(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6183034号
(P6183034)
(45)発行日　平成29年8月23日(2017.8.23)　(24)登録日　平成29年8月4日(2017.8.4)

(51)Int.Cl.　F I
G06F 21/62 (2013.01)　G06F 21/62 327

請求項の数 8 (全 23 頁)

(21)出願番号　特願2013-157734(P2013-157734)
(22)出願日　平成25年7月30日(2013.7.30)
(65)公開番号　特開2015-28698(P2015-28698A)
(43)公開日　平成27年2月12日(2015.2.12)
審査請求日　平成28年4月5日(2016.4.5)

(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　100104190
弁理士　酒井　昭徳
(72)発明者　磯村　則一
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
(72)発明者　齊藤　嵩
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
(72)発明者　伊藤　尚洋
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
最終頁に続く

(54)【発明の名称】アクセス制御プログラム、アクセス制御方法およびシステム

(57)【特許請求の範囲】
【請求項１】
コンピュータに、
アクセス権限が有効となる時間帯を設定可能なデータに対するアクセスを許可する時間帯を示す許可時間帯に基づいて、前記データに対するアクセスを許可するか否かを示すアクセス許可情報を更新し、
前記データの識別子と、前記データの許可時間帯が設定される許可時間情報との対応関係を示す対応情報から、前記データの識別子に対応する前記許可時間情報を特定し、特定した前記許可時間情報の前記アクセス許可情報に基づいて、前記データに対するアクセスを制御する、
処理を実行させることを特徴とするアクセス制御プログラム。
【請求項２】
前記更新する処理は、
前記許可時間帯と前記アクセス許可情報とを対応付けて表す許可時間情報を有する許可時間表に基づいて、前記アクセス許可情報を前記許可時間帯に応じて更新し、
前記制御する処理は、
前記データの識別子と、前記許可時間表の中で前記データの許可時間帯が設定される前記許可時間情報との対応関係を示す対応情報から、前記データの識別子に対応する前記許可時間情報を特定し、特定した前記許可時間情報の前記アクセス許可情報に基づいて、前記データに対するアクセスを制御することを特徴とする請求項１に記載のアクセス制御プ

ログラム。
【請求項３】
前記更新する処理は、
前記許可時間帯の開始時刻に、当該許可時間帯に対応する前記アクセス許可情報をアクセス許可に更新し、前記許可時間帯の終了時刻に、当該許可時間帯に対応する前記アクセス許可情報をアクセス不許可に更新し、
前記制御する処理は、
前記アクセス許可情報がアクセス許可である場合に、前記データに対するアクセスを許可することを特徴とする請求項２に記載のアクセス制御プログラム。
【請求項４】
前記更新する処理は、
現在時刻を取得し、前記許可時間帯の開始時刻および終了時刻のうちの、取得した前記現在時刻に、最も近い時刻を抽出し、前記抽出した時刻になった場合、前記アクセス許可情報を更新することを特徴とする請求項３に記載のアクセス制御プログラム。
【請求項５】
前記更新する処理は、
前記アクセス許可情報が更新された場合、および前記許可時間帯が変更された場合に実行されることを特徴とする請求項４に記載のアクセス制御プログラム。
【請求項６】
前記コンピュータに、
ユーザの識別子と前記データの識別子との対応関係を示す対応情報から、アクセス要求元のユーザの識別子に対応する前記データの識別子を特定する処理を実行させ、
前記制御する処理は、
特定した前記データの識別子と、前記許可時間表の中で前記データの許可時間帯が設定される前記許可時間情報との対応関係を示す対応情報が設定されている場合に、当該対応情報から前記データの識別子に対応する前記許可時間情報を特定することを特徴とする請求項２～５のいずれか一つに記載のアクセス制御プログラム。
【請求項７】
コンピュータが、
アクセス権限が有効となる時間帯を設定可能なデータに対するアクセスを許可する時間帯を示す許可時間帯に基づいて、前記データに対するアクセスを許可するか否かを示すアクセス許可情報を更新し、
前記データの識別子と、前記データの許可時間帯が設定される許可時間情報との対応関係を示す対応情報から、前記データの識別子に対応する前記許可時間情報を特定し、特定した前記許可時間情報の前記アクセス許可情報に基づいて、前記データに対するアクセスを制御する、
処理を実行することを特徴とするアクセス制御方法。
【請求項８】
アクセス権限が有効となる時間帯を設定可能なデータに対するアクセスを許可する時間帯を示す許可時間帯に基づいて、前記データに対するアクセスを許可するか否かを示すアクセス許可情報を更新する更新部と、
前記データの識別子と、前記データの許可時間帯が設定される許可時間情報との対応関係を示す対応情報から、前記データの識別子に対応する前記許可時間情報を特定し、特定した前記許可時間情報の前記アクセス許可情報に基づいて、前記データに対するアクセスを制御する制御部と、
を有することを特徴とするシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、アクセス制御プログラム、アクセス制御方法およびシステムに関する。

【背景技術】
【０００２】
データベースに対するアクセスは、例えば、主体と客体との関係において定義される権限で管理される。主体は、アクセスを管理するシステムによって認証されるユーザである。ユーザの認証には、例えば、ユーザ識別文字列とパスワード文字列の一致判定等の様々な認証手段が使われる。客体は、アクセス対象のデータベース実体である。客体は、例えば、テーブルを構成するカラムにより構造化され、特定の客体を対象としないデータベース管理システムに対する操作コマンドにより抽象化されることがある。
【０００３】
アクセス権限管理は、多くのシステムで行われるシステム運用であり、従来のユーザ識別文字列とパスワード文字列だけでは不十分な場合がある。例えば、夜間のデータベースへのアクセスを完全に抑止するために、夜間はサーバを止めるなどの運用が行われる場合があるため、アクセス権限に有効な時間（時刻）という考え方を導入することがある。
【０００４】
アクセス権限管理に、権限の有効な時間の概念を導入するためには、例えば、テーブルアクセス時に現在時刻を毎回取得して判断することになる。また、データベースの場合、複数のテーブルに対して結合を指示するクエリー等が指定されることがあるため、アクセス対象テーブル単位に時刻確認を含むアクセス権限チェックを行うことになる。
【０００５】
関連する先行技術としては、例えば、クエリーを発行したプロセスに設定されたユーザ名と、クエリーにより指定されたデータベース名、ファイル名および項目名と、クエリーが発行された時刻に基づいて、データベースに対する参照の可否を決定するものがある。また、アクセス属性ファイルに時間情報を含むアクセス属性を設定しておき、アクセス対象ファイルのアクセス時に必ず起動されるファイルアクセス機能によってアクセス属性ファイルを参照し、時間情報を含めたアクセス許可の判定を行う技術がある。また、ファイルへのアクセス要求があった場合、アクセス要求に含まれる情報と、アクセス管理テーブルに登録されたユーザＩＤ、パスワード、許可時間帯および端末ＩＤを基にアクセス可否を判定する技術がある。また、前回の走査時以降プロセッサによってアクセスされていないページフレームを解放した後、スリープ状態となるページアウトデーモンプロセスを所定の間隔でディスパッチする技術がある。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開平１０－２８９１３４号公報
【特許文献２】特開平８－３１４７８６号公報
【特許文献３】特開２０００－２５９５６７号公報
【特許文献４】特開平９－２６９９０２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
しかしながら、従来技術によれば、データベースシステムのアクセス権限管理に時間の概念を導入すると、データアクセスにかかる処理負荷が増大する。例えば、データベースサーバがデータにアクセスする度に、ＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）のシステムコールを呼び出して現在時刻を取得し、許可された時間帯であるかをチェックする場合、アクセス回数に比例してＯＳのシステムコール呼び出し回数が増加し、データアクセスにかかる処理負荷が増大する。
【０００８】
一つの側面では、本発明は、時間帯に基づくアクセス制御にかかる処理負荷の増大を抑制することができるアクセス制御プログラム、アクセス制御方法およびシステムを提供することを目的とする。

