(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4738183号
(P4738183)

(45)発行日　平成23年8月3日(2011.8.3)　(24)登録日　平成23年5月13日(2011.5.13)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330D
G06F 21/24	(2006.01)	G06F	12/14	520B
G09C 1/00	(2006.01)	G06F	12/14	530E
		G06F	12/14	520F
		G09C	1/00	640E

請求項の数 9　(全 15 頁)

(21)出願番号　特願2006-17480(P2006-17480)
(22)出願日　平成18年1月26日(2006.1.26)
(65)公開番号　特開2007-199995(P2007-199995A)
(43)公開日　平成19年8月9日(2007.8.9)
審査請求日　平成20年6月10日(2008.6.10)

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100099461
弁理士　溝井　章司
(72)発明者　山田　耕一
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

審査官　深沢　正志

最終頁に続く

(54)【発明の名称】アクセス制御装置及びアクセス制御方法及びプログラム

(57)【特許請求の範囲】
【請求項１】
ユーザが利用するユーザ端末からのログインを受け付けるとともに、アクセスを要求されたリソースへのユーザ端末のアクセスの許否判断を行うアクセス制御装置であって、
それぞれが二以上のユーザから構成される複数のユーザグループとそれぞれのユーザグループにアクセスが許可されるアクセス許可リソースを示すアクセス制御テーブルを管理するアクセス制御テーブル管理部と、
ログインしているユーザ端末と当該ユーザ端末を利用しているユーザとを示す通信管理テーブルを管理する通信管理テーブル管理部と、
いずれかのユーザ端末から特定のリソースに対するアクセス要求を受信する受信部と、
前記アクセス制御テーブルと前記通信管理テーブルとを用いて、前記アクセス要求の要求元である要求元ユーザのユーザグループのアクセス許可リソースと前記アクセス要求で要求された前記特定のリソースとが一致するか否かを判断するとともに、前記要求元ユーザのユーザグループに属する他のユーザからのログイン状況を判断し、前記要求元ユーザのユーザグループに属する少なくとも一部の他のユーザからのログインがある場合に、前記アクセス要求に対して前記特定のリソースへのアクセスを許可するアクセス許否判断部とを有することを特徴とするアクセス制御装置。
【請求項２】
前記アクセス許否判断部は、
前記要求元ユーザのユーザグループに属する全ての他のユーザからのログインがある場

合に、前記アクセス要求に対して前記特定のリソースへのアクセスを許可することを特徴とする請求項１に記載のアクセス制御装置。

【請求項３】

前記通信管理テーブル管理部は、

ログインしているユーザ端末と当該ユーザ端末を利用しているユーザの位置とを示す通信管理テーブルを管理し、

前記アクセス許否判断部は、

前記要求元ユーザの位置と前記要求元ユーザのユーザグループに属する他のユーザの位置に基づいて、前記アクセス要求に対する許否判断を行うことを特徴とする請求項１に記載のアクセス制御装置。

【請求項４】

前記アクセス制御テーブル管理部は、

ユーザグループごとに、それぞれのユーザグループに属するユーザの位置に関する条件が示されたアクセス制御テーブルを管理し、

前記アクセス許否判断部は、

前記通信管理テーブル管理部に示された前記要求元ユーザの位置と前記要求元ユーザのユーザグループに属する他のユーザの位置が、前記アクセス制御テーブルに示されたユーザの位置に関する条件に合致している場合に、前記アクセス要求に対して前記特定のリソースへのアクセスを許可することを特徴とする請求項３に記載のアクセス制御装置。

【請求項５】

前記受信部は、

ログインを要求するユーザのユーザ端末から、ログイン要求とともに、当該ユーザ端末の位置をユーザの位置として示す位置情報を受信し、

前記通信管理テーブル管理部は、

前記受信部が受信したユーザ端末からの位置情報を前記通信管理テーブルに登録することを特徴とする請求項３に記載のアクセス制御装置。

【請求項６】

前記受信部は、

ログインを要求するユーザのユーザ端末から、ログイン要求とともに、特定の認証情報から分割された部分認証情報を受信し、

前記アクセス許否判断部は、

前記要求元ユーザからのログイン要求時に受信された部分認証情報と前記要求元ユーザのユーザグループに属する他のユーザからのログイン要求時に受信された部分認証情報とから特定の認証情報が復元可能であるか否かに基づいて、前記アクセス要求に対する許否判断を行うことを特徴とする請求項１に記載のアクセス制御装置。

【請求項７】

前記アクセス制御装置は、

ユーザの入退室管理を行う入退室管理装置に接続されており、

前記受信部は、

前記入退室管理装置から、それぞれのユーザの位置を示す位置情報を受信し、

前記通信管理テーブル管理部は、

前記受信部が受信した前記入退室管理装置からの位置情報を前記通信管理テーブルに登録することを特徴とする請求項３に記載のアクセス制御装置。

【請求項８】

ユーザが利用するユーザ端末からのログインを受け付けるとともに、アクセスを要求されたリソースへのユーザ端末のアクセスの許否判断を行うアクセス制御方法であって、

いずれかのユーザ端末から特定のリソースに対するアクセス要求を受信する受信ステップと、

それぞれが二以上のユーザから構成される複数のユーザグループとそれぞれのユーザグループにアクセスが許可されるアクセス許可リソースを示すアクセス制御テーブルと、ロ

グインしているユーザ端末と当該ユーザ端末を利用しているユーザとを示す通信管理テーブルとを用いて、前記アクセス要求の要求元である要求元ユーザのユーザグループのアクセス許可リソースと前記アクセス要求で要求された前記特定のリソースとが一致するか否かを判断するとともに、前記要求元ユーザのユーザグループに属する他のユーザからのログイン状況を判断し、前記要求元ユーザのユーザグループに属する少なくとも一部の他のユーザからのログインがある場合に、前記アクセス要求に対して前記特定のリソースへのアクセスを許可するアクセス許否判断ステップとを有することを特徴とするアクセス制御方法。

【請求項９】

ユーザが利用するユーザ端末からのログインを受け付けるとともに、アクセスを要求されたリソースへのユーザ端末のアクセスの許否判断をコンピュータに実行させるプログラムであって、

