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

特許第4641840号
(P4641840)

(45)発行日　平成23年3月2日(2011.3.2)　(24)登録日　平成22年12月10日(2010.12.10)

| (51)Int.Cl. | | F I | | |
|---|---|---|---|---|
| G06F 21/20 | (2006.01) | G06F | 15/00 | 330B |
| G06F 21/24 | (2006.01) | G06F | 15/00 | 330D |
| H04L 9/32 | (2006.01) | G06F | 12/14 | 530D |
| | | H04L | 9/00 | 673A |

請求項の数 10　(全 17 頁)

(21)出願番号　特願2005-87121(P2005-87121)
(22)出願日　平成17年3月24日(2005.3.24)
(65)公開番号　特開2006-268571(P2006-268571A)
(43)公開日　平成18年10月5日(2006.10.5)
審査請求日　平成20年3月13日(2008.3.13)

(73)特許権者　000005821
パナソニック株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100109210
弁理士　新居　広守
(72)発明者　里村　尚
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　河路　彩
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

審査官　高橋　克

最終頁に続く

(54)【発明の名称】アクセス制御装置、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】
端末装置および少なくとも一つのサーバ装置とネットワークを介して接続され、複数のアクセス権を使い分ける利用者が前記端末装置から行う前記サーバ装置に格納された情報資源へのアクセスを制御するアクセス制御装置であって、
前記複数のアクセス権ごとに認証情報を記憶している認証情報記憶手段と、
外部から取得される識別情報と前記認証情報記憶手段に記憶された認証情報とを照合して前記利用者を識別する利用者識別手段と、
識別に成功すると、前記認証情報記憶手段に記憶されている、識別された利用者に対応する全ての認証情報を次々に用いて前記情報資源へのアクセスを試みるアクセス試行手段と
を備えることを特徴とするアクセス制御装置。
【請求項２】
前記識別情報は、前記利用者に対応する前記認証情報のうちの何れか一つであり、
前記利用者識別手段は、前記識別情報と前記認証情報記憶手段に記憶されている認証情報とを照合することによって、前記利用者を識別する
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】
前記アクセス制御装置は、さらに、
アクセスに成功裏に用いられた認証情報を特定するチケット情報を前記利用者の端末装

置へ送信するチケット送信手段を備え、
前記端末装置は、前記アクセス制御装置から受信されるチケット情報を記録し、その後のアクセスを要求する際に前記チケット情報を前記アクセス制御装置へ送信し、
前記利用者識別手段は、前記端末装置から受信されるチケット情報によって特定される認証情報と前記認証記憶手段に記憶されている認証情報とを照合することによって、前記利用者を識別する
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４】
前記アクセス制御装置は、さらに、
アクセスに成功裏に用いられた認証情報を表す使用結果情報を前記利用者の端末装置へ送信する利用結果情報送信手段
を備え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５】
前記アクセス制御装置は、さらに、
アクセスに成功裏に用いられた認証情報の頻度又は時系列順序を表す履歴情報を記憶している履歴情報記憶手段と、
前記記憶されている認証情報を、前記履歴情報によって示される頻度の高い順又は新しく用いられた順に並べる試行順序決定手段と
を備え、
前記アクセス試行手段は前記記憶されている認証情報を前記試行順序決定手段による並び順に用いて前記情報資源へのアクセスを試みる
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６】
前記アクセス試行手段は、前記記憶されている認証情報の一つを用いて前記情報資源へのアクセスに成功すると、残りの認証情報を用いて試行されるアクセスを抑止する
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７】
前記利用者は自らが兼任する複数の役割ごとにアクセス権を使い分け、
前記認証情報は、前記利用者が前記情報資源を保持しているコンピュータシステムに前記役割に応じたアクセス権を持ってログインするためのログインＩＤ及びパスワードの組である
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８】
前記利用者はアクセスしようとする情報資源を保持しているコンピュータシステムごとにアクセス権を使い分け、
前記認証情報は、前記コンピュータシステムそれぞれに前記利用者がログインするためのログインＩＤ及びパスワードの組である
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９】
端末装置及び少なくとも一つのサーバ装置とネットワークを介して接続され、かつ認証情報記憶手段と利用者識別手段とアクセス試行手段とを備えたアクセス制御装置によって、複数のアクセス権を使い分ける利用者が前記端末装置から行う前記サーバ装置に格納された情報資源へのアクセスを制御するアクセス制御方法であって、
前記認証情報記憶手段は、前記複数のアクセス権ごとに認証情報を記憶しており、
前記利用者識別手段が、外部から取得される識別情報と前記認証情報記憶手段に記憶された認証情報とを照合して前記利用者を識別する利用者識別ステップと、
前記アクセス試行手段が、前記利用者識別ステップにおいて識別に成功すると、前記認証情報記憶手段に記憶されている、識別された利用者に対応する全ての認証情報を次々に用いて前記情報資源へのアクセスを試みるアクセス試行ステップと
を含むことを特徴とするアクセス制御方法。