【課題を解決するための手段】
【０００９】
本発明の一側面によれば、アクセス権限が有効となる時間帯を設定可能なデータに対するアクセスを許可する時間帯を示す許可時間帯に基づいて、前記データに対するアクセスを許可するか否かを示すアクセス許可情報を更新し、前記アクセス許可情報に基づいて、前記データに対するアクセスを制御するアクセス制御プログラム、アクセス制御方法およびシステムが提案される。
【発明の効果】
【００１０】
本発明の一態様によれば、時間帯に基づくアクセス制御にかかる処理負荷の増大を抑制することができるという効果を奏する。
【図面の簡単な説明】
【００１１】
【図１】図１は、実施の形態１にかかるアクセス制御方法の一実施例を示す説明図である。
【図２】図２は、システム２００のシステム構成例を示す説明図である。
【図３】図３は、データベースサーバ１０１のハードウェア構成例を示すブロック図である。
【図４】図４は、権限設定情報４００の記憶内容の一例を示す説明図である。
【図５】図５は、データベースサーバ１０１の機能的構成例を示すブロック図である。
【図６】図６は、権限設定情報４００のユーザ登録処理手順の一例を示すフローチャートである。
【図７】図７は、図６のフローチャートにより登録されたユーザ情報４０１の一例を示す説明図である。
【図８】図８は、権限設定情報４００のユーザ権限登録処理手順の一例を示すフローチャートである。
【図９】図９は、図８のフローチャートにより登録されたユーザＡのユーザ権限の一例を示す説明図である。
【図１０】図１０は、権限設定情報４００のユーザ許可時間帯登録処理手順の一例を示すフローチャートである。
【図１１】図１１は、図１０のフローチャートにより登録されたユーザＡの情報の一例を示す説明図である。
【図１２】図１２は、アクセス許可情報の更新処理手順の一例を示すフローチャートである。
【図１３】図１３は、データベースサーバ１０１によるアクセス権限の検査処理手順の一例を示すフローチャートである。
【図１４】図１４は、実施の形態２にかかる権限設定情報４００の記憶内容の一例を示す説明図である。
【図１５】図１５は、実施の形態２にかかる権限設定情報４００のユーザ許可時間帯登録処理手順の一例を示すフローチャートである。
【図１６】図１６は、図１５のフローチャートにより登録されたユーザＡとユーザＢの情報の一例を示す説明図である。
【図１７】図１７は、実施の形態３にかかるデータベースサーバ１０１の機能的構成例を示すブロック図である。
【図１８】図１８は、実施の形態３にかかるデータベースサーバ１０１によるアクセス権限の検査処理手順の一例を示すフローチャートである。
【発明を実施するための形態】
【００１２】
以下に図面を参照して、本発明にかかるアクセス制御プログラム、アクセス制御方法およびシステムの実施の形態を詳細に説明する。

【００１３】
（実施の形態１）
（アクセス制御方法の一実施例）
図１は、実施の形態１にかかるアクセス制御方法の一実施例を示す説明図である。図１において、データベースサーバ１０１は、クライアント端末１０２からデータベースへのアクセス要求（クエリー）、例えばＳＱＬ（Ｓｔｒｕｃｔｕｒｅｄ　Ｑｕｅｒｙ　Ｌａｎｇｕａｇｅ）文を受け付け、クライアント端末１０２にクエリーの結果を返答するコンピュータである。
【００１４】
クライアント端末１０２は、ユーザ操作によりクエリーを発行するコンピュータである。また、データベースは、複数のアプリケーションやユーザによって共有されるデータを記憶する。例えば、リレーショナルデータベースは、データの集まりを、カラムを有するテーブルの形で表現する。複数のアプリケーションやユーザは、テーブル間に関連を設定することでテーブルを連結させて、データの検索および更新を行うことができる。
【００１５】
本実施の形態では、データベースのアクセス権限管理機構を拡張して、アクセス権限に時間の概念を導入する。具体的には、データベースのデータに、アクセス権限が有効となる時間帯を設定する。ただし、以下の説明では、データベースのデータの一例として、データベースのテーブルを例に挙げて説明する。時間に関するアクセス権限は、剥奪操作が行われなくても、規定された時間外になると無効になる。
【００１６】
データベースサーバ１０１は、ＳＱＬ文のデータ・アクセス・プラン決定時（ＳＱＬ文の翻訳時）に、ＳＱＬ文で指定されたテーブルのアクセス権限を検査し、時間に関するアクセス権限の検査をテーブルアクセス時に実施する。以下、データベースサーバ１０１のアクセス制御処理例について説明する。
【００１７】
（１）データベースサーバ１０１は、権限情報テーブル１１０に、テーブルに対するアクセスを許可する時間帯を示す許可時間帯１１１と、現時刻において、当該テーブルに対するアクセスを許可するか否かを示すアクセス許可情報１１２を付与する。権限情報テーブル１１０は、例えば、ユーザごとに設けられる。
【００１８】
また、アクセス許可情報１１２は、例えば、テーブルに対するアクセス許否を示すフラグ情報である。以下の説明では、テーブルに対するアクセスを許可することを示すアクセス許可情報１１２を「アクセス許可（○）」と表記し、テーブルに対するアクセスを許可しないことを示すアクセス許可情報１１２を「アクセス不許可（×）」と表記する場合がある。アクセス許可情報１１２は、初期状態ではアクセス不許可（×）である。
【００１９】
図１の例では、ユーザＡの権限情報テーブル１１０にテーブル（１）、テーブル（２）、・・・、テーブル（ｎ）の許可時間帯１１１が定義されている。具体的には、例えば、テーブル（１）は、「９：００～１７：００」の時間帯だけアクセスが許可され、テーブル（２）は、「１８：００～２２：００」の時間帯だけアクセスが許可され、テーブル（ｎ）は、「２２：００～２４：００」の時間帯だけアクセスが許可される。現時刻において、テーブル（１）、テーブル（２）、・・・、テーブル（ｎ）のアクセス許可情報１１２は、すべてアクセス不許可（×）である。
【００２０】
（２）データベースサーバ１０１は、権限情報テーブル１１０を更新する。具体的には、例えば、データベースサーバ１０１は、バックグラウンドで、テーブルに定義された許可時間帯１１１の開始時刻になった場合、当該テーブルのアクセス許可情報１１２をアクセス許可（○）に更新する。また、データベースサーバ１０１は、バックグラウンドで、テーブルに定義された許可時間帯１１１の終了時刻になった場合、当該テーブルのアクセ

ス許可情報１１２をアクセス不許可（×）に更新する。

【００２１】

図１の例では、データベースサーバ１０１は、例えば、「９：００」になるとテーブル（１）のアクセス許可情報１１２をアクセス許可（○）に更新する。また、データベースサーバ１０１は、例えば、「１７：００」になるとテーブル（１）のアクセス許可情報１１２をアクセス不許可（×）に更新する。

【００２２】

（３）データベースサーバ１０１は、クライアント端末１０２からデータベースに対するアクセス要求を受け付ける。ここでは、データベースサーバ１０１が、「９：００～１７：００」の時間帯に、ユーザＡが使用するクライアント端末１０２から、データベース内のテーブル（１）に対するアクセス要求を受け付けた場合を想定する。

【００２３】

（４）データベースサーバ１０１は、クライアント端末１０２を使用するユーザの権限情報テーブル１１０を参照することにより、データベース内のテーブルに対するアクセスを制御する。具体的には、例えば、データベースサーバ１０１は、テーブルのアクセス許可情報１１２がアクセス不許可（×）である場合、許可時間外のためアクセスを不許可として、エラー復帰する。一方、テーブルのアクセス許可情報１１２がアクセス許可（○）である場合、データベースサーバ１０１は、アクセスを許可し、データアクセスを続行する。図１の例では、データベースサーバ１０１は、ユーザＡの権限情報テーブル１１０を参照して、テーブル（１）のアクセス許可情報１１２がアクセス許可（○）であるため、テーブル（１）に対するアクセスを許可する。

【００２４】

このように、データベースサーバ１０１によれば、テーブルの許可時間帯１１１に基づいて、当該テーブルに対するアクセスを許可するか否かを示すアクセス許可情報１１２を更新することができる。また、データベースサーバ１０１によれば、クライアント端末１０２からアクセス要求を受け付けた時は、アクセス先のテーブルのアクセス許可情報１１２に基づいて、当該テーブルに対するアクセスを制御することができる。これにより、テーブルへのアクセス時に毎回現在時刻の取得を行うことなく時間帯に基づくアクセス制御を行うことが可能となり、大きなオーバーヘッドを持ち込むことなく、アクセス権限に時間の概念を導入することができる。

【００２５】

（システム２００のシステム構成例）

図２は、システム２００のシステム構成例を示す説明図である。図２において、システム２００は、データベースサーバ１０１と、クライアント端末１０２と、管理端末２０３と、データベース２１０と、を含む。システム２００において、データベースサーバ１０１、クライアント端末１０２および管理端末２０３は、有線または無線のネットワーク２２０を介して接続される。ネットワーク２２０は、例えば、ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）、ＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）、インターネットなどである。

【００２６】

データベースサーバ１０１は、データベース２１０にアクセス可能なコンピュータである。データベースサーバ１０１は、例えば、クライアント端末１０２からデータの検索要求を受信すると、データベース２１０からデータをメモリ（例えば、後述の図３に示すメモリ３０２）に読み込む。そして、データベースサーバ１０１は、メモリに読み込まれたデータに対して検索を行い、その検索結果をクライアント端末１０２に送信する。

【００２７】

クライアント端末１０２は、システム２００のユーザが使用するコンピュータである。管理端末２０３は、システム２００の管理者が使用するコンピュータである。具体的には、例えば、クライアント端末１０２は、ＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）、ノートＰＣ、スマートフォン、携帯電話機、タブレット型ＰＣなどである。