いずれかのユーザ端末から特定のリソースに対するアクセス要求を受信する受信処理と、

それぞれが二以上のユーザから構成される複数のユーザグループとそれぞれのユーザグループにアクセスが許可されるアクセス許可リソースを示すアクセス制御テーブルと、ログインしているユーザ端末と当該ユーザ端末を利用しているユーザとを示す通信管理テーブルとを用いて、前記アクセス要求の要求元である要求元ユーザのユーザグループのアクセス許可リソースと前記アクセス要求で要求された前記特定のリソースとが一致するか否かを判断するとともに、前記要求元ユーザのユーザグループに属する他のユーザからのログイン状況を判断し、前記要求元ユーザのユーザグループに属する少なくとも一部の他のユーザからのログインがある場合に、前記アクセス要求に対して前記特定のリソースへのアクセスを許可するアクセス許否判断処理とをコンピュータに実行させることを特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、例えば、ユーザが利用するユーザ端末がサーバ等のリソースにアクセスする際のアクセス制御技術に関する。

【背景技術】

【０００２】

従来、遠隔地から社内などへアクセスする場合、利用者を認証する手段として、ユーザを識別する情報を利用する。このユーザを識別する情報とは、例えば、ユーザＩＤ・パスワードや、ＩＣカード内に書き込まれた認証書、指紋などである。

特開２００２－６４８６１号公報に開示の「本人認証システム」に示されるように、ユーザの位置を認証に利用したり、特開２００４－４６６６６号公報に開示の「情報ネットワークシステムの制御方法および情報ネットワークシステムならびに移動通信端末」に示されるように、アクセス制御に利用する技術もある。

また、ユーザが遠隔地で使用する端末と、社内などにあるサーバとの通信を行う技術としては、特許第３６０８９０５号に開示の「データ通信システム及びデータ通信方法」で示されるように、クライアントアプリケーションとサーバアプリケーション間の通信を識別する組識別情報を利用し、回線が切断されても復旧できる技術がある。

【特許文献１】特開２００２－６４８６１号公報

【特許文献２】特開２００４－４６６６６号公報

【特許文献３】特許第３６０８９０５号

【発明の開示】

【発明が解決しようとする課題】

【０００３】

従来のユーザ認証方式では、識別情報（ＩＣカード、パスワード、指紋など）が物理的に盗まれる可能性が高い状況下においては、１ユーザ分の識別情報だけでシステムにアク

セスできると、不正アクセスを許す可能性が高くなるという問題があった。

【０００４】

本発明は、このような問題を解決することを主な目的とし、例えば、複数人の同時ログインが必要なアクセス制御を行うことで、認証に必要なものが盗まれた場合等であってもセキュリティを確保することを主な目的とする。

【課題を解決するための手段】

【０００５】

本発明に係るアクセス制御装置は、

ユーザが利用するユーザ端末からのログインを受け付けるとともに、アクセスを要求されたリソースへのユーザ端末のアクセスの許否判断を行うアクセス制御装置であって、

それぞれが二以上のユーザから構成される複数のユーザグループとそれぞれのユーザグループにアクセスが許可されるアクセス許可リソースを示すアクセス制御テーブルを管理するアクセス制御テーブル管理部と、

ログインしているユーザ端末と当該ユーザ端末を利用しているユーザとを示す通信管理テーブルを管理する通信管理テーブル管理部と、

いずれかのユーザ端末から特定のリソースに対するアクセス要求を受信する受信部と、

前記アクセス制御テーブルと前記通信管理テーブルとを用いて、前記アクセス要求の要求元である要求元ユーザのユーザグループのアクセス許可リソースと前記アクセス要求で要求された前記特定のリソースとが一致するか否かを判断するとともに、前記要求元ユーザのユーザグループに属する他のユーザからのログイン状況を判断して、前記アクセス要求に対する許否判断を行うアクセス許否判断部とを有することを特徴とする。

【発明の効果】

【０００６】

本発明によれば、他のユーザのログイン状況を判断してアクセス許否の判断を行うため、ユーザ認証に必要となる物が不正に持ち出された場合にも、正当な他のユーザがログインしていないと不正アクセスを試みる者のアクセス要求は認められないため、セキュリティ強度を向上させることができる。

【発明を実施するための最良の形態】

【０００７】

実施の形態１．

図１は、本実施の形態に係るシステムの構成例を示す図である。

【０００８】

図１において、ＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）端末１００は、ユーザが遠隔地で使用する端末である。図１では、ＰＣ端末１００ａは、ユーザＡ（以下、ｕｓｅｒＡとも表記する）が利用し、クライアントアプリケーションとしてＣｌｉｅｎｔ－ａが搭載されている。また、ＰＣ端末１００ｂは、ユーザＢ（以下、ｕｓｅｒＢとも表記する）が利用し、クライアントアプリケーションとしてＣｌｉｅｎｔ－ｂが搭載されている。ＰＣ端末１００は、ユーザ端末の例である。

ＰＣ端末１００には、ＩＣカードリーダ１１０もしくは指紋認証装置１２０などが接続され、ユーザ認証を行う。ユーザ認証をユーザＩＤ・パスワードで行う場合はこのような装置が無くても良い。また、他の認証手段・認証装置を用いても良い。

【０００９】

サーバ２００は、様々な業務アプリケーションを保持しており、ゲートウェイマシン３００を介してＰＣ端末１００から業務アプリケーションにアクセスされる。サーバ２００自体、また、ＰＣ端末からアクセスされる業務アプリケーションは、リソースの例となる。

図１では、サーバａ２００ａとサーバｂ２００ｂがゲートウェイマシン３００に接続されている。

【００１０】

ＰＣ端末１００からサーバ２００側への通信は、携帯電話の様な回線断が発生しやすい

環境で使われることもある。そのため、端末とゲートウェイマシン３００の間で、例えば、特開２０００－１０１６４０号公報に開示の「クライアント／サーバシステム」に示す方式で、クライアントアプリケーションとサーバアプリケーションを接続し、回線断が発生してもアプリケーションに影響が出ないようにしてもよい。ユーザは、ＰＣ端末１００からサーバ２００に接続するときは、一旦ゲートウェイマシン３００へログインし、ゲートウェイマシン３００を介して目的のサーバへ接続する。ゲートウェイマシン３００へのログインは、通常のユーザ識別情報（ユーザ名／パスワード、指紋、ＩＣカードに収められた認証書など）を利用する。