【請求項１０】
端末装置及び少なくとも一つのサーバ装置とネットワークを介して接続され、かつ認証情報記憶手段と利用者識別手段とアクセス試行手段とを備え、複数のアクセス権を使い分ける利用者が前記端末装置から行う前記サーバ装置に格納された情報資源へのアクセスを制御するアクセス制御装置を実現するためのプログラムであって、
請求項９に記載のアクセス制御方法に含まれるステップ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、アクセス制御装置及びその方法に関し、特に複数のアクセス権を使い分ける利用者が行う情報資源へのアクセスを制御する技術に関する。
【背景技術】
【０００２】
従来の情報処理システムでは、情報資源（データ）の機密性を保つと共に、誤操作による重要データの削除といった事故をできる限り回避するため、利用者ごとにアクセスを制御する技術が実現されている。
【０００３】
図１３は、そのような制御を行う情報処理システムの典型例を表す概念図である。情報処理システム１００は、端末装置１０１及びサーバ装置１０２、１０３がネットワーク１０４で接続されてなる。サーバ装置１０２、１０３は、例えばコンテンツやウェブページ情報といった情報資源とアクセス権のある利用者を示すアクセス権情報とを対応付けて保持すると共に、端末装置１０１の利用者を識別することによって、正当なアクセス権を持つ利用者にのみ情報資源へのアクセスを提供する。
【０００４】
利用者の識別は、利用者固有のログインＩＤ及びパスワードを用いる認証によって、従来広く行われている。
【０００５】
また近年、例えば伝票データやフォームデータといった情報資源に対し、利用者が役割に応じた所定の処理（閲覧、更新、承認等）を行いながら全体処理を進行させるワークフローシステムが実用化されている。
【０００６】
ワークフローシステムでは一人の利用者がしばしば複数の役割を兼任するので、利用者のアクセス権を役割ごとに使い分けることが情報資源の機密性及び安全性の面で好ましい。そのために例えば、兼任する役割の数のログインＩＤ及びパスワードを一人の利用者について定め、その中の一つが入力されることによってその利用者の認証と同時に当面の役割の識別をも行い、識別された役割に応じてアクセスを制御することが行われる。
【０００７】
図１４は、そのような制御に用いられる利用者情報の一具体例である。この利用者情報は利用者情報テーブル２００に格納され、グループＩＤ欄２０１には利用者のＩＤが保持され、ＩＤ欄２０２、パスワード欄２０３、及び情報資源欄２０４には、その利用者が兼任する役割それぞれに対応するログインＩＤ、暗号化されたパスワード、及びその役割においてアクセス許可される情報資源のアドレスが保持される。
【０００８】
この具体例によれば、利用者”Ｇ０００１２３４”は、自らが兼任する役割に対応するログインＩＤ”００００００１”、”００４００２４”、及び”００７０５２３”のうちの当面の役割に対応する一つとパスワードとを入力することによって認証を受け、その役割に対応する情報資源へのアクセス権を得ることができる。
【０００９】
なお、利用者にとって複数のログインＩＤとパスワードとを安全に管理して使い分ける