【００２８】
（データベースサーバ１０１のハードウェア構成例）
図３は、データベースサーバ１０１のハードウェア構成例を示すブロック図である。図３において、データベースサーバ１０１は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）３０１と、メモリ３０２と、Ｉ／Ｆ（Ｉｎｔｅｒｆａｃｅ）３０３と、磁気ディスクドライブ３０４と、磁気ディスク３０５と、を有する。また、各構成部は、バス３００によってそれぞれ接続される。
【００２９】
ここで、ＣＰＵ３０１は、データベースサーバ１０１の全体の制御を司る。メモリ３０２は、例えば、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）およびフラッシュＲＯＭなどを有する。具体的には、例えば、フラッシュＲＯＭやＲＯＭが各種プログラムを記憶し、ＲＡＭがＣＰＵ３０１のワークエリアとして使用される。メモリ３０２に記憶されるプログラムは、ＣＰＵ３０１にロードされることで、コーディングされている処理をＣＰＵ３０１に実行させる。
【００３０】
Ｉ／Ｆ３０３は、通信回線を通じてネットワーク２２０に接続され、ネットワーク２２０を介して他のコンピュータ（例えば、図２に示したクライアント端末１０２および管理端末２０３）に接続される。そして、Ｉ／Ｆ３０３は、ネットワーク２２０と内部のインターフェースを司り、他のコンピュータからのデータの入出力を制御する。Ｉ／Ｆ３０３には、例えば、モデムやＬＡＮアダプタなどを採用することができる。
【００３１】
磁気ディスクドライブ３０４は、ＣＰＵ３０１の制御にしたがって磁気ディスク３０５に対するデータのリード／ライトを制御する。磁気ディスク３０５は、磁気ディスクドライブ３０４の制御で書き込まれたデータを記憶する。
【００３２】
なお、データベースサーバ１０１は、上述した構成部のほか、例えば、ＳＳＤ（Ｓｏｌｉｄ Ｓｔａｔｅ Ｄｒｉｖｅ）、キーボード、マウス、ディスプレイなどを有することにしてもよい。また、図２に示したクライアント端末１０２および管理端末２０３についても、上述したデータベースサーバ１０１と同様のハードウェア構成例により実現することができる。
【００３３】
（権限設定情報４００の記憶内容）
つぎに、データベースサーバ１０１が用いる権限設定情報４００の記憶内容について説明する。権限設定情報４００は、例えば、図３に示したメモリ３０２、磁気ディスク３０５などの記憶装置に記憶される。
【００３４】
図４は、権限設定情報４００の記憶内容の一例を示す説明図である。図４において、権限設定情報４００は、ユーザ情報４０１（例えば、ユーザ情報４０１－１，４０１－２）と権限情報テーブル４０２（例えば、権限情報テーブル４０２－１，４０２－２）とを含む構成である。
【００３５】
ユーザ情報４０１は、ユーザ名、テーブル数、および権限情報テーブルポインタのフィールドを有し、各フィールドに情報を設定することにより、ユーザごとのテーブルに関する情報を記憶する。
【００３６】
ここで、ユーザ名は、データベースサーバ１０１にアクセスする権限を有するユーザを一意に識別するユーザの識別子である。テーブル数は、ユーザに対する権限が規定されたテーブルの数を示す。権限情報テーブルポインタは、ユーザ情報４０１と、当該ユーザの権限が設定された権限情報テーブル４０２との対応関係を示す対応情報である。権限情報テーブルポインタは、例えば、権限情報テーブル４０２のメモリ３０２上のアドレスを示

すポインタである。

【００３７】

例えば、ユーザ情報４０１－１は、ユーザ名にユーザＡ、テーブル数に３、権限情報テーブルポインタに権限情報テーブル４０２－１へのポインタを記憶している。また、ユーザ情報４０１－２は、ユーザ名にユーザＢ、テーブル数に２、権限情報テーブルポインタに権限情報テーブル４０２－２へのポインタを記憶している。

【００３８】

権限情報テーブル４０２は、テーブル名、権限、許可時間帯、およびアクセス許可情報のフィールドを有し、各フィールドに情報を設定することにより、テーブルごとに、ユーザの権限に関する情報を記憶する。

【００３９】

ここで、テーブル名は、データベース２１０に記憶されるテーブルを一意に識別するテーブルの識別子である。権限は、権限情報テーブル４０２と対応しているユーザ情報４０１におけるユーザに、当該テーブルに対して許可されている権限を示す。権限には、例えば、参照、更新等が存在する。許可時間帯は、ユーザに当該テーブルに対してアクセスを許可する時間帯を示す。例えば、許可する時間帯は、許可開始時刻と許可終了時刻で示すことができる。アクセス許可情報は、現時刻において、ユーザに当該テーブルに対してアクセスを許可するか否かを示す。例えば、アクセス許可情報に、「○」が設定された場合、アクセスを許可し、「×」が設定された場合、アクセスを許可しないとすることができる。

【００４０】

例えば、権限情報テーブル４０２－１は、テーブル名として、テーブル（１）からテーブル（３）を有する。権限情報テーブル４０２－１は、ユーザＡがテーブル（１）とテーブル（２）に対して、参照、更新が可能であること、９：００～１７：００の時間帯にアクセスが許可されていること、アクセス許可情報が「○」であり、現時刻において、アクセスが許可されていることを示す。同様に、ユーザＡが、テーブル（３）に対して、参照が可能であること、１８：００～２２：００の時間帯にアクセスが許可されていること、アクセス許可情報が「×」であり、現時刻において、アクセスが許可されていないことを示す。

【００４１】

（データベースサーバ１０１の機能的構成例）

図５は、データベースサーバ１０１の機能的構成例を示すブロック図である。図５において、データベースサーバ１０１は、受付部５０１と、ＳＱＬ翻訳部５０２と、権限検査部５０３と、アクセス許可検査部５０４と、データアクセス部５０５と、権限情報管理部５０６と、権限設定更新部５０７とを含む構成である。各機能部は、具体的には、例えば、図２に示したメモリ３０２、磁気ディスク３０５などの記憶装置に記憶されたプログラムをＣＰＵ３０１に実行させることにより、または、Ｉ／Ｆ３０３により、その機能を実現する。各機能部の処理結果は、例えば、図３に示したメモリ３０２、磁気ディスク３０５などの記憶装置に記憶される。

【００４２】

受付部５０１は、クライアント端末１０２からのデータのアクセス要求を受け付ける機能を有する。例えば、ユーザはＳＱＬ文を実行し、ネットワーク２２０を介してデータベース２１０のデータにアクセスを要求し、受付部５０１は、このデータアクセス要求を受け付ける。

【００４３】

ＳＱＬ翻訳部５０２は、データアクセス要求からデータのアクセス手順を作成する機能を有する。例えば、ＳＱＬ文からデータにアクセスするユーザ名、データアクセスに必要なテーブル名等を抽出する。

【００４４】

権限検査部５０３は、権限情報テーブル４０２の権限フィールドを参照して、ユーザの

テーブルへのアクセス要求の許可および不許可を判断する機能を有する。権限検査部５０３は、アクセス要求を許可と判断した場合、アクセス許可検査部５０４に制御を移し、アクセス要求を不許可と判断した場合、データアクセス要求をエラー終了させる。

【００４５】

例えば、ユーザＡがＳＱＬ文でテーブル（１）に対して参照アクセスを要求した場合、権限検査部５０３は、ユーザＡのテーブル（１）の権限を示す権限情報テーブル４０２－１を参照し、権限に参照が存在するため、アクセス要求を許可と判断する。また、ユーザＡがＳＱＬ文でテーブル（３）に対して更新アクセスを要求した場合、権限検査部５０３は、ユーザＡのテーブル（３）の権限を示す権限情報テーブル４０２－１を参照し、権限に更新が存在しないため、アクセス要求を不許可と判断する。

【００４６】

アクセス許可検査部５０４は、権限情報テーブル４０２のアクセス許可情報を参照して、許可された時間帯であるか否かを判断する機能を有する。アクセス許可検査部５０４は、許可された時間帯であると判断した場合、データアクセス部５０５に制御を移し、許可された時間帯でないと判断した場合、データアクセス要求をエラー終了させる。つまり、アクセス許可検査部５０４は、データアクセス時に毎回、現在時刻を取得することなく、アクセス許可情報の状態で許可された時間帯であるか否かを判断する。

【００４７】

例えば、ユーザＡがＳＱＬ文でテーブル（１）に対して参照アクセスを要求した場合、アクセス許可検査部５０４は、ユーザＡのテーブル（１）のアクセス許可を示す権限情報テーブル４０２－１を参照し、アクセス許可情報が○であるため、許可された時間帯であると判断する。また、ユーザＡがＳＱＬ文でテーブル（３）に対して参照アクセスを要求した場合、アクセス許可検査部５０４は、ユーザＡのテーブル（３）のアクセス許可を示す権限情報テーブル４０２－１を参照し、アクセス許可情報は×であるため、許可された時間帯でないと判断する。

【００４８】

データアクセス部５０５は、ＳＱＬ翻訳部５０２によって作成されたアクセス手順に従ってデータベース２１０にアクセスし、データアクセス結果を受付部５０１に返信する機能を有する。受付部５０１はデータアクセス結果をクライアント端末１０２に送信する。

【００４９】

権限情報管理部５０６は、権限設定情報４００のユーザ情報４０１における、ユーザ名、テーブル数、および権限情報テーブルポインタのフィールドを登録、更新する機能を有する。また、権限情報管理部５０６は、権限設定情報４００の権限情報テーブル４０２における、テーブル名、権限、および許可時間帯を登録、更新する機能を有する。さらに、権限情報管理部５０６は、権限設定情報４００の権限情報テーブル４０２におけるアクセス許可情報を登録する機能を有する。例えば、管理端末２０３から管理者が、データベースサーバ１０１にコマンド操作を行うことにより、登録、更新することができる。