【００１１】

ゲートウェイマシン３００は、ＰＣ端末１００からのログイン要求を受付け、更に、ログイン中のＰＣ端末１００からいずれかのサーバ２００（リソース）又はいずれかの業務アプリケーション（リソース）に対するアクセス要求があった場合に、アクセス要求に対する許否判断を行う。

ゲートウェイマシン３００は、アクセス制御装置の例である。

ゲートウェイマシン３００は、図１に示すように、受信部３０１、ユーザ認証部３０２、アプリケーションアクセス制御部３０３、送信部３０４、組織別情報管理部３０５、通信管理テーブル管理部３０６、アクセス制御テーブル管理部３０７から構成される。

【００１２】

ゲートウェイマシン３００において、受信部３０１は、ログイン要求、アクセス要求などのＰＣ端末１００からのデータ、またサーバ２００からＰＣ端末へのデータ等を受信する。

ユーザ認証部３０２は、ＰＣ端末１００からログイン要求があった場合に、ＰＣ端末１００を利用するユーザの認証を行う。なお、ＩＣカードリーダ１１０、指紋認証装置１２０による認証のみ行い、ユーザＩＤ・パスワード認証を行わない場合は、ユーザ認証部３０２はなくてもよい。

【００１３】

アプリケーションアクセス制御部３０３は、ログイン中のＰＣ端末１００からいずれかのリソースに対するアクセス要求があった場合に、要求されたリソースへのアクセスを許可するか否かを判定する。アプリケーションアクセス制御部３０３は、後述する通信管理テーブル及びアクセス制御テーブルを用いてアクセス制御を行う。なお、アプリケーションアクセス制御部３０３は、アクセス許否判断部の例である。

送信部３０４は、アクセスを許可したＰＣ端末１００からのデータをサーバ２００に送信し、また、サーバ２００からのデータをＰＣ端末１００に送信する。

組織別情報管理部３０５は、ＰＣ端末１００を利用するユーザが所属する組織情報を管理する。

通信管理テーブル管理部３０６は、通信管理テーブルを管理する。通信管理テーブルは、ログインしているＰＣ端末１００と当該ＰＣ端末１００を利用しているユーザ等を示すテーブルである。通信管理テーブル管理部３０６は、例えば、図２に示すような通信管理テーブルを管理する。通信管理テーブルでは、ゲートウェイマシン３００に接続しているＰＣ端末（クライアント）の情報に加え、ユーザ情報を持つ。

アクセス制御テーブル管理部３０７は、アクセス制御テーブルを管理する。アクセス制御テーブルは、それぞれが二以上のユーザから構成される複数のユーザグループとそれぞれのユーザグループにアクセスが許可されるリソース（アクセス許可リソース）等を示すテーブルである。アクセス制御テーブル管理部３０７は、例えば、図３に示すようなアクセス制御テーブルを管理する。アクセス制御テーブルでは、許可のためにどのようなユーザの接続が必要かという条件（許可のタイプ）と必要なユーザが揃うとアクセスできるリソースの情報（接続許可サーバ）を持つ。なお、アクセス制御に関する情報が、ユーザが所属する組織情報と関連するような場合は、ＬＤＡＰ（Ｌｉｇｈｔｗｅｉｇｈｔ　Ｄｉｒｅｃｔｏｒｙ　Ａｃｃｅｓｓ　Ｐｒｏｔｏｃｏｌ）を用いて管理しても良い。

【００１４】

通信管理テーブル管理部３０６、アクセス制御テーブル管理部３０７は、例えば、磁気ディスク装置や半導体メモリ等により実現され、通信管理テーブル、アクセス制御テーブルはこれら磁気ディスク装置や半導体メモリ等に記憶されている。

【００１５】

ここで、アプリケーションアクセス制御部３０３によるアクセス制御動作の概要を説明する。

図３のアクセス制御テーブルにおいて、グループＩＤ：１のグループに属するユーザは、ｕｓｅｒＡとｕｓｅｒＢであり、「許可のタイプ」の欄に示すように全所属ユーザｕｓｅｒＡ、ｕｓｅｒＢが接続（ログイン）している場合に、ｓｅｒｖｅｒ－ａに対するアクセスが可能となる。そして、ｕｓｅｒＡとｕｓｅｒＢの両者がＰＣ端末１００を用いてゲートウェイマシン３００に接続している場合、図２のように、ｕｓｅｒＡとｕｓｅｒＢが通信管理テーブルに記述され、そして、ｕｓｅｒＡとｕｓｅｒＢの属するグループのグループＩＤ：１がそれぞれの「グループＩＤ」の欄に記述される。ｕｓｅｒＡ又はｕｓｅｒＢからｓｅｒｖｅｒ－ａに対するアクセス要求があった場合、通信管理テーブルにおいてｕｓｅｒＡ又はｕｓｅｒＢにはグループＩＤ：１が記述されており、アクセス制御テーブルにおいてグループＩＤ：１のグループが接続できるサーバはｓｅｒｖｅｒ－ａなので、ｕｓｅｒＡ又はｕｓｅｒＢはｓｅｒｖｅｒ－ａへの接続が可能となる。リソースへの接続を許可するかどうかは、この例のようにグループに所属する全ユーザが接続している場合以外でも、グループ中のあるユーザ数以上が接続している場合とすることも出来る。

また、図２及び図３では、アクセスが許可されるアクセス許可リソースは、接続許可サーバと、サーバ単位となっているが、業務アプリケーション単位としてもよい。

【００１６】

図１０は、実施の形態１におけるゲートウェイマシン３００のハードウェア構成例を示す図である。

図１０において、ゲートウェイマシン３００は、プログラムを実行するＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）１３７を備えている。ＣＰＵ１３７は、バス１３８を介してＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）１３９、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）１４０、通信ボード１４４、ＣＲＴ（Ｃａｔｈｏｄｅ　Ｒａｙ　Ｔｕｂｅ）表示装置１４１、Ｋ／Ｂ１４２、マウス１４３、ＦＤＤ（Ｆｌｅｘｉｂｌｅ　Ｄｉｓｋ　Ｄｒｉｖｅ）１４５、磁気ディスク装置１４６、コンパクトディスク装置（ＣＤＤ）１８６、プリンタ装置１８７、スキャナ装置１８８と接続されていてもよい。

