(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7131314号
(P7131314)

(45)発行日　令和4年9月6日(2022.9.6)

(24)登録日　令和4年8月29日(2022.8.29)

(51)国際特許分類
Ｇ０６Ｆ　21/62　(2013.01)

ＦＩ
Ｇ０６Ｆ　21/62　３５４

請求項の数　7　（全16頁）

(21)出願番号　特願2018-211642(P2018-211642)
(22)出願日　平成30年11月9日(2018.11.9)
(65)公開番号　特開2020-77339(P2020-77339A)
(43)公開日　令和2年5月21日(2020.5.21)
審査請求日　令和3年8月10日(2021.8.10)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　110002147弁理士法人酒井国際特許事務所
(72)発明者　谷口 和博
神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内
審査官　平井 誠

最終頁に続く

(54)【発明の名称】　情報管理プログラム、情報管理方法、情報管理装置、情報処理プログラム、情報処理方法及び情報処理装置

(57)【特許請求の範囲】

【請求項１】

ある個人の情報へのアクセス要求を、前記ある個人の情報を含みうる第１のデータテーブルと前記ある個人の情報を含みうる第２のデータテーブルとの指定とともに受け付け、

前記第１のデータテーブルと前記第２のデータテーブルとに同一のキーが含まれるか否かに応じて、前記アクセス要求に対する応答結果である前記第１のデータテーブルと前記第２のデータテーブルとを組み合わせたデータが個人を特定する情報を含み得るか否かを判定し、

前記アクセス要求が前記第１のデータテーブルと前記第２のデータテーブルを前記キーによって組み合わせる要求である場合、又は、前記第１のデータテーブル又は前記第２のデータテーブルから前記キーを用いて前記ある個人の情報を検索する場合に、前記アクセス要求が前記個人を特定する情報へのアクセスであると判定した場合に前記データへのアクセスの禁止または応答結果の秘匿化を実行するとともに、不正アクセスを示す第１のアラートを出力し、

前記アクセス要求が前記第１のデータテーブル又は前記第２のデータテーブルから前記キーを検索する場合に、前記アクセス要求が前記個人を特定する情報へのアクセスである可能性があると判定した場合に予兆アクセスを示す第２のアラートを出力するように制御する

処理をコンピュータに実行させることを特徴とする情報管理プログラム。

【請求項２】

前記制御する処理は、

前記アクセス要求が前記個人を特定する情報へのアクセスであると判定した場合に、前記アクセス要求が正常な業務のポリシーに即した個人を特定する情報へのアクセスであるか否かをさらに判定し、ポリシーに即した個人を特定する情報へのアクセスであると判定した場合に前記データへのアクセスの禁止または応答結果の秘匿化を実行することを特徴とする請求項１に記載の情報管理プログラム。

【請求項３】

前記ポリシーには、前記アクセス要求が行われる時間帯、前記アクセス要求を行うアプリケーション、前記アクセス要求を行うクライアント装置の少なくとも一つが含まれることを特徴とする請求項２に記載の情報管理プログラム。

【請求項４】

前記第２のデータテーブルに設定された参照制約を用いて前記第２のデータテーブルと前記第１のデータテーブルとの関連を特定する処理を前記コンピュータにさらに実行させることを特徴とする請求項１乃至３のいずれか一項に記載の情報管理プログラム。

【請求項５】

複数のデータテーブルの中から氏名及び生年月日を含むデータテーブルを前記第１のデータテーブルとして特定する処理を前記コンピュータにさらに実行させることを特徴とする請求項１乃至４のいずれか一項に記載の情報管理プログラム。

【請求項６】

ある個人の情報へのアクセス要求を、前記ある個人の情報を含みうる第１のデータテーブルと前記ある個人の情報を含みうる第２のデータテーブルとの指定とともに受け付け、

前記第１のデータテーブルと前記第２のデータテーブルとに同一のキーが含まれるか否かに応じて、前記アクセス要求に対する応答結果である前記第１のデータテーブルと前記第２のデータテーブルとを組み合わせたデータが個人を特定する情報を含み得るか否かを判定し、

前記アクセス要求が前記第１のデータテーブルと前記第２のデータテーブルを前記キーによって組み合わせる要求である場合、又は、前記第１のデータテーブル又は前記第２のデータテーブルから前記キーを用いて前記ある個人の情報を検索する場合に、前記アクセス要求が前記個人を特定する情報へのアクセスであると判定した場合に前記データへのアクセスの禁止または応答結果の秘匿化を実行するとともに、不正アクセスを示す第１のアラートを出力し、

前記アクセス要求が前記第１のデータテーブル又は前記第２のデータテーブルから前記キーを検索する場合に、前記アクセス要求が前記個人を特定する情報へのアクセスである可能性があると判定した場合に予兆アクセスを示す第２のアラートを出力するように制御する

処理をコンピュータが実行することを特徴とする情報管理方法。

【請求項７】

ある個人の情報へのアクセス要求を、前記ある個人の情報を含みうる第１のデータテーブルと前記ある個人の情報を含みうる第２のデータテーブルとの指定とともに受け付け、前記第１のデータテーブルと前記第２のデータテーブルとに同一のキーが含まれるか否かに応じて、前記アクセス要求に対する応答結果である前記第１のデータテーブルと前記第２のデータテーブルとを組み合わせたデータが個人を特定する情報を含み得るか否かを判定する判定部と、

前記アクセス要求が前記第１のデータテーブルと前記第２のデータテーブルを前記キーによって組み合わせる要求である場合、又は、前記第１のデータテーブル又は前記第２のデータテーブルから前記キーを用いて前記ある個人の情報を検索する場合に、前記アクセス要求が前記個人を特定する情報へのアクセスであると判定した場合に前記データへのアクセスの禁止または応答結果の秘匿化を実行するとともに、不正アクセスを示す第１のアラートを出力し、前記アクセス要求が前記第１のデータテーブル又は前記第２のデータテーブルから前記キーを検索する場合に、前記アクセス要求が前記個人を特定する情報へのアクセスである可能性があると判定した場合に予兆アクセスを示す第２のアラートを出力するように制御する処理部と、