ことは極めて煩雑である。そこで、利用者の認証には単一のログインＩＤとパスワードとを用いることとし、認証が成功した後その利用者に明示的に役割を選択させることによって、前述した煩雑さを軽減すると同時に、役割ごとにアクセスを制御しつつ適切なワークフロー処理を行う技術が開示されている（例えば特許文献１を参照）。

【特許文献１】特開平２００３－２５６６２９号公報

【発明の開示】

【発明が解決しようとする課題】

【００１０】

しかしながら、前述した従来の技術によれば、一人の利用者が一つのログインＩＤとパスワードとを管理すれば足りるという効果が得られるものの、利用者にとって役割を明示的に選択する煩雑さが依然残る。特に一人の利用者が次々と役割を切り替えながら作業を進めていく状況において、切り替えの都度役割を選択し直す手順は作業の迅速性を阻害し、その結果システム全体の作業効率が損なわれるという問題もある。

【００１１】

本発明は、上記の問題点を解決するためになされたものであり、複数のアクセス権を使い分ける利用者（例えば、ワークフローシステムにおいて複数の役割を兼任する利用者）が行うアクセスを効率的に制御するアクセス制御装置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】

【００１２】

本発明に係るアクセス制御装置は、端末装置および少なくとも一つのサーバ装置とネットワークを介して接続され、複数のアクセス権を使い分ける利用者が前記端末装置から行う前記サーバ装置に格納された情報資源へのアクセスを制御するアクセス制御装置であって、前記複数のアクセス権ごとに認証情報を記憶している認証情報記憶手段と、外部から取得される識別情報と前記認証情報記憶手段に記憶された認証情報とを照合して前記利用者を識別する利用者識別手段と、識別に成功すると、前記認証情報記憶手段に記憶されている、識別された利用者に対応する全ての認証情報を次々に用いて前記情報資源へのアクセスを試みるアクセス試行手段とを備える。

【００１３】

この構成によれば、ひとたび利用者が識別されるとその利用者の全てのアクセス権に対応する認証情報を用いて前記情報資源へのアクセスが試みられるので、利用者にとって、単一の識別情報（例えば、ログインＩＤ及びパスワード）を入力して識別を受けるだけで自らが使い得るアクセス権の何れか一つが得られるという、優れた利便性と迅速な操作性とが発揮される。

【００１４】

また、前記識別情報は、前記利用者に対応する前記認証情報のうちの何れか一つであり、前記利用者識別手段は、前記識別情報と前記認証情報記憶手段に記憶されている認証情報とを照合することによって、前記利用者を識別してもよい。

【００１５】

この構成によれば、利用者は前記認証情報のうち何れか（例えば、最も覚えやすい又はたまたま思い出した）一つを用いて識別を受けることができるので、前記識別情報を前記認証情報と別途に設定する必要なしに、優れた利便性と迅速な操作性とを利用者に提供できる。

【００１６】

また、前記アクセス制御装置は、さらに、アクセスに成功裏に用いられた認証情報を特定するチケット情報を前記利用者の端末装置へ送信するチケット送信手段を備え、前記端末装置は、前記アクセス制御装置から受信されるチケット情報を記録し、その後のアクセスを要求する際に前記チケット情報を前記アクセス制御装置へ送信し、前記利用者識別手段は、前記端末装置から受信されるチケット情報によって特定される認証情報と前記認証記憶手段に記憶されている認証情報とを照合することによって、前記利用者を識別してもよい。