【００１７】

ＲＡＭは、揮発性メモリの一例である。ＲＯＭ、ＦＤＤ、ＣＤＤ、磁気ディスク装置、光ディスク装置は、不揮発性メモリの一例である。

通信ボード１４４は、ＦＡＸ機、電話器、ＬＡＮ等に接続されていてもよい。

また、通信ボード１４４は、図１に示すように、所定の通信回線を通じてＰＣ端末１００、サーバ２００に接続されており、図１に示す受信部３０１及び送信部３０４の一部を構成する。

【００１８】

磁気ディスク装置１４６には、オペレーティングシステム（ＯＳ）１４７、ウィンドウシステム１４８、プログラム群１４９、ファイル群１５０が記憶されている。プログラム群は、ＣＰＵ１３７、ＯＳ１４７、ウィンドウシステム１４８により実行される。

【００１９】

上記プログラム群１４９には、本実施の形態及び以下に述べる実施の形態の説明において「～部」として説明する機能を実行するプログラムが記憶されている。プログラムは、ＣＰＵにより読み出され実行される。

【００２０】

ファイル群１５０には、例えば、通信管理テーブル、アクセス制御テーブルが含まれる。また、本実施の形態及び以下に述べる実施の形態の説明において、「～の判定結果」、

「～の計算結果」、「～の処理結果」として説明するものが、「～ファイル」として記憶されている。

【００２１】

また、以下に述べる実施の形態の説明において説明するフローチャートの矢印の部分は主としてデータの入出力を示し、そのデータの入出力のためにデータは、磁気ディスク装置、ＦＤ（Ｆｌｅｘｉｂｌｅ　Ｄｉｓｋ）、光ディスク、ＣＤ（コンパクトディスク）、ＭＤ（ミニディスク）、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｋ）等のその他の記録媒体に記録される。あるいは、信号線やその他の伝送媒体により伝送される。

【００２２】

また、以下に述べる実施の形態の説明において「～部」として説明するものは、ＲＯＭ１３９に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェアのみ、或いは、ハードウェアのみ、或いは、ソフトウェアとハードウェアとの組み合わせ、さらには、ファームウェアとの組み合わせで実施されても構わない。

【００２３】

また、以下に述べる実施の形態を実施するプログラムは、また、磁気ディスク装置、ＦＤ（Ｆｌｅｘｉｂｌｅ　Ｄｉｓｋ）、光ディスク、ＣＤ（コンパクトディスク）、ＭＤ（ミニディスク）、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｋ）等のその他の記録媒体による記録装置を用いて記憶されても構わない。

【００２４】

次に、図４及び図５のフローチャートを参照して本実施の形態に係るゲートウェイマシン３００の動作例を説明する。

図４は、ユーザがＰＣ端末１００を用いてゲートウェイマシン３００にログインする際の動作を示し、図５は、ユーザが特定のリソースへのアクセスをゲートウェイマシン３００に要求する際の動作を示す。

【００２５】

先ず、図４を用いてログイン時の動作を説明する。

最初に、ゲートウェイマシン３００の受信部３０１が、ＰＣ端末１００からのログイン要求を受信し（Ｓ４０１）、必要であれば、ユーザ認証部３０２がＰＣ端末１００のユーザのユーザ認証を行う（Ｓ４０２）。ユーザ認証時に、ゲートウェイマシン３００に送られた認証情報は、通信管理テーブルのユーザ情報欄に格納される。なお、ＩＣカードリーダ１１０、指紋認証装置１２０による認証のみ行い、ユーザＩＤ・パスワード認証を行わない場合は、この処理を省略してもよい。

ユーザ認証にて認証されなかった場合（Ｓ４０３でＮｏ）は、ＰＣ端末１００に対して送信部３０４からエラー情報を送信する。認証された場合（Ｓ４０３でＹｅｓ）は、アプリケーションアクセス制御部３０３がアクセス制御テーブル管理部３０７と通信し、アクセス制御テーブルを参照して当該ＰＣ端末１００のユーザが該当するレコードを抽出する（Ｓ４０４）。

例えば、ログイン要求がユーザＡのＰＣ端末１００ａから送信されている場合、アクセス制御テーブルのｕｓｅｒＡが含まれるレコード（グループＩＤ：１のレコードと、グループＩＤ：３のレコード）が抽出される。

次に、アプリケーションアクセス制御部３０３が通信管理テーブル管理部３０６と通信し、通信管理テーブルを参照し、他のユーザのログイン状況を分析し、必要な他のユーザがログインしているか否かを判断する（Ｓ４０５）。例えば、グループＩＤ：１のグループは、全ユーザのログインが必要であり、他のユーザであるユーザＢがＰＣ端末１００ｂを用いてログインしているかどうかを判断する。同様に、グループＩＤ：３のグループに対しても他のユーザのログイン状況を判断する。

必要なユーザがログインしていない場合（Ｓ４０６でＮｏの場合）は、通信管理テーブルのグループＩＤ欄に、グループＩＤ：０を書き込む（Ｓ４０８）。

一方、必要なユーザがログインしている場合（Ｓ４０６でＹｅｓの場合）は、そのグル

ープＩＤを通信管理テーブルに書き込む（Ｓ４０７）。たとえば、図３に示すように、グループＩＤ：１がｕｓｅｒＡとｕｓｅｒＢで構成される場合、ｕｓｅｒＡとｕｓｅｒＢが接続していると、通信管理テーブルのグループＩＤ欄に、１を書き込む。セッションＩＤは、特開２０００－１０１６４０号公報に開示の「クライアント／サーバシステム」と同様に、端末とゲートウェイマシン３００間の通信メッセージに付加される。この際、同じユーザグループに属する他のユーザのグループＩＤが０である場合は、この他のユーザに対しても通信管理テーブルにグループＩＤを書き込む。例えば、グループＩＤ：１がｕｓｅｒＡとｕｓｅｒＢで構成される場合、最初にｕｓｅｒＢが単独でログイン要求を送信していた場合、その時点では、ｕｓｅｒＡはログインしていないので、ｕｓｅｒＢに対してグループＩＤ：０が書き込まれるが、その後ｕｓｅｒＡがログイン要求を送信すると、ｕｓｅｒＡとｕｓｅｒＢの両者がログインした状態になるので、通信管理テーブルのｕｓｅｒＢのレコードについてもグループＩＤ：１を設定する。