を有することを特徴とする情報管理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報管理プログラム、情報管理方法、情報管理装置、情報処理プログラム、情報処理方法及び情報処理装置に関する。
【背景技術】
【０００２】
改正個人情報保護法の全面施行により、平成２９年５月３０日から個人情報を取り扱う全ての事業者に個人情報保護法が適用され、各事業者に対して個人情報に関する厳正な取扱いが求められる。このため、個人情報の安全管理に関する対策を講じる動きが活発化しつつある。特に、個人情報の漏洩に関しては、企業の存続にも大きく影響を与えることから、個人情報を取り扱う管理部門での企業コンプライアンスの徹底だけでなく、個人情報データベースシステムでのセキュリティ対策が重要となっている。
【０００３】
個人情報データベースシステムでは、個人情報だけでなく準個人情報のセキュリティ対策も重要である。ここで、「準個人情報」とは、個人情報の要素となる情報であり、関連する情報と組み合わせることで個人情報となり得る情報である。
【０００４】
図１１は、準個人情報を説明するための図である。図１１において、準個人情報テーブル１１ａは、ＳＮＳ（Social Networking Service）を利用するユーザの氏名や生年月日などの準個人情報を管理するテーブルである。準個人情報テーブル１１ａには個人情報の一部が含まれる。準個人情報テーブル１１ａには、アカウントデータとして、アカウントＩＤ、氏名、メールアドレス、生年月日、住所、電話番号が含まれる。
【０００５】
アカウントＩＤは、ユーザのＳＮＳのアカウントを識別する識別子である。氏名は、ユーザの名前である。メールアドレスは、ユーザのメールアドレスである。生年月日は、ユーザが生まれた年月日である。住所は、ユーザの住所である。電話番号は、ユーザの電話番号である。
【０００６】
関連テーブル１１ｂは、投稿内容などアカウントに付随した情報をリアルタイムに蓄積するテーブルである。関連テーブル１１ｂには人物の詳細な行動などが記録され、関連テーブル１１ｂに蓄積される情報は、個人は特定されないが秘匿性のある情報である。関連テーブル１１ｂには、投稿データとして、ポストＩＤ、アカウントＩＤ、投稿日、投稿内容が含まれる。
【０００７】
ポストＩＤは、投稿を識別する識別子である。アカウントＩＤは、投稿したユーザのアカウントを識別する識別子である。投稿日は、投稿された年月日である。投稿内容は、投稿された内容である。
【０００８】
準個人情報テーブル１１ａと関連テーブル１１ｂは、アカウントＩＤを用いて結合が可能である。また、アカウントデータに対する投稿データの関係は１：ｎ（ｎは正の整数）である。アカウントＩＤを用いてアカウントデータと投稿データを組み合わせることで個人の行動や嗜好が判明するので、アカウントデータと投稿データを組み合わせた情報は個人情報となる。
【０００９】
なお、携帯端末から顧客情報の閲覧を要求されると、表示条件テーブルに登録された年月日、携帯端末識別情報、顧客名が閲覧要求と合致する場合に、顧客情報を携帯端末に表示させることで、携帯端末からの重要情報の漏洩リスクを最小限に抑える従来技術がある。
【００１０】

また、取得要求で要求されたデータが格納される列の機密識別属性を参照して該データが機密情報であるか否かを判定し、機密情報である場合には列の射影を禁止することで、機密情報を保護するデータベース管理システムがある。

【００１１】

また、操作対象データ又はその所有者ごとにアクセス制御ルールを作成しなくても済むようにすることで、データ蓄積システムの管理者の負担を軽減する従来技術がある。この従来技術では、データ蓄積システムは、データ操作要求を受信した場合に、このデータ操作要求により指定されたアクセス者情報、操作種別情報及びデータ集合識別情報の全てが一致することを第１の検索条件とする。また、データ蓄積システムは、データ操作要求により指定された操作対象の患者データに含まれる複数の項目のうちアクセス制御データキーとして用いる項目の１つ以上の組み合わせと一致することを第２の検索条件とする。そして、第１及び第２の検索条件を満足するアクセス制御ルールを、アクセス制御リスト記憶部から検索し、このアクセス制御ルールをもとにアクセス拒否を判定する。

【００１２】

また、参照者が参照した被参照者に関する個人情報やライフログ情報が複数統合されて、被参照者が公開したくないと考える範囲まで個人の特定が絞り込まれるのを防ぐ従来技術がある。この従来技術では、開示要求取得部が、参照者が公開を要求している公開情報を示す開示要求を取得する。すると、情報開示制御部は、参照情報記憶部が記憶する参照情報に含まれる公開情報と開示要求が示す公開情報との組み合わせが、拒否情報記憶部が記憶する拒否情報に含まれるか否かを判定する。そして、情報開示制御部は、拒否情報に含まれると判定した場合、開示要求が示す公開情報の該参照者への送信を禁止し、拒否情報に含まれないと判定した場合、開示要求が示す公開情報を公開情報記憶部から読み出して、情報開示部に参照者端末へ送信させる。

【先行技術文献】

【特許文献】

【００１３】

【文献】特開２０１５－１７６３１０号公報
特開２００８－１３４９３６号公報
特開２０１３－１３４７３１号公報
特開２０１１－２５７８６３号公報

【発明の概要】

【発明が解決しようとする課題】

【００１４】

しかしながら、上記技術では複数のテーブルに記憶されたデータの組み合わせにより個人情報となる情報であるか否かを判定する場合に、開示を禁止する情報となる可能性のあるテーブルの組み合わせを予め設定しておく必要があり処理が煩雑となる。