【００５０】

権限設定更新部５０７は、権限設定情報４００の権限情報テーブル４０２におけるアクセス許可情報を許可時間帯に基づいて、定期的に更新する機能を有する。例えば、権限設定更新部５０７は、バックグラウンドで動作するプロセス（デーモン、サービス等）として実現され、データベースシステム起動時、または権限情報が更新時に起動される。例えば、権限情報テーブル４０２－１であった場合、９：００になると、アクセス許可情報を○に更新して、１７：００になると×に更新する。

【００５１】

（権限設定情報の登録および更新）

図６は、権限設定情報４００のユーザ登録処理手順の一例を示すフローチャートである。まず、権限情報管理部５０６は、利用者登録文（ＣＲＥＡＴＥ　ＵＳＥＲ文）とユーザ情報４０１を参照する（ステップＳ６０１）。利用者登録文は例えば、

　　ＣＲＥＡＴＥ　ＵＳＥＲ　ユーザＡ

ＣＲＥＡＴＥ　ＵＳＥＲ　ユーザＢ
ＣＲＥＡＴＥ　ＵＳＥＲ　ユーザＸ
で記述される。

【００５２】
次に、権限情報管理部５０６は、当該ユーザがすでに定義済みかどうか確認する（ステップＳ６０２）。ここで、ユーザが定義済みである場合（ステップＳ６０２：Ｙｅｓ）、ステップＳ６０５に移行し、ユーザが未定義である場合（ステップＳ６０２：Ｎｏ）、ステップＳ６０３に移行する。

【００５３】
ユーザが未定義である場合、権限情報管理部５０６は、利用者登録文を基にユーザ情報４０１にユーザ名を登録する（ステップＳ６０３）。次に、テーブル数、権限情報テーブルポインタをゼロで初期化する（ステップＳ６０４）。一方、ユーザが定義済みである場合、既に定義済みであるため、エラー終了する（ステップＳ６０５）。これにより、本フローチャートによる一連の処理は終了する。本フローチャートを実行することにより、ユーザ情報４０１にユーザ名が登録される。図７は、図６のフローチャートにより登録されたユーザ情報４０１の一例を示す説明図である。

【００５４】
図８は、権限設定情報４００のユーザ権限登録処理手順の一例を示すフローチャートである。まず、権限情報管理部５０６は、権限登録文（ＧＲＡＮＴ文）を基に、当該ユーザ名と合致するユーザ情報４０１を参照する（ステップＳ８０１）。権限登録文は例えば、
ＧＲＡＮＴ　ＳＥＬＥＣＴ　ＯＮ　マスタ表　ＴＯ　ユーザＡ，ユーザＢ，ユーザＸ
ＧＲＡＮＴ　ＩＮＳＥＲＴ　ＯＮ　取引履歴表　ＴＯ　ユーザＡ，ユーザＢ，ユーザＸ
で記述される。

【００５５】
次に、権限情報管理部５０６は、ユーザ情報４０１のテーブル数が０であるかどうか確認する（ステップＳ８０２）。ここで、ユーザ情報４０１のテーブル数が０である場合（ステップＳ８０２：Ｙｅｓ）、ステップＳ８０３に移行し、０でない場合（ステップＳ８０２：Ｎｏ）、ステップＳ８０６に移行する。

【００５６】
ユーザ情報４０１のテーブル数が０である場合、権限情報管理部５０６は、権限情報テーブル４０２を作成し（ステップＳ８０３）、権限登録文で指定された「テーブル名」と「権限」を登録する（ステップＳ８０４）。なお、「許可時間帯」と「アクセス許可情報」には、何も設定しない。次に、権限情報管理部５０６は、ユーザ情報４０１の「テーブル数」と「権限情報テーブルポインタ」を設定する（ステップＳ８０５）。

【００５７】
一方、ユーザ情報４０１のテーブル数が０でない場合、権限情報管理部５０６は、権限登録文を基に、当該テーブル名と合致する権限情報テーブル４０２を参照し（ステップＳ８０６）、当該テーブル名が登録済みの場合、登録済みの「権限」に権限登録文で指定された「権限」を追加し、当該テーブル名が未登録の場合、権限登録文で指定された「テーブル名」「権限」を追加する（ステップＳ８０７）。この場合も、「許可時間帯」と「アクセス許可情報」は、何も設定しない。これにより、本フローチャートによる一連の処理は終了する。本フローチャートを実行することにより、権限情報テーブル４０２にテーブル名および権限が登録される。図９は、図８のフローチャートにより登録されたユーザＡのユーザ権限の一例を示す説明図である。

【００５８】
図１０は、権限設定情報４００のユーザ許可時間帯登録処理手順の一例を示すフローチャートである。まず、権限情報管理部５０６は、権限登録文（ＧＲＡＮＴ文）を基に、当該ユーザ名とテーブル名に合致するユーザ情報４０１、および権限情報テーブル４０２を参照する（ステップＳ１００１）。権限登録文は例えば、

ＧＲＡＮＴ　ＰＥＲＭＩＳＳＩＯＮ＿ＴＩＭＥ　ＴＯ　ユーザＡ　ＯＮ　ＴＡＢＬＥ　マスタ表，取引履歴表　ＷＩＴＨ　ＴＩＭＥ＿ＲＡＮＧＥ　（９：００，１７：００）
ＧＲＡＮＴ　ＰＥＲＭＩＳＳＩＯＮ＿ＴＩＭＥ　ＴＯ　ユーザＢ　ＯＮ　ＴＡＢＬＥ　マスタ表，取引履歴表　ＷＩＴＨ　ＴＩＭＥ＿ＲＡＮＧＥ　（９：００，１７：００）
で記述される。

【００５９】

次に、権限情報管理部５０６は、合致するユーザ名とテーブル名があるかどうか確認する（ステップＳ１００２）。ここで、ユーザ名とテーブル名が存在する場合（ステップＳ１００２：Ｙｅｓ）、ステップＳ１００３に移行し、存在しない場合（ステップＳ１００２：Ｎｏ）、ステップＳ１００５に移行する。

【００６０】

ユーザ名とテーブル名が存在する場合、権限情報管理部５０６は、権限情報テーブル４０２に許可時間帯フィールドに権限登録文に指定された時間帯を設定し、アクセス許可情報をアクセス不許可（×）に設定する（ステップＳ１００３）。その後、権限情報管理部５０６は、権限設定更新部５０７に権限情報テーブル４０２の変更を通知する（ステップＳ１００４）。一方、ユーザ名とテーブル名が存在しない場合、未登録のため、エラー終了する（ステップＳ１００５）。これにより、本フローチャートによる一連の処理は終了する。本フローチャートを実行することにより、権限情報テーブル４０２に許可時間帯およびアクセス許可情報が登録される。図１１は、図１０のフローチャートにより登録されたユーザＡの情報の一例を示す説明図である。

【００６１】

（権限設定更新部５０７によるアクセス許可情報の更新）

図１２は、アクセス許可情報の更新処理手順の一例を示すフローチャートである。まず、権限設定更新部５０７は、権限情報テーブル４０２の許可時間帯の参照を行う（ステップＳ１２０１）。その後、権限設定更新部５０７は、現在時刻を取得し（ステップＳ１２０２）、許可時間帯の開始時刻および終了時刻の中から、最も現在時刻に近い時刻を抽出すると共に、その時刻が許可開始時刻か許可終了時刻かを判断して待避する（ステップＳ１２０３）。権限設定更新部５０７は、現在時刻から抽出した時刻までの時間差を算出し（ステップＳ１２０４）、抽出した時刻までスリープする（ステップＳ１２０５）。例えば、権限設定更新部５０７は、時間差分ｓｌｅｅｐを使用することができる。その後、抽出した時刻に達すると、権限設定更新部５０７は、スリープから解除され、当該許可時間帯のアクセス許可情報を更新する（ステップＳ１２０６）。先に待避した時刻が許可開始時刻である場合、アクセス許可情報を○に更新し、待避した時刻が許可終了時刻である場合、アクセス許可情報を×に更新する。これにより、本フローチャートによる一連の処理は終了する。本フローチャートを実行することにより、権限情報テーブル４０２のアクセス許可情報が更新される。

【００６２】

（データベースサーバ１０１におけるアクセス制御）

図１３は、データベースサーバ１０１によるアクセス権限の検査処理手順の一例を示すフローチャートである。受付部５０１は、クライアント端末１０２からデータベースサーバ１０１へのデータアクセス要求（ＳＱＬ文）を受け付ける。ＳＱＬ翻訳部５０２は、ＳＱＬ文からデータにアクセスするユーザ名、データアクセスに必要なテーブル名等を抽出する（ステップＳ１３０１）。次に権限検査部５０３は、ユーザ情報４０１と当該ユーザの権限が設定された権限情報テーブル４０２との対応関係を示す権限情報テーブルポインタから、当該ユーザに対応する権限情報テーブル４０２を特定し、権限設定情報４００の特定した権限情報テーブル４０２の権限を参照して、ユーザがテーブルにアクセス可能であるかを検査する（ステップＳ１３０２）。ここで、ユーザがテーブルにアクセス可能である場合（ステップＳ１３０２：Ｙｅｓ）、ステップＳ１３０３に移行し、アクセス不可能な場合（ステップＳ１３０２：Ｎｏ）、ステップＳ１３０４に移行する。