【００２６】

次に、図５を用いてＰＣ端末１００から特定のリソースに対するアクセス要求があった際の動作を説明する。

最初に、ゲートウェイマシン３００の受信部３０１が、ＰＣ端末１００からのアクセス要求を受信する（Ｓ５０１）（受信ステップ）。

次に、アプリケーションアクセス制御部３０３が通信管理テーブル管理部３０６と通信し、アクセス要求にあるセッションＩＤを元に、通信管理テーブルを参照し、該当するレコードのグループＩＤの欄に書かれている値（グループＩＤ）を読み込む（Ｓ５０２）（アクセス許否判断ステップ）。

読み込んだグループＩＤの値が０である場合（Ｓ５０３でＹｅｓの場合）は、他の必要なユーザがログインしていない状態なので、要求のあったリソースへのアクセスを禁止し（Ｓ５０７）（アクセス許否判断ステップ）、アクセス要求はサーバ２００へは送られない。

一方、グループＩＤが０でない場合（Ｓ５０３でＮｏの場合）は、他の必要なユーザがログインしている状態なので、アプリケーションアクセス制御部３０３がアクセス制御テーブル管理部３０７と通信し、グループＩＤの番号から、アクセス制御テーブルを参照し、ＰＣ端末１００がアクセスしようとした要求リソースとアクセス制御テーブルの「接続許可サーバ」の欄に記載されているアクセス許可リソースが一致するか否かを判断する（Ｓ５０４）（アクセス許否判断ステップ）。

要求リソースとアクセス許可リソースが一致する場合（Ｓ５０５でＹｅｓの場合）は、要求のあったリソースへのアクセスを許可し、ＰＣ端末１００からのアクセス要求を対象となるサーバ２００へ渡す（Ｓ５０６）（アクセス許否判断ステップ）。また、同じ通信路上でサーバ２００からデータが送られてきた場合も、ＰＣ端末１００側へデータを渡す。

一方、要求リソースとアクセス許可リソースが一致しない場合（Ｓ５０５でＮｏの場合）は、要求のあったリソースへのアクセスを禁止し（Ｓ５０７）（アクセス許否判断ステップ）、アクセス要求はサーバ２００へは送られない。

【００２７】

以上により、アクセス制御テーブルの所属ユーザＩＤに合致する複数のユーザが接続している時のみ、端末とサーバ間の通信が可能となり、認証に必要となる物（ＩＣカード、パスワード、指、クライアントＰＣ）が１セットだけ持ち出されて、不正にアクセスしようとしても、２人同時ログインが必要となるリソースにはアクセスできない。

【００２８】

なお、以上の図４及び図５の説明では、ＰＣ端末１００のログイン後に、ＰＣ端末１００からアクセス要求が送信される場合を想定しているが、ＰＣ端末１００からログイン要求とアクセス要求を同時に送信するようにしてもよい。この場合は、図４の処理の後、図５のＳ５０２以降の処理を続けて行うようにすればよい。

【００２９】

以上説明したように、本実施の形態に係るゲートウェイマシン３００は、通信管理テーブルとアクセス制御テーブルを持ち、ゲートウェイマシン３００に接続しているユーザを通信管理テーブルで管理し、アクセス制御テーブルに記述された組み合わせのユーザが接続している場合にユーザにサーバへの接続を許可するという特徴を持つ。

【００３０】

このように、本実施の形態によれば、ＩＣカード、パスワード、生体情報などを用いた認証に加えてゲートウェイマシン３００が、通信管理テーブルとアクセス制御テーブルとを用いてユーザグループに属する他のユーザのログイン状況を判断してアクセス要求に対するアクセス許否判断を行うため、アクセスを許可するための条件が加重されている。また、認証に必要となる物が不正に持ち出された場合にも、正当な他のユーザがログインしていないと不正アクセスを試みる者のアクセス要求は認められないため、セキュリティ強度を向上させることができる。また、新たな認証装置などのハードウェアを追加することなく既存のハードウェア資源でセキュリティ強度を向上させることができる。

【００３１】

実施の形態２．

本実施の形態では、実施の形態１に示したアクセス制御に加えて、ログインする２ユーザが同一エリア（同一の部屋、建物、地域など）にいるかどうか等をチェックして、アクセス制御を行う。

【００３２】

全体のシステム構成例及びゲートウェイマシン３００の内部構成例は、図１のものと同様である。

【００３３】

本実施の形態に係るゲートウェイマシン３００の動作例を図８を参照して説明する。

ＰＣ端末１００が存在する位置を取得するため、位置情報（ＧＰＳ（Ｇｌｏｂａｌ Ｐｏｓｉｔｉｏｎｉｎｇ Ｓｙｓｔｅｍ）の位置情報、モデムから取得する電話番号、携帯電話のエリア情報、ネットワークのＩＰアドレスなど）をＰＣ端末１００側で取得する。

取得した位置情報は、ログイン要求と共にゲートウェイマシン３００へ送信する。ゲートウェイマシン３００では、実施の形態１で説明したように、ログイン要求の受信（Ｓ４０１）、ユーザ認証（Ｓ４０２、Ｓ４０３）、アクセス制御テーブルのレコードの取得（Ｓ４０４）、他のユーザのログイン有無の判断（Ｓ４０４、Ｓ４０５）を行う。これらは、図４に示した動作と同じなので詳細な説明を省略する。