【００１５】

本発明は、１つの側面では、予め設定することなしに準個人情報と関連情報の組み合わせによる個人情報漏洩を抑止可能とすることを目的とする。

【課題を解決するための手段】

【００１６】

１つの態様では、情報管理プログラムは、ある個人の情報へのアクセス要求を、前記ある個人の情報を含みうる第１のデータテーブルと前記ある個人の情報を含みうる第２のデータテーブルとの指定とともに受け付ける処理をコンピュータに実行させる。そして、前記情報管理プログラムは、前記第１のデータテーブルと前記第２のデータテーブルとに同一のキーが含まれるか否かに応じて、前記アクセス要求に対する応答結果が個人を特定する情報を含み得るか否かを判定する処理を前記コンピュータに実行させる。ここで、応答結果は、前記第１のデータテーブルと前記第２のデータテーブルとを組み合わせたデータである。そして、前記情報管理プログラムは、個人を特定する情報を含み得ると判定した場合に前記アクセス要求に対する応答の出力を制御する。

【発明の効果】
【００１７】
１つの側面では、本発明は、予め設定することなしに準個人情報と関連情報の組み合わせによる個人情報漏洩を抑止可能とすることができる。
【図面の簡単な説明】
【００１８】
【図１】図１は、実施例に係るＤＢＭＳの機能構成を示す図である。
【図２】図２は、テーブル属性情報とポリシー情報の例を示す図である。
【図３】図３は、参照制約の一例を示す図である。
【図４】図４は、予兆アクセス及び個人情報アクセスの例を示す図である。
【図５】図５は、アラームの例を示す図である。
【図６】図６は、ＳＱＬ問合せ処理のフローを示すフローチャートである。
【図７】図７は、検知処理のフローを示すフローチャートである。
【図８】図８は、リスク評価及びアラート発信処理のフローを示すフローチャートである。
【図９】図９は、データ秘匿化処理のフローを示すフローチャートである。
【図１０】図１０は、実施例に係るデータベース管理プログラムを実行するコンピュータのハードウェア構成を示す図である。
【図１１】図１１は、準個人情報を説明するための図である。
【発明を実施するための形態】
【００１９】
以下に、本願の開示する情報管理プログラム、情報管理方法、情報管理装置、情報処理プログラム、情報処理方法及び情報処理装置の実施例を図面に基づいて詳細に説明する。なお、この実施例は開示の技術を限定するものではない。
【実施例】
【００２０】
まず、実施例に係るデータベース管理システム（ＤＢＭＳ：Database Management System）の機能構成について説明する。図１は、実施例に係るＤＢＭＳの機能構成を示す図である。図１に示すように、実施例に係るＤＢＭＳ１は、テーブル記憶部１１と、メタ情報記憶部１２と、属性情報作成部１３と、監査ログ記憶部１４と、ＳＱＬ処理部２０とを有する。
【００２１】
テーブル記憶部１１は、図１１に例を示した準個人情報テーブル１１ａと関連テーブル１１ｂを記憶する。準個人情報テーブル１１ａと関連テーブル１１ｂの組み合わせにより個人情報が特定される。なお、関連テーブル１１ｂは複数あってもよい。また、テーブル記憶部１１は、準個人情報テーブル１１ａでもなく関連テーブル１１ｂでもないテーブルも記憶する。
【００２２】
メタ情報記憶部１２は、テーブル記憶部１１が記憶する情報に関する情報をメタ情報として記憶する。メタ情報記憶部１２は、テーブル属性情報１２ａとポリシー情報１２ｂと定義情報１２ｃを記憶する。テーブル属性情報１２ａは、テーブルの属性に関する情報である。ポリシー情報１２ｂは、準個人情報テーブル１１ａ及び関連テーブル１１ｂにアクセスする正常な業務のポリシーに関する情報である。定義情報１２ｃは、テーブルを定義する情報である。
【００２３】
図２は、テーブル属性情報１２ａとポリシー情報１２ｂの例を示す図である。図２（ａ）に示すように、テーブル属性情報１２ａには、テーブル名と、属性と、準個人情報テーブル名と、結合キーとが含まれる。
【００２４】
テーブル名は、テーブルを識別する名前である。属性は、テーブルが準個人情報テーブル１１ａであるか関連テーブル１１ｂであるかその他の非対象テーブルであるかを示す。

準個人情報テーブル名は、テーブルが関連テーブル１１ｂである場合に、結合される準個人情報テーブル１１ａの名前である。結合キーは、準個人情報テーブル１１ａと関連テーブル１１ｂの結合に用いられるキーである。

【００２５】

例えば、「ａｃｃｏｕｎｔ」で識別されるテーブルは、準個人情報テーブル１１ａであり、関連テーブル１１ｂとの結合に用いられるキーは、「ａｃｃ＿ｉｄ」である。また、「ｐｏｓｔ＿ｍｅｓｓａｇｅ」で識別されるテーブルは、関連テーブル１１ｂであり、結合される準個人情報テーブル１１ａは「ａｃｃｏｕｎｔ」であり、準個人情報テーブル１１ａとの結合に用いられるキーは、「ａｃｃ＿ｉｄ」である。

【００２６】

図２（ｂ）に示すように、ポリシー情報１２ｂには、準個人情報テーブル名と、種別と、ポリシーとが含まれる。

【００２７】

準個人情報テーブル名は、ポリシーが適用される準個人情報テーブル１１ａを識別する名前である。種別は、ポリシーの種別である。種別には、正常な業務が準個人情報テーブル１１ａにアクセスする時間である「アクセス時間」と、正常な業務の名前である「業務アプリケーション名」と、アクセスする装置を示す「クライアントマシン」がある。

【００２８】

ポリシーは、正常なアクセスに関する情報であり、種別毎に異なる。種別が「アクセス時間」の場合には、ポリシーは、正常なアクセスが行われる時間帯である。種別が「業務アプリケーション名」の場合には、ポリシーは、正常なアクセスを行うアプリケーションの名前である。種別が「クライアントマシン」の場合には、ポリシーは、正常なアクセスを行うクライアント装置のＩＰ（Internet Protocol）アドレスである。

【００２９】

例えば、「ａｃｃｏｕｎｔ」で識別される準個人情報テーブル１１ａは、ＩＰアドレスが「１９２．３３．４４．＊」である装置で動作する「ａｐｌ０１」から「００：００：００」－「０６：２９：５９」にアクセスされる。

