前記得られるデータセットは前記第１のアクセス条件と前記第２のアクセス条件との双方に関連付けられた

ように構成され、前記得られるデータセットへの不正アクセスが、前記得られるデータセットを使用する資格を与える前に、前記第１のアクセス条件と前記第２のアクセス条件との双方が満たされることを要求することにより防がれる、システム。

【請求項２９】

請求項２８に記載のシステムであって、前記キュレーションシステムは、データユーザに前記第１のデータセット又は前記得られるデータセットへのアクセス権を付与するようにさらに構成された、システム。

【請求項３０】

請求項２８に記載のシステムであって、前記キュレーションシステムは、前記得られるデータセットにアクセスするための資格を確立するようにさらに構成され、前記資格は、前記第１のデータセットのデータ所有者とデータユーザとの間に確立される、システム。