次に、ログイン要求とともに送信されたＰＣ端末１００の位置情報に基づいてＰＣ端末１００の位置を判断する（Ｓ８０１）。

次に、ログイン要求を送信してきたＰＣ端末１００の位置が位置条件に合致するか否かを判断する（Ｓ８０２）。本実施の形態の通信管理テーブルでは、図６に示す様に、ＰＣ端末１００から送られてきた位置情報が書込まれる。この例では、制御室や作業室といった場所の名前となっているが、端末から送られてくる位置情報の形式であれば、他の形式（座標、住所、ＩＰアドレスなど）でもかまわない。一方、本実施の形態のアクセス制御テーブルでは、図７に示すように、「許可のタイプ」欄に、位置情報も合致した場合に、接続許可サーバへのアクセスが許されるように条件が設定されている。位置照合の組み合わせとしては、同一エリア内に居る、同一エリア内に居ない、各ユーザが指定のエリア内に居るなどがある。例えば、２人一組で作業を行う場合で、１人が制御室、もう１人が作業室に居るときのみサーバへのアクセスを許すように設定することが出来る。

このように、通信管理テーブルより同じユーザグループに属する他のユーザが利用しているＰＣ端末１００の位置を取得し、ログイン要求を送信してきたユーザのＰＣ端末１００の位置がアクセス制御テーブルに示されている位置条件に合致するかどうかを判断する。

この結果、位置条件に合致する場合は、対応するグループＩＤとログイン要求を送信してきたＰＣ端末１００の位置情報を通信管理テーブルに書き込む（Ｓ８０３）。

一方、Ｓ４０６及びＳ８０２においてＮｏであった場合は、グループＩＤ：０とログイ

ン要求を送信してきたＰＣ端末１００の位置情報を通信管理テーブルに書き込む（Ｓ８０４）。
アクセス要求が送信されてきた場合の動作は、図５に示したものと同様である。
【００３４】
また、上記の説明と異なり、ログイン要求受信時に位置条件が合致するか否かの判断（Ｓ８０２）を行わずに、アクセス要求受信時に位置条件が合致するか否かの判断を行うようにしてもよい。
この場合は、図８においてＳ８０１とＳ８０２の判断を省略し、一方で、図５のＳ５０３とＳ５０４の間で、通信管理テーブル（図６）に記述されている同じユーザグループに属する各ユーザの位置情報とアクセス管理テーブル（図７）の「許可タイプ」に記述されている位置条件とを比較して、Ｓ８０１とＳ８０２の判断を行うようにしてもよい。
【００３５】
このように、本実施の形態に係るゲートウェイマシン３００は、通信管理テーブルで、ゲートウェイマシン３００に接続しているユーザの位置情報を管理し、アクセス制御テーブルに記述された、ユーザの組み合わせ・位置にあるユーザに対し、サーバへの接続を許可するという特徴を持つ。
【００３６】
以上により、正規ユーザがアクセスしている間に、不正ユーザが別の場所からアクセスしようとしても、ユーザの位置が、アクセス制御テーブルに設定された許可される位置と異なる場合、２人同時ログインが必要となるリソースにはアクセスできず、セキュリティを確保できる。また、新たな認証装置などのハードウェアを追加することなく既存のハードウェア資源でセキュリティ強度を向上させることができる。
【００３７】
実施の形態３．
本実施の形態では、実施の形態２のアクセス制御に加え、ユーザがサーバへ接続する際の、識別情報を、複数ユーザで分割共有する。
たとえば、サーバへアクセスする際に必要となるクライアント認証書を半分に分割し、２ユーザで分割された認証書（部分認証情報）をそれぞれ持ち、同時にその２ユーザがゲートウェイマシン３００へログインし、ＰＣ端末１００から半分の認証書をゲートウェイマシン３００へ送り、ゲートウェイマシン３００が元の認証書へ復元し、ゲートウェイマシン３００から目的のサーバへ認証書を使用して接続する。ＰＣ端末１００からはゲートウェイマシン３００を経由して、目的のサーバへ接続する。一方、ゲートウェイマシン３００において分割された認証書から元の認証書が復元できない場合は、ゲートウェイマシン３００においてサーバ２００へのアクセスが拒否される。
【００３８】
このように、本実施の形態に係るゲートウェイマシン３００は、サーバへの接続に必要となる認証情報を分割し、ゲートウェイマシン３００で通信管理テーブルとアクセス制御テーブルを使った認証後に、すべての認証情報がそろうとサーバに対し、復元した認証情報を送り、サーバで認証できるようにすることを特徴とする。つまり、本実施の形態に係るゲートウェイマシン３００は、ログイン要求を行ったユーザからの分割された認証情報（部分認証情報）とログイン要求を行ったユーザのユーザグループに属する他のユーザからの分割された認証情報（部分認証情報）とから元の認証情報が復元可能であるか否かに基づいて、アクセス要求に対する許否判断を行うことを特徴とする。
【００３９】
以上のように、本実施の形態によれば、認証書を分割することにより、分割後の認証書が一定数以上盗まれないと、不正なアクセスは出来ない。そのため、認証書の盗難に対して、分割しない認証書を使うよりも安全性が高い。
【００４０】
実施の形態４．
上記実施の形態２では、ユーザがいる位置を取得するために、ＰＣ端末１００に接続ま

たは内蔵された位置取得手段を用いて位置を取得していたが、本実施の形態では、入退室管理装置のように、ＰＣ端末１００とは直接接続されていない位置取得手段を用いる。

図９が本実施の形態のシステム構成例を示す図である。

図９において、入退出管理システム５００では、部屋の入り口などに設置された指紋照合装置や非接触ＩＣカードリーダにて、認証された人物のみが部屋に入ることが出来るようになっている。また、入退出管理コントローラ（入退室管理装置）６００は、指紋照合装置や非接触ＩＣカードリーダに接続されており、入退出管理コントローラ６００により入退室を行った人物のＩＤ、時刻などの入退出ログ情報を収集する。

ゲートウェイマシン３００では、入退出管理コントローラ６００に接続されており、入退出管理コントローラ６００から入退出ログ情報を取得する。この入退出ログ情報には、ユーザの位置を示す位置情報が含まれている。

ユーザがＰＣ端末１００からゲートウェイマシン３００にログイン要求を送信してきたときは、入退出ログ情報を用いてユーザが現在存在する位置を求め、通信管理テーブルに記述する。その他の動作は実施の形態２と同様である。

【００４１】

このように、本実施の形態に係るゲートウェイマシン３００は、入退出管理コントローラ６００に接続されており、入退出管理コントローラ６００から入退出ログ情報を取得し、取得した入退出ログ情報を用いて通信管理テーブルでユーザの位置情報を管理するという特徴を持つ。