【００３０】

なお、準個人情報テーブル名が「ｄｅｆａｕｌｔ」であるエントリは、デフォルト値を示す。図２（ｂ）では、デフォルト値は、「アクセス時間」が「００：００：００」－「０５：５９：５９」である。このように、ポリシー情報１２ｂには、「アクセス時間」、「業務アプリケーション名」、「クライアントマシン」のうち一つ以上が含まれればよい。

【００３１】

属性情報作成部１３は、テーブル記憶部１１が記憶するテーブルを解析してテーブル属性情報１２ａを作成し、メタ情報としてメタ情報記憶部１２に格納する。属性情報作成部１３は、テーブルに格納されているデータのカラム（列）を氏名や生年月日などの名詞句に自然言語解析を用いて分類し、例えば、氏名と生年月日をカラムに含むテーブルを準個人情報テーブル１１ａとして特定する。

【００３２】

属性情報作成部１３は、例えば、ＤＢＭＳ１が定期的に非同期で行っている統計情報の最新化の延長で準個人情報テーブル１１ａを特定する。あるいは、属性情報作成部１３は、ＳＱＬ文によるデータ格納時に準個人情報テーブル１１ａを特定してもよい。あるいは、属性情報作成部１３は、システム管理者からキーボードやタッチパネルによるテーブル名の入力を受け付けて、準個人情報テーブル１１ａを特定してもよい。

【００３３】

属性情報作成部１３は、準個人情報テーブル１１ａの一意性制約が設定されたカラムを用いて関連テーブル１１ｂを特定する。その理由は、準個人情報テーブル１１ａのようなアカウントを管理するテーブルの場合、アカウントを一意に示す識別子に一意性制約が設定されるためである。

【００３４】

関連テーブル１１ｂは、準個人情報テーブル１１ａで一意性制約が設定された識別子を結合キーとして準個人情報テーブル１１ａに関連付けられる。関連テーブル１１ｂでは、準個人情報テーブル１１ａに関連付けられることを示すために、外部キー制約である参照制約が設定される。属性情報作成部１３は、準個人情報テーブル１１ａで一意性制約が設定された識別子を参照する参照制約を用いて関連テーブル１１ｂを特定する。

【００３５】

図３は、参照制約の一例を示す図である。図３では、「ｐｏｓｔ＿ｍｅｓｓａｇｅ」で識別されるテーブル（ＴＡＢＬＥ）において、「ＣＯＮＳＴＲＡＩＮＴ　ｃｓ１　ＦＯＲＥＩＧＮ　ＫＥＹ（ａｃｃ＿ｉｄ）　ＲＥＦＥＲＥＮＣＥＳ　ａｃｃｏｕｎｔ（ａｃｃ＿ｉｄ）」が参照制約である。

【００３６】

「ａｃｃｏｕｎｔ」で識別される準個人情報テーブル１１ａでは、「ＰＲＩＭＡＲＹ　ＫＥＹ（ａｃｃ＿ｉｄ）」により「ａｃｃ＿ｉｄ」に一意性制約が設定される。また、参照制約で、「ａｃｃｏｕｎｔ」で識別される準個人情報テーブル１１ａの「ａｃｃ＿ｉｄ」が外部キーとして参照され、「ａｃｃ＿ｉｄ」が結合キーとなる。「ｃｓ１」は、参照制約を識別する識別子である。参照制約は定義情報１２ｃに含まれる。

【００３７】

図１に戻って、監査ログ記憶部１４は、テーブルへの不正アクセスや予兆アクセスが行われた場合のアラートを記憶する。ここで、予兆アクセスとは、個人情報へのアクセスの予兆となるアクセスである。

【００３８】

ＳＱＬ処理部２０は、ＳＱＬ問合せを処理する。ＳＱＬ処理部２０は、関係判断部２１と、検知部２２と、リスク評価部２３と、アラート発信部２４と、データ秘匿部２５とを有する。

【００３９】

関係判断部２１は、ＳＱＬによる問合せが準個人情報テーブル１１ａと関連テーブル１１ｂの少なくとも一方へのアクセスであるか否かをテーブル属性情報１２ａを参照して判断する。

【００４０】

検知部２２は、関係判断部２１により準個人情報テーブル１１ａと関連テーブル１１ｂの少なくとも一方へのアクセスであると判断されたＳＱＬ問合せの中から、予兆アクセス又は個人情報アクセスを検知する。

【００４１】

検知部２２は、結合キーをＳＱＬ文の選択列に指定している場合に、ＳＱＬ問合せを予兆アクセスとして検知する。検知部２２は、結合キーをＳＱＬ文の条件列に指定している場合に、ＳＱＬ問合せを個人情報アクセスとして検知する。検知部２２は、ＳＱＬ文で準個人情報テーブル１１ａと関連テーブル１１ｂを結合している場合に、ＳＱＬ問合せを個人情報アクセスとして検知する。

【００４２】

図４は、予兆アクセス及び個人情報アクセスの例を示す図である。図４（ａ）は、結合キーをＳＱＬ文の選択列に指定する予兆アクセスの例を示す。図４（ｂ）は、結合キーをＳＱＬ文の条件列に指定する個人情報アクセスの例を示し、図４（ｃ）は、ＳＱＬ文で準個人情報テーブル１１ａと関連テーブル１１ｂを結合する個人情報アクセスの例を示す。

【００４３】

図４（ａ）は、準個人情報テーブル１１ａ又は関連テーブル１１ｂを検索するために結合キーを事前に検索していることを示す。図４（ａ）の最初の例は結合キー「ａｃｃ＿ｉｄ」を準個人情報テーブル１１ａ「ａｃｃｏｕｎｔ」から検索し、図４（ａ）の２番目の例は結合キー「ａｃｃ＿ｉｄ」を関連テーブル１１ｂ「ｐｏｓｔ＿ｍｅｓｓａｇｅ」から検索している。