【００６３】

ユーザがテーブルにアクセス可能である場合、アクセス許可検査部５０４は、権限情報テーブル４０２のアクセス許可情報を参照して、許可された時間帯であるか否かを判断する（ステップＳ１３０３）。ここで、許可された時間帯である場合（ステップＳ１３０３：Ｙｅｓ）、ステップＳ１３０５に移行し、許可された時間帯でない場合（ステップＳ１３０３：Ｎｏ）、ステップＳ１３０４に移行する。

【００６４】

許可された時間帯である場合、データアクセス部５０５は、アクセス手順に従ってデータベース２１０をアクセスし、結果を受付部５０１に返信する（ステップＳ１３０５）。逆に、ユーザがテーブルにアクセス不可能である場合、または許可された時間帯でない場合、データアクセス部５０５は、アクセス不許可でエラーを返す（ステップＳ１３０４）。

【００６５】

この場合、業務アプリケーションにエラー復帰するが、このトランザクションの扱いは利用システムの運用ポリシーに任せ、トランザクション継続、あるいはトランザクションキャンセルか、のいずれかが選択できるようにしておくことができる（既存のＳＱＬ文エラー発生時のＳＱＬ文単位のキャンセルと同等の扱いとする）。これにより、本フローチャートによる一連の処理は終了する。本フローチャートを実行することにより、テーブルの権限およびアクセス許可情報が検査される。

【００６６】

以上説明したように、実施の形態１によるデータベースサーバ１０１は、テーブルに対するアクセスを許可する時間帯を示す許可時間帯と、現時刻において、ユーザに当該テーブルに対してアクセスを許可するか否かを示すアクセス許可情報を権限情報テーブル１１０に付与する。データベースサーバ１０１は、バックグラウンドでアクセス許可情報を更新する。データベースサーバ１０１は、クライアント端末１０２からデータアクセス時に、アクセス許可情報を参照することでアクセス許可を判断する。このため、データベースサーバ１０１は、データアクセス時に現在時刻の取得を行うことがない。これにより、データアクセスにかかる処理時間を増大することなく、時間帯に基づくアクセス権の制御を実行することが可能となる。また、高頻度・大量データ・高速処理が要求されるデータベースシステム、例えば、利用者の処理要求に基づいてデータを処理し、処理結果を即座に利用者に送り返すオンライントランザクション処理に、アクセス権限管理に有効な時間の概念を導入できる。

【００６７】

また、データベースサーバ１０１は、権限の有効な時間という考え方を導入することで、動的な権限関係が実現できる。例えば、ある時間帯に関しては特定の利用者や利用資源に限定するなど、データアクセスを確実に抑止することができ、利便性向上とセキュリティが強化（ガード機構）される。また、データアクセス制御の中でアクセス許可を検査することで、データベースサーバ１０１は、データアクセス中の中断を行うことができる。このため、夜間バッチの処理遅延に伴う終了予定時刻の超過、翌朝のオンライン業務の開始時間の遅れを回避するなど、運用性が向上する。

【００６８】

また、データベースサーバ１０１は、許可時間帯の開始時刻に、テーブルに対するアクセス許可情報をアクセス許可に更新し、許可時間帯の終了時刻に、テーブルに対するアクセス許可情報をアクセス不許可に更新し、アクセス許可情報がアクセス許可である場合に、テーブルに対するアクセスを許可する。これにより、データベースサーバ１０１が、ＯＳのシステムコールを呼び出して現在時刻を取得する回数は、許可時間帯の開始時刻と終了時刻の回数に限定される。

【００６９】

また、データベースサーバ１０１は、現在時刻を取得し、許可時間帯の開始時刻および終了時刻のうちの、取得した現在時刻に、最も近い時刻を抽出し、抽出した時刻になるまでスリープし、抽出した時刻になった場合、前記アクセス許可情報を更新する。これによ

り、データベースサーバ１０１は、許可時間帯の開始時刻と終了時刻の間に、スリープすることができる。

【００７０】

（時間規定の権限定義）

アクセスを許可する時間帯を規定する時間規定は、時間規定オブジェクトを新たに作り、時間規定オブジェクトを権限付与時に指定することによって実現することができる。例えば、２１時から日をまたがって翌朝３時までを夜間と定義（夜間Ｔ）し、あるバッチ処理を実現する業務アプリケーション（ユーザＡ）を夜間だけ実行させたい場合には、以下のように、ＧＲＡＮＴ　ＳＱＬ文にＯＮ句を拡張することで、毎日２１時から２７時だけ実行可能とさせることができる。なお、日をまたがった場合は、前日から継続する場合という意味で、２３時、２４時、２５時、２６時…と指定する。

ＣＲＥＡＴＥ　ＴＩＭＥ　ＲＡＮＧＥ　夜間Ｔ　（２１：００，２７：００）

ＧＲＡＮＴ　起動権限　ＴＯ　ユーザＡ　ＯＮ　夜間Ｔ

【００７１】

なお、時間の概念は連続性を持つために、不用意に取り込むと、定義関係に矛盾を起こす場合がある。例えば、ユーザＡがユーザＣに２１時から２５時までの間だけ権限を与え、ユーザＢが同じユーザＣに２４時から２８時までの間だけ権限を与えたとすると、２１時から２４時、２４時から２５時、２５時から２８時までの３つの期間をどのように解釈するのかの仕組みが必要となる。そこで、時間規定（ＴＩＭＥ　ＲＡＮＧＥ）というオブジェクトを新たに用意し、システム内では、分離した時間規定しか許さないことにすることもできる。この場合、２１時から２５時、２４時から２８時という２つの重複期間を持つ時間規定は定義できず、２１時から２４時、２４時から２５時、２５時から２８時までの３つの時間規定を使い回すことになる。

【００７２】

（実施の形態２）

つぎに、実施の形態２にかかるデータベースサーバ１０１について説明する。なお、実施の形態１で説明した箇所と同一箇所については、図示および説明を省略する。

【００７３】

実施の形態１では、データベースサーバ１０１が、時間帯によるアクセスの許可を、テーブルごとのアクセス許可情報で判断する。しかし、データベース２１０は対象テーブルの数が多くなる特徴がある。このため、対象テーブル数の増加に比例して、許可時間帯とアクセス許可情報の情報量が増加し、メモリ使用量の増大化を招いてしまう。さらに、データベースサーバ１０１は、許可時間帯とアクセス許可情報の検索と更新のための時間を使用する。そこで、実施の形態２では、許可時間帯およびアクセス許可情報のフィールドを、許可時間帯を基に許可時間表１４０３に集約する。これにより、データベースサーバ１０１は、許可時間帯およびアクセス許可情報の縮小化を実現する。

【００７４】

図１４は、実施の形態２にかかる権限設定情報４００の記憶内容の一例を示す説明図である。図１４において、権限設定情報４００は、ユーザ情報１４０１と、権限情報テーブル１４０２と、許可時間表１４０３とを含む構成である。ここで、ユーザ情報１４０１は、図４による実施の形態１のユーザ情報４０１と同じ構成である。

【００７５】

図１４において、権限情報テーブル１４０２は、テーブル名、権限、許可時間表ポインタを有し、各フィールドに情報を設定することにより、テーブルごとに、ユーザの権限情報を記憶している。

【００７６】

ここで、テーブル名と権限は、図４による実施の形態１と同じ機能を有する。許可時間表ポインタは、当該テーブルの許可時間帯が設定される許可時間表１４０３のカラムとの対応関係を示す対応情報である。許可時間表ポインタは、当該テーブルの許可時間帯が設定される許可時間表１４０３のカラムのメモリ３０２上のアドレスを示すポインタである

。例えば、図１４において、権限情報テーブル１４０２－１のテーブル（１）の許可時間表ポインタは、テーブル（１）の許可時間帯が９：００－１７：００であるため、当該許可時間帯が設定された許可時間表１４０３の許可時間帯９：００－１７：００のカラムのアドレスを示す。同様に、権限情報テーブル１４０２－１のテーブル（２）の許可時間表ポインタは、許可時間表１４０３の許可時間帯９：００－１７：００のカラムのアドレスを示す。一方、権限情報テーブル１４０２－１のテーブル（３）の許可時間表ポインタは、許可時間表１４０３の許可時間帯１８：００－２２：００のカラムのアドレスを示す。

【００７７】

図１４において、許可時間表１４０３は、許可時間帯およびアクセス許可情報のフィールドを有し、各フィールドに情報を設定することにより、許可時間帯ごとのアクセス許可情報を記憶している。許可時間表１４０３は、許可時間帯およびアクセス許可情報を有する許可時間情報であるカラムから構成され、各カラムは、許可時間表ポインタによる対応関係を有するテーブルの許可時間帯およびアクセス許可情報を示す。許可時間帯とアクセス許可情報は、図４による実施の形態１の権限情報テーブル４０２が有する許可時間帯とアクセス許可情報と同じ機能を有する。