【００４２】

以上により、実施の形態２の効果に加え、入退出管理システムから入退出ログを取得することにより、ＰＣ端末を利用するユーザの位置情報を利用して、複数ユーザが同時ログインした場合に利用できるようなアクセス制御を行うことが出来る。

【図面の簡単な説明】

【００４３】

【図１】実施の形態１～３に係るゲートウェイマシンを含む全体システムの構成例を示す図。

【図２】実施の形態１に係る通信管理テーブルの例を示す図。

【図３】実施の形態１に係るアクセス制御テーブルの例を示す図。

【図４】実施の形態１に係るゲートウェイマシンの動作例を示すフローチャート図。

【図５】実施の形態１に係るゲートウェイマシンの動作例を示すフローチャート図。

【図６】実施の形態２に係る通信管理テーブルの例を示す図。

【図７】実施の形態２に係るアクセス制御テーブルの例を示す図。

【図８】実施の形態２に係るゲートウェイマシンの動作例を示すフローチャート図。

【図９】実施の形態４に係るゲートウェイマシンを含む全体システムの構成例を示す図。

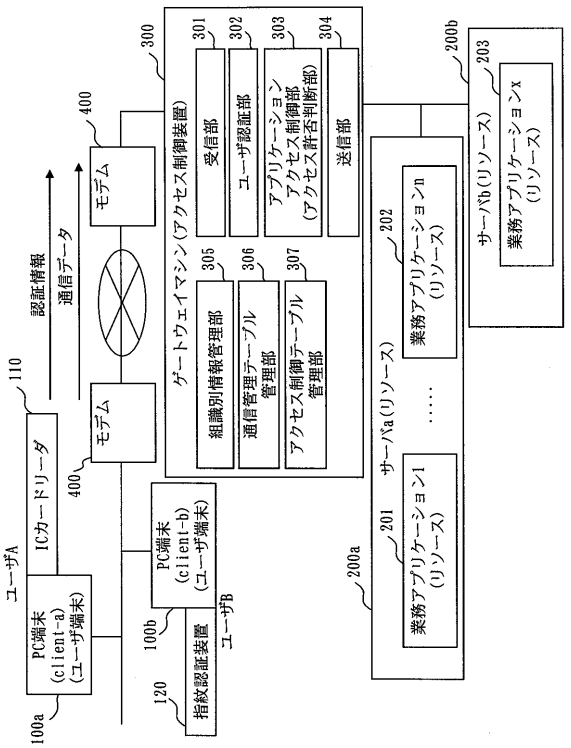
【図１０】実施の形態１～４に係るゲートウェイマシンのハードウェア構成例を示す図。

【符号の説明】

【００４４】

１００　ＰＣ端末、１１０　ＩＣカードリーダ、１２０　指紋認証装置、２００　サーバ、２０１　業務アプリケーション、２０２　業務アプリケーション、２０３　業務アプリケーション、３００　ゲートウェイマシン、３０１　受信部、３０２　ユーザ認証部、３０３　アプリケーションアクセス制御部、３０４　送信部、３０５　組織別情報管理部、３０６　通信管理テーブル管理部、３０７　アクセス制御テーブル管理部、４００　モデム。

【図１】



【図２】

通信管理テーブルの例

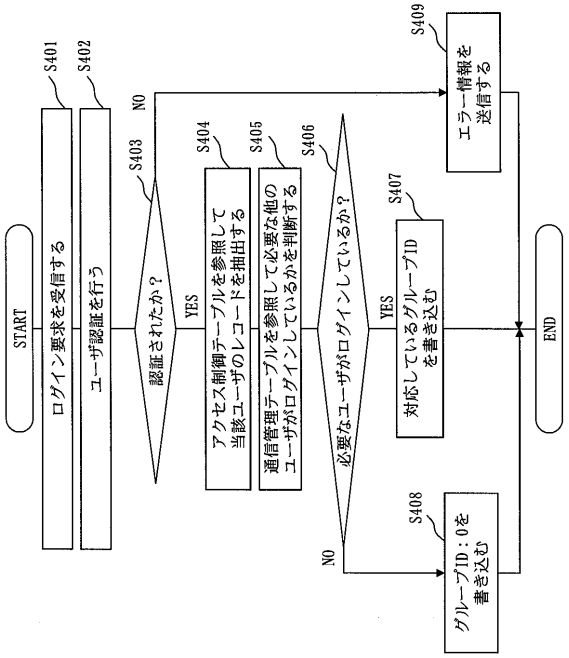
セッションID	回線有効フラグ	クライアントアプリケーション識別情報		サーバアプリケーション識別情報		ユーザ情報		グループID
		hostname	ソケット	hostname	ソケット	ユーザID		
1	有効	client-a	1	server-a	3	userA		1
2	無効							
3	有効	client-b	2	server-a	5	userB		1
…								

【図３】

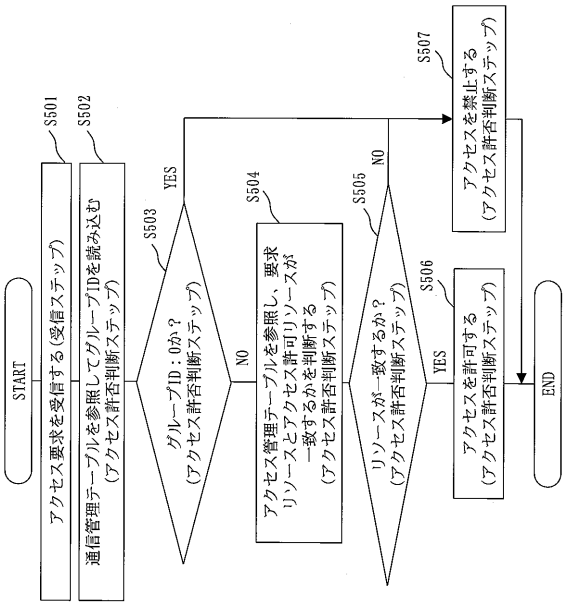
アクセス制御テーブルの例

グループID	所属ユーザID	許可のタイプ	接続許可サーバ
1	userA, userB	全所属ユーザ接続時	server-a
2	userB, userC, userD	2ユーザ以上接続時	server-b
3	userA, userC	全ユーザ接続時	server-c