【００１７】
この構成によれば、利用者の識別が前記チケット情報を用いて行われるので、利用者は、チケット情報が得られた後は、単に所望の情報資源へのアクセスを試みるだけで自らが使い得るアクセス権の何れか一つを得られるという、非常に優れた利便性と迅速な操作性とが発揮される。
【００１８】
また、前記アクセス制御装置は、さらに、アクセスに成功裏に用いられた認証情報を表す使用結果情報を前記利用者の端末装置へ送信する利用結果情報送信手段を備えてもよい。
【００１９】
この構成によれば、アクセスに成功裏に用いられたログインＩＤを利用者の端末に表示することができるので、利用者は自らがどのアクセス権を得たかを、確実かつ容易に知ることができる。
【００２０】
また、前記アクセス制御装置は、さらに、アクセスに成功裏に用いられた認証情報の頻度又は時系列順序を表す履歴情報を記憶している履歴情報記憶手段と、前記記憶されている認証情報を、前記履歴情報によって示される頻度の高い順又は新しく用いられた順に並べる試行順序決定手段とを備え、前記アクセス試行手段は前記記憶されている認証情報を前記試行順序決定手段による並び順に用いて前記情報資源へのアクセスを試みてもよい。
【００２１】
この構成によれば、よく用いられる認証情報や新しく使われた認証情報から順に前記情報資源へのアクセスに用いられるので、利用者にとってより重要と考えられる認証情報ほど優先的に用いることができる。
【００２２】
また、前記アクセス試行手段は、前記記憶されている認証情報の一つを用いて前記情報資源へのアクセスに成功すると、残りの認証情報を用いて試行されるアクセスを抑止してもよい。
【００２３】
この構成によれば、前記情報資源が得られた時点以降のアクセスが抑止されるので、通信トラフィック量の削減と処理時間の短縮とが実現される。
【００２４】
また、前記利用者は自らが兼任する複数の役割ごとにアクセス権を使い分け、前記認証情報は、前記利用者が前記情報資源を保持しているコンピュータシステムに前記複数の役割ごとのアクセス権を持ってログインするためのログインＩＤ及びパスワードの組であるとしてもよい。
【００２５】
この構成は、例えば、前記コンピュータシステムがワークフローシステムとして機能している場合に、そのワークフローシステムにおける複数の役割を兼任する利用者が行うアクセスを制御するのに好適である。ワークフローシステムでは、しばしば一人の利用者が複数の役割を兼任することとなるからである。
【００２６】
また、前記利用者はアクセスしようとする情報資源を保持している複数のコンピュータシステムごとにアクセス権を使い分け、前記認証情報は、前記複数のコンピュータシステムそれぞれに前記利用者がログインするためのログインＩＤ及びパスワードの組であるとしてもよい。
【００２７】
この構成は、例えば、前記複数のコンピュータシステムが、それぞれネットワークバンキングシステム、航空券予約システム、ネットワーク通販システム等として機能している場合に、それぞれのシステムにアクセス権を持つ利用者が行うアクセスを制御するのに好

適である。利用者は、それらのシステムごとのログインＩＤ及びパスワードの組のうち何れか一つ（例えば、最も覚えやすい一つ、又はたまたま思い出した一つ）を用いてひとたび識別を受けた後は、どのシステムにもログインできるという、極めて優れた利便性を享受できる。

【００２８】

また、本発明は、このようなアクセス制御装置として実現できるだけでなく、このようなアクセス制御装置が備える特徴的な手段によって実行される処理をステップとするアクセス制御方法として実現することも、また、それらのステップをコンピュータに実行させるプログラムとして実現することもできる。そして、そのようなプログラムは、ＣＤ－ＲＯＭ等の記録媒体やインターネット等の伝送媒体を介して配信できることはいうまでもない。

【発明の効果】

【００２９】

本発明のアクセス制御装置は、一人の利用者が使い分けるアクセス権それぞれに対応して認証情報を記憶しており、ひとたび利用者が識別されるとその利用者の全てのアクセス権に対応する認証情報を用いて情報資源へのアクセスを試みるので、利用者にとって、単一の識別情報（例えば、ログインＩＤ及びパスワードの一組）を入力して識別を受けるだけで自らが使い得るアクセス権の何れか一つが得られるという、優れた利便性と迅速な操作性とが発揮される。