【００４４】

図４（ｂ）では、結合キーから個人情報が検索されている。図４（ｂ）の最初のＳＱＬ文で関連テーブル１１ｂ「ｐｏｓｔ＿ｍｅｓｓａｇｅ」から「ｍｅｓｓａｇｅ（投稿内容）」が検索されている。そして、２番目のＳＱＬ文で準個人情報テーブル１１ａ「ａｃｃｏｕｎｔ」から「ｎａｍｅ（氏名）」と「ａｄｄｒｅｓｓ（住所）」が検索されている。２つのＳＱＬ文の検索結果を組み合わせると、個人情報が得られる。

【００４５】

図４（ｃ）では、一つのＳＱＬ文で完結させて、個人情報が検索されている。図４（ｃ）の例では、「ｐｏｓｔ＿ｍｅｓｓａｇｅ」と「ａｃｃｏｕｎｔ」で「ａｃｃ＿ｉｄ」が等しく、「ａｃｃｏｕｎｔ」の「ｎａｍｅ（氏名）」の一部に「ｈｏｇｅ」を含む「ｍｅｓｓａｇｅ（投稿内容）」が検索されている。

【００４６】

リスク評価部２３は、検知部２２により検知された予兆アクセス及び個人情報アクセスのリスクを評価する。リスク評価部２３は、検知部２２により予兆アクセスが検知された場合には、監視が必要であると判定する。また、リスク評価部２３は、検知部２２により個人情報アクセスが検知された場合には、ポリシー情報１２ｂに基づいて、正常な業務のポリシーに沿った正常アクセスであるのか正常な業務のポリシーに沿わない不正アクセスであるのかを判定する。

【００４７】

アラート発信部２４は、リスク評価部２３により監視が必要であると判定された場合及び不正アクセスであると判定された場合に、アラームを監査ログ記憶部１４に出力する。図５は、アラームの例を示す図である。図５（ａ）は、予兆アクセスが行われた場合のアラートを示し、図５（ｂ）は、不正アクセスが行われた場合のアラートを示す。

【００４８】

図５（ａ）に示すように、アラート発信部２４が結合キー（ｆｏｒｅｉｇｎ ｋｅｙ）を出力することで、システム管理者は結合キーを条件列に指定する検索に限定して、実際に個人情報をアクセスする問合せを監視することができる。また、図５（ｂ）に示すように、アラート発信部２４がアラートを出力することで、システム管理者は不正なアクセスが行われたことを知ることができる。

【００４９】

また、アラート発信部２４は、リスク評価部２３により不正アクセスであると判定された場合に、不正アクセスのコネクションを強制切断する。

【００５０】

データ秘匿部２５は、リスク評価部２３により正常アクセスであると判定された場合に、準個人情報テーブル１１ａと関連テーブル１１ｂへの問合せ結果を秘匿化して出力する。なお、業務によって秘匿化が必要ない場合には、データ秘匿部２５は、秘匿化を行うことなく問合せ結果を出力する。

【００５１】

次に、ＳＱＬ問合せ処理のフローについて説明する。図６は、ＳＱＬ問合せ処理のフローを示すフローチャートである。図６に示すように、ＳＱＬ処理部２０は、ユーザを認証するユーザ認証処理を行い（ステップＳ１）、ユーザ認証に成功すると、ユーザが入力したＳＱＬ文の読み込みを行う（ステップＳ２）。

【００５２】

そして、ＳＱＬ処理部２０は、ＳＱＬ文の字句解析及び構文解析を行い（ステップＳ３）、意味解析を行う（ステップＳ４）。ＳＱＬ処理部２０は、意味解析を行う際に、ＳＱＬによる問合せが準個人情報テーブル１１ａと関連テーブル１１ｂの少なくとも一方へのアクセスであるか否かをテーブル属性情報１２ａを参照して判断する。そして、ＳＱＬ処理部２０は、ＳＱＬによる問合せが準個人情報テーブル１１ａと関連テーブル１１ｂの少なくとも一方へのアクセスであると判断すると、予兆アクセス又は個人情報アクセスを検知する処理を行う。

【００５３】

そして、ＳＱＬ処理部２０は、ＳＱＬ問合せを実行する実行プランを生成する（ステップＳ５）。ＳＱＬ処理部２０は、クエリ実行の際に、アクセスリスクを評価し、評価結果に基づいてアラートの出力等の対応処理を行う。

【００５４】

そして、ＳＱＬ処理部２０は、不正アクセスでない場合には、問合せを実行するクエリ実行処理を行い（ステップＳ６）、問合せ結果を通知する（ステップＳ７）。ＳＱＬ処理部２０は、正常アクセスの問合せ結果を通知する際にデータの秘匿化を行う。

【００５５】

このように、ＳＱＬ処理部２０は、意味解析を行う際に、予兆アクセス又は個人情報アクセスを検知することで、個人情報の漏洩を防ぐことができる。

【００５６】

次に、検知処理のフローについて説明する。ここで、検知処理とは、ＳＱＬによる問合せが準個人情報テーブル１１ａと関連テーブル１１ｂの少なくとも一方への予兆アクセス又は個人情報アクセスを検知する処理である。図７は、検知処理のフローを示すフローチャートである。

【００５７】

図７に示すように、ＳＱＬ処理部２０は、メタ情報記憶部１２から、アクセス対象テーブルの属性を取得し（ステップＳ１１）、ＳＱＬ問合せが準個人情報テーブル１１ａと関連テーブル１１ｂを結合して検索するか否かを判定する（ステップＳ１２）。そして、ＳＱＬ問合せが準個人情報テーブル１１ａと関連テーブル１１ｂを結合して検索する場合には、ＳＱＬ処理部２０は、ＳＱＬ問合せを個人情報アクセスと判断する（ステップＳ１３）。

【００５８】

一方、ＳＱＬ問合せが準個人情報テーブル１１ａと関連テーブル１１ｂを結合した検索でない場合には、ＳＱＬ処理部２０は、ＳＱＬ問合せが準個人情報テーブル１１ａ又は関連テーブル１１ｂを結合キーを条件に検索するか否かを判定する（ステップＳ１４）。そして、ＳＱＬ問合せが準個人情報テーブル１１ａ又は関連テーブル１１ｂを結合キーを条件に検索する場合には、ＳＱＬ処理部２０は、ＳＱＬ問合せを個人情報アクセスと判断する（ステップＳ１３）。