【図４】



【図５】



【図６】

位置情報を使用した通信管理テーブルの例

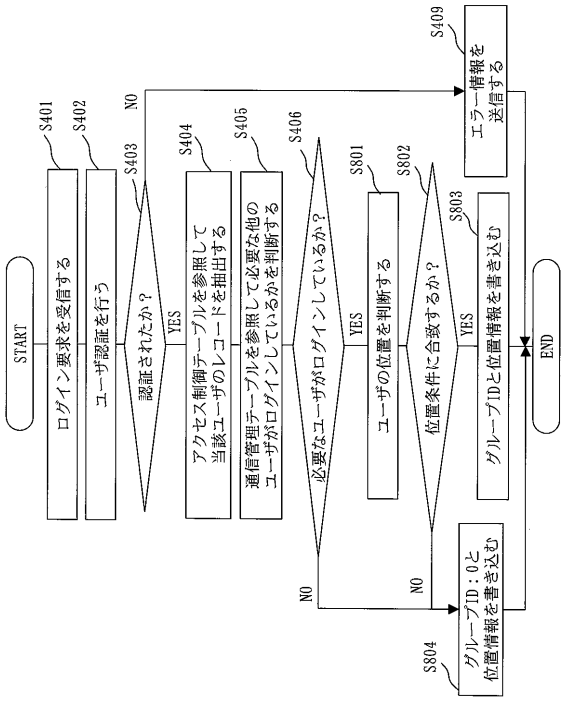
セッションID	回線有効フラグ	クライアントアプリケーション識別情報		サーバアプリケーション識別情報		ユーザ情報		グループID
		hostname	ソケット	hostname	ソケット	ユーザID	位置	
1	有効	client-a	1	server-a	3	userA	制御室	1
2	無効							
3	有効	client-b	2	server-a	5	userB	作業室	1
…								

【図７】

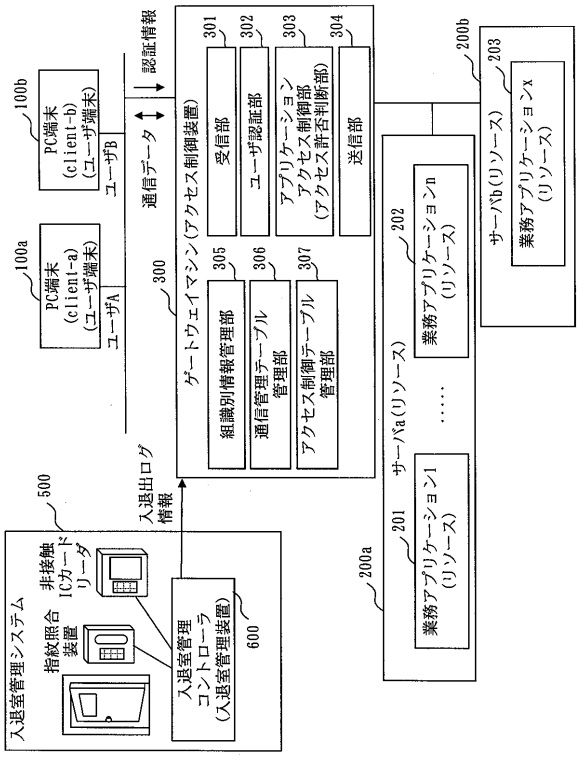
位置情報を使用したアクセス制御テーブルの例

グループID	所属ユーザID	許可のタイプ	接続許可サーバ
1	userA, userB	全所属ユーザ接続、userAが制御室から接続、userBが作業室から接続時	server-a
2	userB, userC, userD	2ユーザ以上同一室内から接続時	server-b
3	userA, userC	全ユーザ、同一市内から接続時	server-c

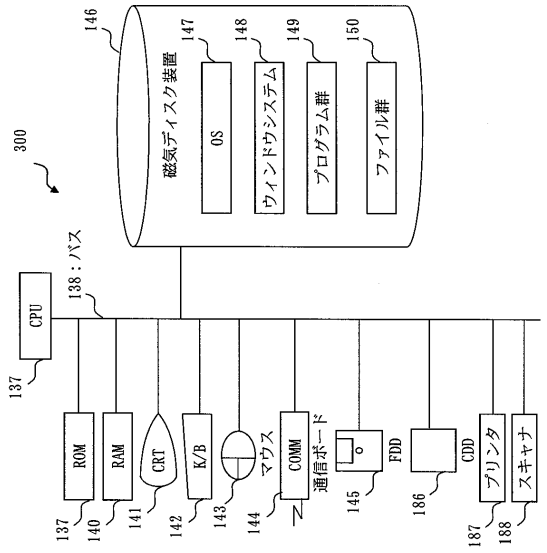
【図８】



【図９】


入退室管理システム
500
非接触
ICカード
リーダ
指紋照合
装置
入退室管理
コントローラ
(入退室管理装置)
600
入退出ログ
情報
100a
PC端末
(client-a)
(ユーザ端末)
ユーザA
100b
PC端末
(client-b)
(ユーザ端末)
ユーザB
通信データ
認証情報
300
ゲートウェイマシン(アクセス制御装置)
301
受信部
302
ユーザ認証部
303
アプリケーション
アクセス制御部
(アクセス許否判断部)
304
送信部
305
組織別情報管理部
306
通信管理テーブル
管理部
307
アクセス制御テーブル
管理部
200a
サーバa(リソース)
201
業務アプリケーション1
(リソース)
202
業務アプリケーションn
(リソース)
200b
サーバb(リソース)
203
業務アプリケーションx
(リソース)

【図１０】


300
146
磁気ディスク装置
147
OS
148
ウィンドウシステム
149
プログラム群
150
ファイル群
CPU
137
138:バス
ROM
137
RAM
140
CRT
141
K/B
142
マウス
143
144
COMM
通信ボード
145
FDD
186
CDD
プリンタ
187
スキャナ
188

フロントページの続き

(56)参考文献 特開２００４－０７８３２７（ＪＰ，Ａ）
特開２００１－１７５６０１（ＪＰ，Ａ）
特開２００１－３２５２３２（ＪＰ，Ａ）
特開２００１－３３１４５０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／００　－　２１／２４