【００７８】

例えば、図１４において、権限情報テーブル１４０２－１は、テーブル名として、テーブル（１）からテーブル（３）を有する。権限情報テーブル１４０２－１は、ユーザＡがテーブル（１）に対して、参照、更新が可能であることを示し、許可時間表ポインタにより、許可時間表１４０３の許可時間帯９：００～１７：００のカラムに対応することを示す。許可時間表１４０３は、９：００～１７：００の時間帯にアクセスが許可されていること、アクセス許可情報が○であり、現時刻において、アクセスが許可されていることを示す。同様に、権限情報テーブル１４０２－１は、ユーザＡが、テーブル（３）に対して、参照が可能であることを示し、許可時間表ポインタにより、許可時間表１４０３の許可時間帯１８：００～２２：００のカラムに対応することを示す。許可時間表１４０３は、１８：００～２２：００の時間帯にアクセスが許可されていること、アクセス許可情報が×であり、現時刻において、アクセスが許可されていないことを示す。

【００７９】

なお、図１４の権限設定情報４００の場合、データベースサーバ１０１のアクセス許可検査部５０４は、テーブル名と、当該テーブルの許可時間帯が設定される許可時間表１４０３のカラムとの対応関係を示す許可時間表ポインタから、許可時間表１４０３のカラムを特定し、当該カラムのアクセス許可情報を参照して、許可された時間帯であるか否かを判断する。

【００８０】

図１４の権限設定情報４００は、図４の権限情報テーブル４０２が有する許可時間帯およびアクセス許可情報のフィールドを、許可時間帯を基に許可時間表１４０３に集約したものである。これは、データベースサーバ１０１のデータベース２１０がテーブル正規化でグループ化される特徴を有することを利用して、集約することができる。この集約（グループ化）により、許可時間帯およびアクセス許可情報の縮小化を実現できる。これにより、データベースサーバ１０１は、許可時間帯およびアクセス許可情報の検索と更新に必要な時間を少なくすることができる。例えば、図４の権限設定情報４００では、権限設定更新部５０７は、５つの許可時間帯、アクセス許可情報を参照、更新する必要があるが、図１４の権限設定情報４００では、権限設定更新部５０７は、２つの許可時間帯、アクセス許可情報のみを参照、更新するだけでよい。

【００８１】

なお、権限情報テーブル１４０２のテーブル名ごとにある許可時間表ポインタは、一つのテーブル名に複数持たせることもできる。これにより、権限情報テーブル１４０２は、９：００～１１：００と１５：００～１７：００のように１つのテーブルに複数の時間帯を許可することが可能になる。

【００８２】

図１５は、実施の形態２にかかる権限設定情報４００のユーザ許可時間帯登録処理手順の一例を示すフローチャートである。なお、権限設定情報４００のユーザ登録および権限設定情報４００のユーザ権限登録は、図４の権限設定情報４００と同じフローチャートで実現できる。

【００８３】

まず、権限情報管理部５０６は、権限登録文（ＧＲＡＮＴ文）を基に、当該ユーザ名とテーブル名に合致するユーザ情報４０１、および権限情報テーブル４０２を参照する（ステップＳ１５０１）。権限登録文は例えば、

ＧＲＡＮＴ ＰＥＲＭＩＳＳＩＯＮ＿ＴＩＭＥ ＴＯ ユーザＡ ＯＮ ＴＡＢＬＥ マスタ表，取引履歴表 ＷＩＴＨ ＴＩＭＥ＿ＲＡＮＧＥ （９：００，１７：００）

ＧＲＡＮＴ ＰＥＲＭＩＳＳＩＯＮ＿ＴＩＭＥ ＴＯ ユーザＢ ＯＮ ＴＡＢＬＥ マスタ表，取引履歴表 ＷＩＴＨ ＴＩＭＥ＿ＲＡＮＧＥ （９：００，１７：００）

で記述される。

【００８４】

次に、権限情報管理部５０６は、合致するユーザ名とテーブル名があるかどうか確認する（ステップＳ１５０２）。ここで、ユーザ名とテーブル名が存在する場合（ステップＳ１５０２：Ｙｅｓ）、ステップＳ１５０３に移行し、存在しない場合（ステップＳ１５０２：Ｎｏ）、ステップＳ１５０４に移行する。

【００８５】

ユーザ名とテーブル名が存在する場合、権限情報管理部５０６は、許可時間表１４０３を参照し、権限登録文の許可時間帯と合致する許可時間帯が存在するかどうか確認する（ステップＳ１５０３）。ここで、合致する許可時間帯が存在する場合、ステップＳ１５０５に移行し、存在しない場合、ステップＳ１５０６に移行する。一方、ユーザ名とテーブル名が存在しない場合、未登録のため、エラー終了する（ステップＳ１５０４）。

【００８６】

合致する許可時間帯が存在する場合、権限情報管理部５０６は、合致した許可時間帯のアドレスを権限情報テーブル１４０２の許可時間表ポインタに設定する（ステップＳ１５０５）。逆に、合致する許可時間帯が存在しない場合、権限情報管理部５０６は、許可時間表１４０３に、今回指定された許可時間帯を登録し、アクセス許可情報をアクセス不許可（×）に設定する（ステップＳ１５０６）。その後、権限情報管理部５０６は、登録した許可時間帯のアドレスを権限情報テーブル１４０２の許可時間表ポインタに設定し（ステップＳ１５０７）、権限設定更新部５０７に権限情報テーブル４０２の変更を通知する（ステップＳ１５０８）。これにより、本フローチャートによる一連の処理は終了する。本フローチャートを実行することにより、許可時間表１４０３に許可時間帯およびアクセス許可情報が登録される。図１６は、図１５のフローチャートにより登録されたユーザＡとユーザＢの情報の一例を示す説明図である。

【００８７】

以上説明したように、実施の形態２にかかるデータベースサーバ１０１は、許可時間帯とアクセス許可情報とを対応付けて表すカラムを有する許可時間表１４０３に基づいて、アクセス許可情報を許可時間帯に応じて更新する。データベースサーバ１０１は、テーブル名と、許可時間表１４０３の中でテーブルの許可時間帯が設定されるカラムとの対応関係を示すポインタから、テーブル名に対応するカラムを特定し、特定したカラムのアクセス許可情報に基づいて、テーブルに対するアクセスを制御する。これにより、許可時間帯およびアクセス許可情報の縮小化を実現でき、データベースサーバ１０１は、許可時間帯およびアクセス許可情報の検索と更新に使用する時間を少なくすることができる。

【００８８】

（実施の形態３）

つぎに、実施の形態３にかかるデータベースサーバ１０１について説明する。なお、実施の形態１，２で説明した箇所と同一箇所については、図示および説明を省略する。

【００８９】

実施の形態１および２では、データベースサーバ１０１は、すべてのユーザに対して、時間帯によるアクセスの許可を判断する。このため、時間規定が付与されないユーザはデータアクセスを行うことができない。そこで、実施の形態３では、時間規定付与の有無を検査することより、時間規定が付与されないユーザにデータアクセスを可能とする。

【００９０】

図１７は、実施の形態３にかかるデータベースサーバ１０１の機能的構成例を示すブロック図である。図１７において、データベースサーバ１０１は、受付部５０１と、ＳＱＬ翻訳部５０２と、権限検査部５０３と、時間規定確認部１７０１と、アクセス許可検査部５０４と、データアクセス部５０５と、権限情報管理部５０６と、権限設定更新部５０７とを含む構成である。各機能部は、図５に示した機能部と同様に実行され、処理結果が記憶される。

【００９１】

時間規定確認部１７０１は、ユーザの情報を参照し、時間規定付与の有無を検査する機能を有する。当該ユーザに時間規定付与が無ければ、アクセス許可検査部５０４の検査を行うことなく、当該ユーザにデータアクセスを許可する。時間規定付与の有無は、例えば、当該実行ユーザの権限情報テーブル４０２に許可時間帯が設定されているか、または当該ユーザの権限情報テーブル１４０２の許可時間表ポインタに値が設定されているかどうかで判断することができる。

【００９２】

図１８は、実施の形態３にかかるデータベースサーバ１０１によるアクセス権限の検査処理手順の一例を示すフローチャートである。ステップＳ１８０１とステップＳ１８０２は、それぞれ、図１３におけるステップＳ１３０１とステップＳ１３０２と同じ処理を実行するステップである。ユーザがテーブルにアクセス可能である場合、時間規定確認部１７０１は、ユーザの情報を参照し、時間規定付与の有無を検査する（ステップ１８０３）。ここで、ユーザに時間規定付与がある場合（ステップＳ１８０３：Ｙｅｓ）、ステップＳ１８０４に移行し、時間規定付与がない場合（ステップＳ１８０３：Ｎｏ）、ステップＳ１８０６に移行する。

【００９３】

ユーザに時間規定付与がある場合、図１３のステップＳ１３０３以降と同じ処理が実行される（ステップＳ１８０４～Ｓ１８０６）。逆に、時間規定付与がない場合、アクセス手順に従ってデータベース２１０をアクセスし、結果を受付部５０１に返信する（ステップＳ１８０６）。これにより、本フローチャートによる一連の処理は終了する。本フローチャートを実行することにより、テーブルの権限、時間規定の付与およびアクセス許可情報が検査される。