【発明を実施するための最良の形態】

【００３０】

本発明の実施の形態に係るアクセス制御装置は、端末装置とサーバ装置とを接続して設けられ、一人の利用者が兼任する複数の役割それぞれに対応してサーバ装置上で利用者認証を受けるための認証情報であるログインＩＤ及びパスワードを記憶している。このアクセス制御装置は、端末装置から受け取るログインＩＤ及びパスワードを記憶しているログインＩＤ及びパスワードと照合することによって利用者を識別する。そして、識別された利用者の全てのログインＩＤ及びパスワードを順次使用しながら、端末装置から受け取るアクセスリクエストをサーバ装置へと転送する。

【００３１】

以下、このアクセス制御装置について、図面を参照しながら詳細に説明する。

（全体構成）

図１は、このアクセス制御装置を含む情報処理システムの全体構成を示す機能ブロック図である。情報処理システム１は、端末装置２、第１通信網３、アクセス制御装置４、第２通信網５、及びサーバ装置６から構成される。

【００３２】

アクセス制御装置４は、第１通信部１０、利用者識別部２０、認証情報参照部３０、認証情報記憶部４０、試行順序決定部５０、履歴情報記憶部６０、アクセス試行部７０、履歴情報更新部８０、及び第２通信部９０から構成される。

【００３３】

アクセス制御装置４は、例えば図示しないＣＰＵ（Central Processing Unit）、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）、ハードディスク装置、及びネットワークアダプタ等を含むコンピュータシステムによって実現されるとしてもよい。その場合、第１通信部１０及び第２通信部９０の機能はネットワークアダプタによって実現され、認証情報記憶部４０及び履歴情報記憶部６０の機能はハードディスク装置によって実現され、利用者識別部２０、認証情報参照部３０、試行順序決定部５０、アクセス試行部７０、及び履歴情報更新部８０の機能はＣＰＵがＲＯＭに保持されているプログラムを、ＲＡＭを作業用のメモリに用いて実行することによって実現される。

【００３４】

もちろん、アクセス制御装置４を、個々の構成要素の機能を統合する１チップＩＣ（Integrated Circuit）として実現することもできる。

【００３５】
（認証情報）
図２は、認証情報記憶部４０に記憶されている認証情報の一具体例である。この認証情報は認証情報テーブル４００に格納され、グループＩＤ欄４０１には利用者のＩＤが保持され、ＩＤ欄４０２及びパスワード欄４０３には、利用者が兼任する役割それぞれに対応するログインＩＤ及び暗号化されたパスワードが保持される。
【００３６】
なお、役割を兼任しない（単一の役割のみを果たす）利用者を統一的に処理するため、利用者”Ｇ０００２９５５”に示すような一つのＩＤ及びパスワードを持つ利用者が認証情報に含まれていても構わないものとする。
【００３７】
（履歴情報）
図３は、履歴情報記憶部６０に記憶されている履歴情報の一具体例である。この履歴情報は履歴情報テーブル６００に格納され、グループＩＤ欄６０１には利用者のＩＤが保持され、ＩＤ欄６０２にはその利用者によるアクセスに使用されたログインＩＤが所定個数まで時系列順に保持される。
【００３８】
（動作）
以下、アクセス制御装置４の動作を、端末装置２及びサーバ装置６との連携動作を含めて詳細に説明する。
【００３９】
図４は、端末装置２、アクセス制御装置４、及びサーバ装置６の連携動作の一例を示すフローチャートである。この動作は、アクセス制御装置４が、サーバ装置６に格納されている情報資源をリクエストする情報（この例ではページＡリクエスト情報）を端末装置２から受信すると開始される。ページＡリクエスト情報は、例えば、端末装置２で動作しているウェブブラウザ上で、利用者がページＡへのリンクをクリックする、又はページＡのＵＲＬ（Uniform Resource Locator）を入力するといった操作を行うことによって送信される。
【００４０】
ページＡリクエスト情報が受信されると、利用者識別部２０は、ログインプロンプト情報を、第１通信部１０を介して端末装置２へ送信する（Ｓ１０）。このログインプロンプト情報は、利用者にログインＩＤ及びパスワードの入力を促す情報である。端末装置２は、ログインプロンプト情報を受信すると、例えば前述したウェブブラウザの画面上にログインＩＤ及びパスワードの入力フィールドを持ったログインプロンプトを表示する（Ｓ２０）。フローチャートに見られるように、この例では、ページＡへのリンクがクリックされた後ページＡが表示される前に、ログインプロンプトの表示が行われるとした。
【００４１】
図５（Ａ）及び（Ｂ）は、端末装置２に表示されるログインプロンプトの一例である。ここでは、ログインプロンプトが、画面の下端及びポップアップに表示される例を示している。
【００４２】
利用者は、このログインプロンプトに例えば、自らを識別する識別情報として認証情報記憶部４０に記憶されているログインＩＤ及びパスワードの何れか一組を入力する。端末装置２は、利用者から受け付けたログインＩＤ及びパスワードをアクセス制御装置４へ送信する（Ｓ２１）。
【００４３】
利用者識別部２０は、端末装置２から受信されるログインＩＤ及びパスワードを、認証情報記憶部４０に記憶されているログインＩＤ及びパスワードのそれぞれと照合する。そして、合致するログインＩＤ及びパスワードがある場合に、端末装置２の利用者がそのログインＩＤに対応するグループＩＤによって示される利用者であると識別する。