【００５９】

一方、ＳＱＬ問合せが準個人情報テーブル１１ａ又は関連テーブル１１ｂの結合キーを条件にした検索でない場合は、ＳＱＬ処理部２０は、ＳＱＬ問合せが準個人情報テーブル１１ａ又は関連テーブル１１ｂから結合キーを検索するかを判定する（ステップＳ１５）。そして、ＳＱＬ問合せが準個人情報テーブル１１ａ又は関連テーブル１１ｂから結合キーを検索する場合には、ＳＱＬ処理部２０は、ＳＱＬ問合せを予兆アクセスと判断する（ステップＳ１６）。

【００６０】

一方、ＳＱＬ問合せが準個人情報テーブル１１ａ又は関連テーブル１１ｂからの結合キーの検索でない場合には、ＳＱＬ処理部２０は、ＳＱＬ問合せを個人情報アクセスにも予兆アクセスにも該当せずと判断する（ステップＳ１７）。

【００６１】

このように、ＳＱＬ処理部２０は、アクセス対象テーブルの属性とアクセス対象テーブルへの検索内容に基づいて予兆アクセス及び個人情報アクセスを検知するので、個人情報の漏洩を防ぐことができる。なお、ステップＳ１２、ステップＳ１４及びステップＳ１５の判定は他の順番で行われてもよい。例えば、ステップＳ１５、ステップＳ１４、ステップＳ１２の順に判定が行われてもよい。

【００６２】

次に、リスク評価及びアラート発信処理のフローについて説明する。図８は、リスク評価及びアラート発信処理のフローを示すフローチャートである。

【００６３】

図８に示すように、ＳＱＬ処理部２０は、ＳＱＬ問合せを個人情報アクセスと判断したか否かを判定し（ステップＳ２１）、ＳＱＬ問合せを個人情報アクセスと判断した場合には、ＳＱＬ問合せが正常な業務のポリシーに即しているかを判定する（ステップＳ２２）。そして、ＳＱＬ処理部２０は、ＳＱＬ問合せが正常な業務のポリシーに即していない場合は、ＳＱＬ問合せを不正アクセスと判断し（ステップＳ２３）、監査ログ記憶部１４へアラートを出力し（ステップＳ２４）、コネクションを強制切断する（ステップＳ２５）。

【００６４】

一方、ＳＱＬ問合せが正常な業務のポリシーに即している場合には、ＳＱＬ処理部２０は、ＳＱＬ問合せを正常アクセスと判断する（ステップＳ２６）。また、ＳＱＬ問合せを個人情報アクセスでないと判断した場合には、ＳＱＬ処理部２０は、ＳＱＬ問合せを予兆アクセスと判断したか否かを判定する（ステップＳ２７）。そして、ＳＱＬ処理部２０は、ＳＱＬ問合せを予兆アクセスと判断した場合には、要監視と判断し（ステップＳ２８）、監査ログ記憶部１４へアラートを出力する（ステップＳ２９）。

【００６５】

このように、ＳＱＬ処理部２０は、不正アクセスに対してコネクションを強制切断するので、個人情報の漏洩を防ぐことができる。

【００６６】

次に、データ秘匿化処理のフローについて説明する。図９は、データ秘匿化処理のフローを示すフローチャートである。図９に示すように、ＳＱＬ処理部２０は、正常アクセスと判断したか否かを判定し（ステップＳ３１）、正常アクセスと判断した場合には、データの秘匿化を行う（ステップＳ３２）。

【００６７】

このように、ＳＱＬ処理部２０は、個人情報が特定される情報を提供する場合にデータを秘匿化することで、個人情報の漏洩を防ぐことができる。

【００６８】

上述してきたように、実施例では、属性情報作成部１３が、準個人情報テーブル１１ａと結合キーで結合される関連テーブル１１ｂを特定し、テーブル属性情報１２ａに登録する。そして、関係判断部２１が、テーブル属性情報１２ａを参照して、ＳＱＬ問合せが準個人情報テーブル１１ａと関連テーブル１１ｂの少なくとも一方へのアクセスであるか否かを判断する。そして、関係判断部２１がＳＱＬ問合せが準個人情報テーブル１１ａと関連テーブル１１ｂの少なくとも一方へのアクセスであると判断すると、検知部２２が、ＳＱＬ問合せが予兆アクセス又は個人情報アクセスであるか否かを判定する。そして、リスク評価部２３が、ポリシー情報１２ｂに基づいて、個人情報アクセスが正常アクセスであるか不正アクセスであるかを判定する。そして、アラート発信部２４が、予兆アクセスに対してはアラートの出力を行い、不正アクセスに対してはアラートの出力とコネクションの強制切断を行う。したがって、ＤＢＭＳ１は、準個人情報テーブル１１ａと関連テーブル１１ｂを組み合わせることで特定される個人情報の漏洩を防ぐことができる。

【００６９】

また、実施例では、ＳＱＬ問合せが準個人情報テーブル１１ａの情報と関連テーブル１１ｂの情報を結合キーで組み合わせる検索である場合に、検知部２２は、ＳＱＬ問合せが個人情報アクセスであると判定する。あるいは、ＳＱＬ問合せが準個人情報テーブル１１ａ又は関連テーブル１１ｂから結合キーを用いて情報を検索する場合に、検知部２２は、ＳＱＬ問合せが個人情報アクセスであると判定する。また、ＳＱＬ問合せが準個人情報テーブル１１ａ又は関連テーブル１１ｂから結合キーを検索する場合に、検知部２２は、ＳＱＬ問合せが予兆アクセスであると判定する。したがって、ＤＢＭＳ１は、個人情報アクセスと予兆アクセスを検知することができる。