【００９４】

以上説明したように、実施の形態３にかかるデータベースサーバ１０１は、ユーザ名と権限情報テーブル４０２との対応関係を示すポインタから、ユーザ名に対応する権限情報テーブル４０２を特定する処理を実行させる。データベースサーバ１０１は、特定した権限情報テーブル４０２に、許可時間表１４０３の中でテーブルの許可時間帯が設定されるカラムとの対応関係を示すポインタが設定されている場合に、当該ポインタからテーブル名に対応する許可時間情報を特定する。これにより、時間規定確認部１７０１がユーザの情報を参照し、時間規定付与の有無を検査することにより、データベースサーバ１０１は、時間規定付与がないユーザにデータアクセスを行うことを可能にする。

【００９５】

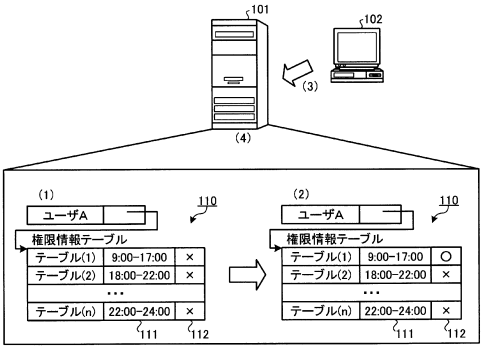
なお、本実施の形態で説明したアクセス制御プログラムは、予め用意されたプログラムをパーソナル・コンピュータやワークステーション等のコンピュータで実行することにより実現することができる。本アクセス制御プログラムは、ハードディスク、フレキシブルディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ等のコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行される。また、本アクセス制御プログラムは、インターネット等のネットワークを介して配布してもよ

い。
【００９６】
上述した実施の形態に関し、さらに以下の付記を開示する。
【００９７】
（付記１）コンピュータに、
アクセス権限が有効となる時間帯を設定可能なデータに対するアクセスを許可する時間帯を示す許可時間帯に基づいて、前記データに対するアクセスを許可するか否かを示すアクセス許可情報を更新し、
前記アクセス許可情報に基づいて、前記データに対するアクセスを制御する、
処理を実行させることを特徴とするアクセス制御プログラム。
【００９８】
（付記２）前記更新する処理は、
前記許可時間帯と前記アクセス許可情報とを対応付けて表す許可時間情報を有する許可時間表に基づいて、前記アクセス許可情報を前記許可時間帯に応じて更新し、
前記制御する処理は、
前記データの識別子と、前記許可時間表の中で前記データの許可時間帯が設定される前記許可時間情報との対応関係を示す対応情報から、前記データの識別子に対応する前記許可時間情報を特定し、特定した前記許可時間情報の前記アクセス許可情報に基づいて、前記データに対するアクセスを制御することを特徴とする付記１に記載のアクセス制御プログラム。
【００９９】
（付記３）前記更新する処理は、
前記許可時間帯の開始時刻に、当該許可時間帯に対応する前記アクセス許可情報をアクセス許可に更新し、前記許可時間帯の終了時刻に、当該許可時間帯に対応する前記アクセス許可情報をアクセス不許可に更新し、
前記制御する処理は、
前記アクセス許可情報がアクセス許可である場合に、前記データに対するアクセスを許可することを特徴とする付記２に記載のアクセス制御プログラム。
【０１００】
（付記４）前記更新する処理は、
現在時刻を取得し、前記許可時間帯の開始時刻および終了時刻のうちの、取得した前記現在時刻に、最も近い時刻を抽出し、前記抽出した時刻になった場合、前記アクセス許可情報を更新することを特徴とする付記３に記載のアクセス制御プログラム。
【０１０１】
（付記５）前記更新する処理は、
前記アクセス許可情報が更新された場合、および前記許可時間帯が変更された場合に実行されることを特徴とする付記４に記載のアクセス制御プログラム。
【０１０２】
（付記６）前記コンピュータに、
ユーザの識別子と前記データの識別子との対応関係を示す対応情報から、アクセス要求元のユーザの識別子に対応する前記データの識別子を特定する処理を実行させ、
前記制御する処理は、
特定した前記データの識別子と、前記許可時間表の中で前記データの許可時間帯が設定される前記許可時間情報との対応関係を示す対応情報が設定されている場合に、当該対応情報から前記データの識別子に対応する前記許可時間情報を特定することを特徴とする付記２～５のいずれか一つに記載のアクセス制御プログラム。
【０１０３】
（付記７）コンピュータに、
アクセス権限が有効となる時間帯を設定可能なデータに対するアクセスを許可する時間帯を示す許可時間帯に基づいて、前記データに対するアクセスを許可するか否かを示すア

クセス許可情報を更新し、
前記アクセス許可情報に基づいて、前記データに対するアクセスを制御する、
処理を実行させるアクセス制御プログラムを記録したことを特徴とする前記コンピュータに読み取り可能な記録媒体。
【０１０４】
（付記８）コンピュータが、
アクセス権限が有効となる時間帯を設定可能なデータに対するアクセスを許可する時間帯を示す許可時間帯に基づいて、前記データに対するアクセスを許可するか否かを示すアクセス許可情報を更新し、
前記アクセス許可情報に基づいて、前記データに対するアクセスを制御する、
処理を実行することを特徴とするアクセス制御方法。
【０１０５】
（付記９）アクセス権限が有効となる時間帯を設定可能なデータに対するアクセスを許可する時間帯を示す許可時間帯に基づいて、前記データに対するアクセスを許可するか否かを示すアクセス許可情報を更新する更新部と、
前記アクセス許可情報に基づいて、前記データに対するアクセスを制御する制御部と、
を有することを特徴とするシステム。
【符号の説明】
【０１０６】
１０１　データベースサーバ
１０２　クライアント端末
２００　システム
２０３　管理端末
２１０　データベース
２２０　ネットワーク
５０１　受付部
５０２　ＳＱＬ翻訳部
５０３　権限検査部
５０４　アクセス許可検査部
５０５　データアクセス部
５０６　権限情報管理部
５０７　権限設定更新部
１７０１　時間規定確認部