【００７０】

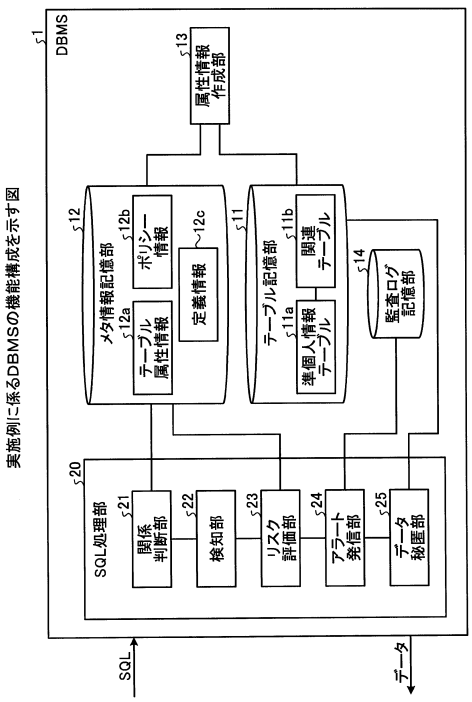
また、実施例では、リスク評価部２３が、ポリシー情報１２ｂに基づいて個人情報アクセスが正常アクセスであるか否かを判定するので、ＤＢＭＳ１は、ポリシーに沿ったアクセスを許可することができる。

【００７１】
　また、実施例では、ポリシー情報１２ｂには、アクセス時間、業務アプリケーション名及びクライアントマシンの情報が含まれるので、リスク評価部２３は、ポリシーに沿った正常アクセスを特定することができる。
【００７２】
　また、実施例では、属性情報作成部１３は、複数のテーブルの中から氏名及び生年月日を含むテーブルを準個人情報テーブル１１ａとして特定するので、準個人情報テーブル１１ａを正確に特定することができる。
【００７３】
　また、実施例では、属性情報作成部１３は、定義情報１２ｃから関連テーブル１１ｂに設定された参照制約の情報を取り出して、準個人情報テーブル１１ａと関連テーブル１１ｂの関連を特定するので、関連テーブル１１ｂを正確に特定することができる。
【００７４】
　なお、実施例では、ＤＢＭＳ１について説明したが、ＤＢＭＳ１の機能は、データベース管理プログラムをコンピュータで実行することで実現される。そこで、データベース管理プログラムを実行するコンピュータについて説明する。
【００７５】
　図１０は、実施例に係るデータベース管理プログラムを実行するコンピュータのハードウェア構成を示す図である。図１０に示すように、コンピュータ５０は、メインメモリ５１と、ＣＰＵ（Central Processing Unit）５２と、ＬＡＮ（Local Area Network）インタフェース５３と、ＨＤＤ（Hard Disk Drive）５４とを有する。また、コンピュータ５０は、スーパーＩＯ（Input Output）５５と、ＤＶＩ（Digital Visual Interface）５６と、ＯＤＤ（Optical Disk Drive）５７とを有する。
【００７６】
　メインメモリ５１は、プログラムやプログラムの実行途中結果等を記憶するメモリである。ＣＰＵ５２は、メインメモリ５１からプログラムを読み出して実行する中央処理装置である。ＣＰＵ５２は、メモリコントローラを有するチップセットを含む。
【００７７】
　ＬＡＮインタフェース５３は、コンピュータ５０をＬＡＮ経由で他のコンピュータに接続するためのインタフェースである。ＨＤＤ５４は、プログラムやデータを格納するディスク装置であり、スーパーＩＯ５５は、マウスやキーボード等の入力装置を接続するためのインタフェースである。ＤＶＩ５６は、液晶表示装置を接続するインタフェースであり、ＯＤＤ５７は、ＤＶＤの読み書きを行う装置である。
【００７８】
　ＬＡＮインタフェース５３は、ＰＣＩエクスプレス（ＰＣＩｅ）によりＣＰＵ５２に接続され、ＨＤＤ５４及びＯＤＤ５７は、ＳＡＴＡ（Serial Advanced Technology Attachment）によりＣＰＵ５２に接続される。スーパーＩＯ５５は、ＬＰＣ（Low Pin Count）によりＣＰＵ５２に接続される。
【００７９】
　そして、コンピュータ５０において実行されるデータベース管理プログラムは、コンピュータ５０により読み出し可能な記録媒体の一例であるＤＶＤに記憶され、ＯＤＤ５７によってＤＶＤから読み出されてコンピュータ５０にインストールされる。あるいは、データベース管理プログラムは、ＬＡＮインタフェース５３を介して接続された他のコンピュータシステムのデータベース等に記憶され、これらのデータベースから読み出されてコンピュータ５０にインストールされる。そして、インストールされたデータベース管理プログラムは、ＨＤＤ５４に記憶され、メインメモリ５１に読み出されてＣＰＵ５２によって実行される。
【符号の説明】
【００８０】
　１　ＤＢＭＳ

１１　テーブル記憶部
１１ａ　準個人情報テーブル
１１ｂ　関連テーブル
１２　メタ情報記憶部
１２ａ　テーブル属性情報
１２ｂ　ポリシー情報
１２ｃ　定義情報
１３　属性情報作成部
１４　監査ログ記憶部
２０　ＳＱＬ処理部
２１　関係判断部
２２　検知部
２３　リスク評価部
２４　アラート発信部
２５　データ秘匿部
５０　コンピュータ
５１　メインメモリ
５２　ＣＰＵ
５３　ＬＡＮインタフェース
５４　ＨＤＤ
５５　スーパーＩＯ
５６　ＤＶＩ
５７　ＯＤＤ

【図面】

【図１】



【図２】

テーブル属性情報とポリシー情報の例を示す図

(a)テーブル属性情報（メタ情報）

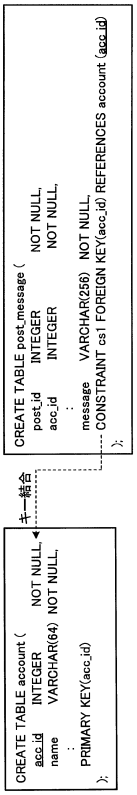
テーブル名	属性	準個人情報テーブル名	結合キー
account	準個人情報テーブル	-	acc_id
post_message	関連テーブル	account	acc_id
history	非対象テーブル	-	-