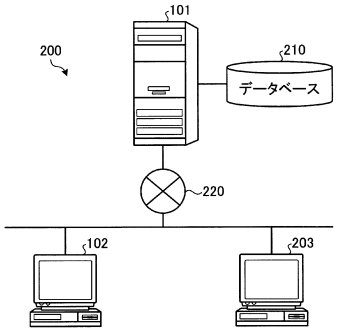
【図１】

実施の形態1にかかるアクセス制御方法の一実施例を示す説明図



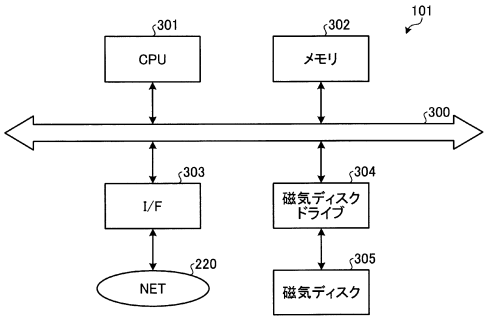
【図２】

システム200のシステム構成例を示す説明図



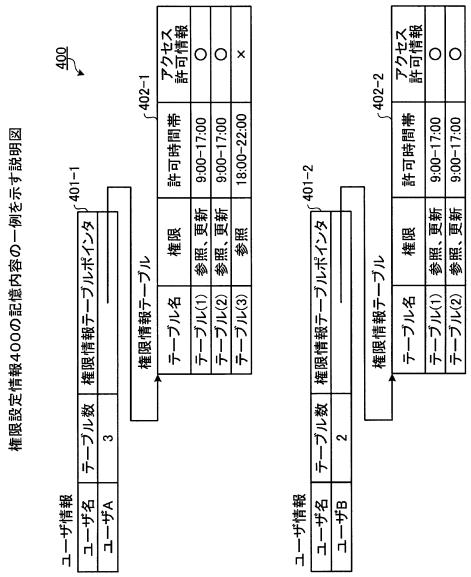
【図３】

データベースサーバ101のハードウェア構成例を示すブロック図



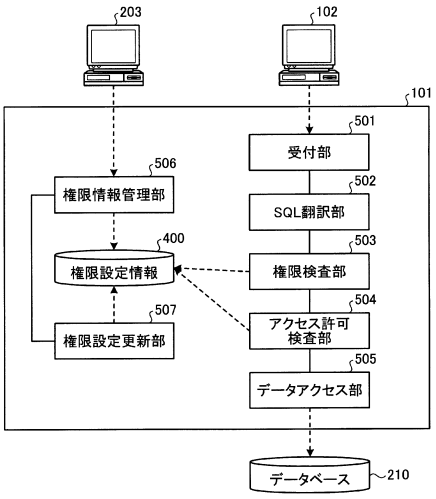
【図４】

権限設定情報400の記憶内容の一例を示す説明図



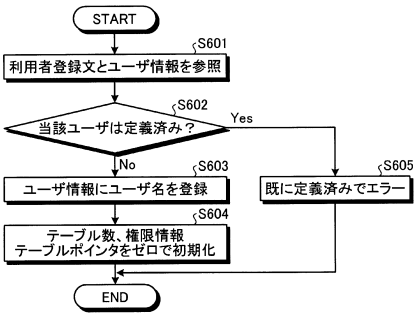
【図５】

データベースサーバ101の機能的構成例を示すブロック図



【図６】

権限設定情報400のユーザ登録処理手順の一例を示すフローチャート



【図７】

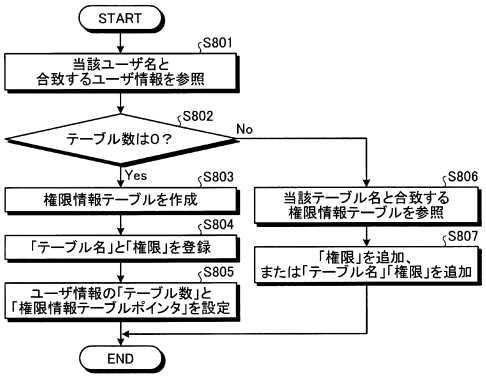
図6のフローチャートにより登録されたユーザ情報401の一例を示す説明図

ユーザ情報 401

ユーザ名	テーブル数	権限情報テーブルポインタ
ユーザA	0	0
ユーザB	0	0
ユーザX	0	0

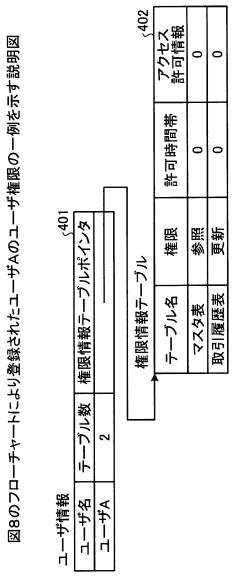
【図８】

権限設定情報400のユーザ権限登録処理手順の一例を示すフローチャート



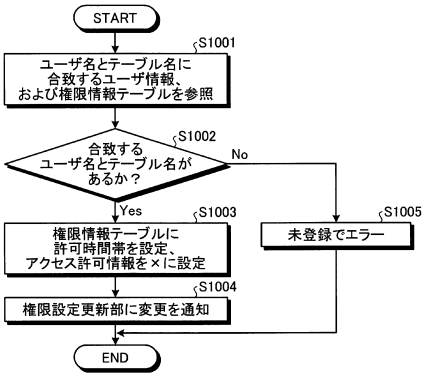
【図９】

図8のフローチャートにより登録されたユーザAのユーザ権限の一例を示す説明図

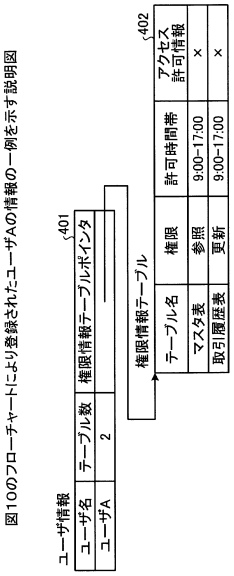


【図１０】

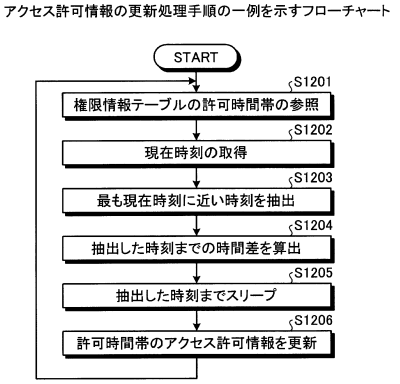
権限設定情報400のユーザ許可時間帯登録処理手順
の一例を示すフローチャート



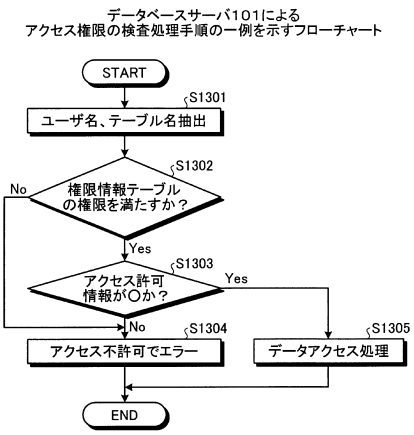
【図１１】



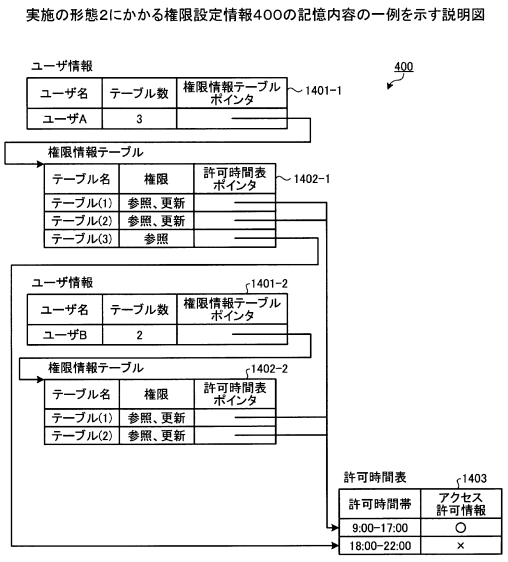
【図１２】



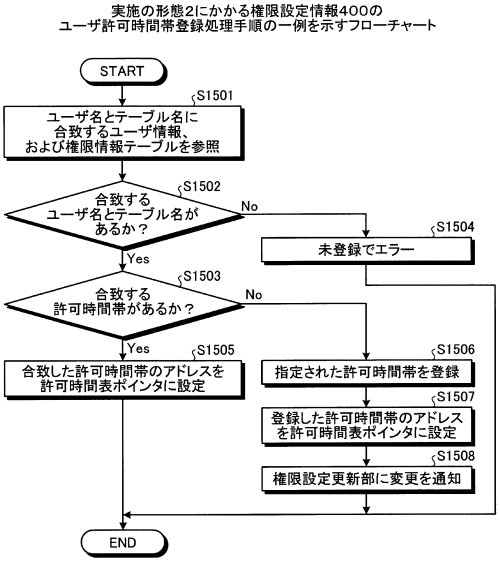
【図１３】



【図１４】

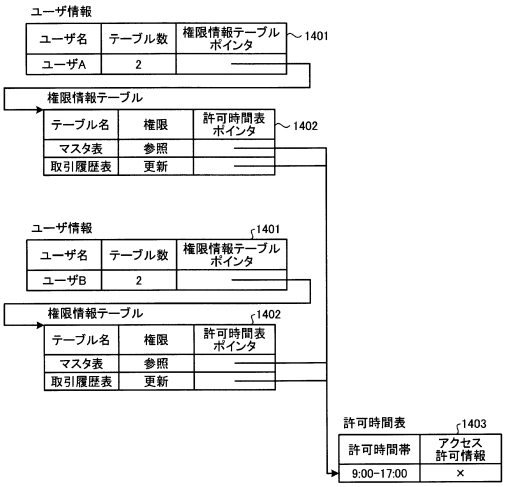


【図１５】



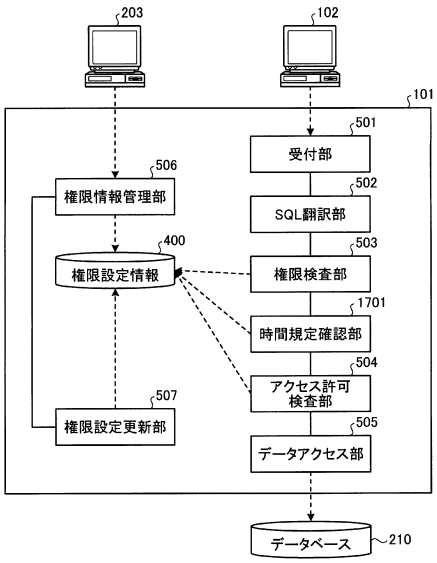
【図１６】

図15のフローチャートにより登録された
ユーザAとユーザBの情報の一例を示す説明図



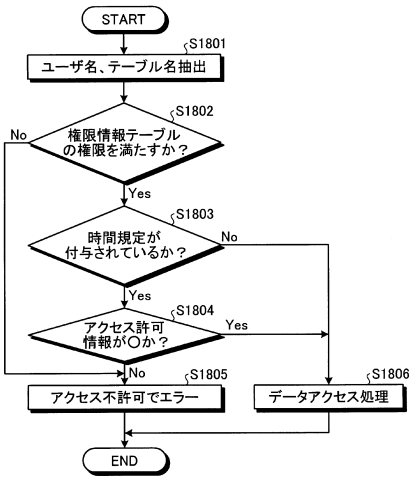
【図１７】

実施の形態3にかかるデータベースサーバ101の
機能的構成例を示すブロック図



【図１８】

実施の形態3にかかるデータベースサーバ101による
アクセス権限の検査処理手順の一例を示すフローチャート



フロントページの続き

審査官　伏本　正典

(56)参考文献　特開平０４－１２３１４６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６２