(b)ポリシー情報（メタ情報）

準個人情報テーブル名	種別	ポリシー
default	アクセス時間	00:00:00 - 05:59:59
account	アクセス時間	00:00:00 - 06:29:59
	業務アプリケーション名	apl01
	クライアントマシン	192.33.44.*

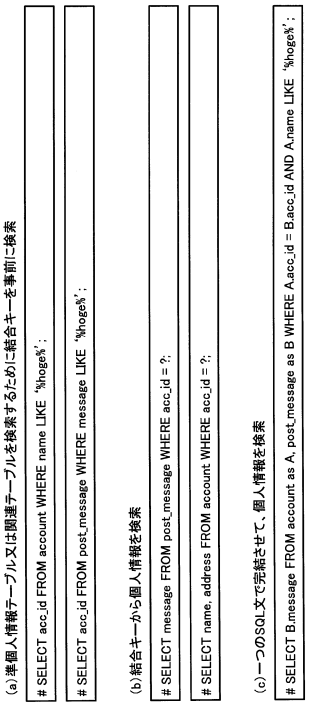
【図３】

参照制約の一例を示す図



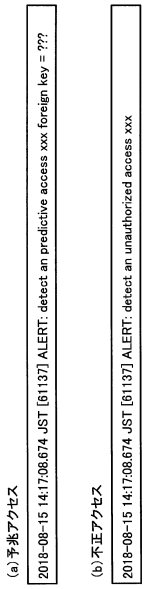
【図４】

予兆アクセス及び個人情報アクセスの例を示す図



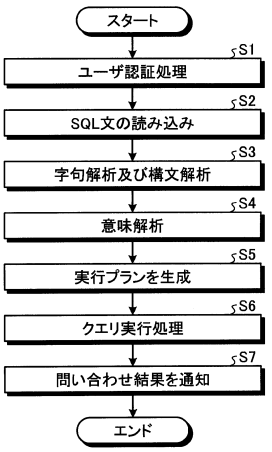
【図５】

アラームの例を示す図



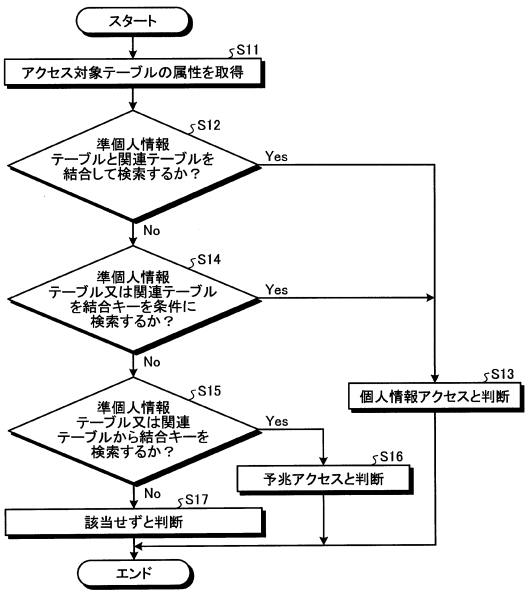
【図６】

SQL問合せ処理のフローを示すフローチャート



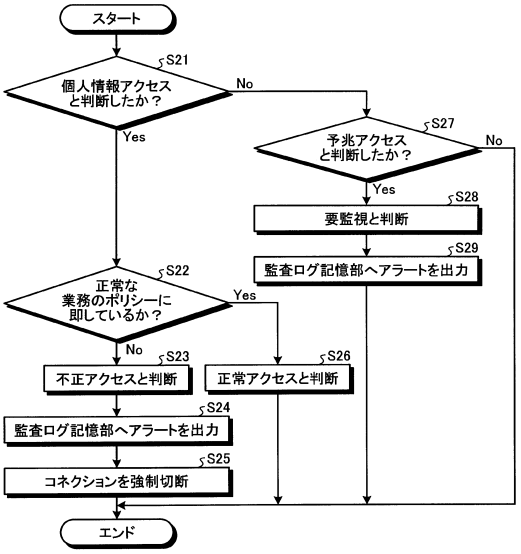
【図７】

検知処理のフローを示すフローチャート



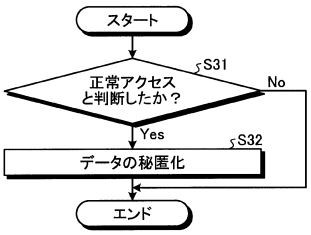
【図８】

リスク評価及びアラート発信処理のフローを示すフローチャート



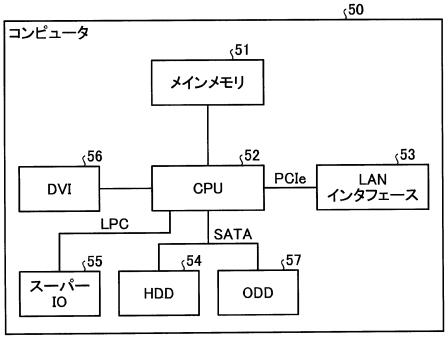
【図９】

データ秘匿化処理のフローを示すフローチャート



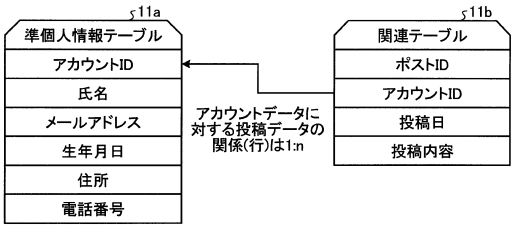
【図１０】

実施例に係るデータベース管理プログラムを実行するコンピュータのハードウェア構成を示す図



【図１１】

準個人情報を説明するための図



フロントページの続き

(56)参考文献 特開２００５－１８２７０７（ＪＰ，Ａ）
特開２００２－３１２２２０（ＪＰ，Ａ）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／６２