【００４４】
識別に成功すると、認証情報参照部３０は、識別された利用者に対応する全てのログインＩＤを認証情報記憶部４０から参照する（Ｓ３０）。
【００４５】
試行順序決定部５０は、認証情報参照部３０によって参照されたログインＩＤを、履歴情報記憶部６０における記録順序に基づいて、より新しく使用された順に並べる（Ｓ４０）。
【００４６】
アクセス試行部７０は、試行順序決定部５０によって並べられた順にログインＩＤを一つ選択しては、そのログインＩＤ及び対応するパスワードと共に、ページＡリクエスト情報をサーバ装置６へ送信する（Ｓ５０）。
【００４７】
サーバ装置６は、アクセス制御装置４から受信されるログインＩＤ及びパスワードで利用者を認証した上で、ページＡリクエスト情報を次のように処理する。認証に成功した場合にはページＡの内容を返答し、認証に失敗した場合にはアクセス拒否応答情報を返答する。
【００４８】
アクセス試行部７０は、サーバ装置６からの返答に応じて、使用したログインＩＤごとにページＡの内容が得られたか否か、及びページＡの内容が得られた場合にはその内容を、図示しないバッファメモリに記録する。
【００４９】
参照履歴更新部８０は、ページＡの内容の取得に最初に成功したログインＩＤを、利用者を示すグループＩＤに対応付けて履歴情報記憶部６０に新たに記録すると共に、その利用者に対応する所定数を超えるログインＩＤがあれば古いものから削除する（Ｓ７０）。
【００５０】
アクセス試行部７０は、ページＡの内容の取得に最初に成功したログインＩＤ（この例ではＩＤ２）を示すチケット２、ページＡ情報、及びＩＤ使用結果情報（この例では、ページＡがＩＤ２を使用してアクセスされ、さらにＩＤ３を使用してもアクセス可能であることを示す情報）を端末装置２に返送する（Ｓ８０）。ここでチケットは、例えば、ページの取得に最初に成功したログインＩＤの認証情報に含まれている位置を示す索引情報であるとしてもよく、具体的に周知のクッキー情報を用いて表してもよい。
【００５１】
端末装置２は、アクセス制御装置４から受信されたチケットを記憶し（Ｓ９０）、受信されたページの内容を表示し（Ｓ９２）、受信されたＩＤ使用結果情報を表示する（Ｓ９３）。チケットは、例えば端末装置２に設けられるクッキーデータファイル（不図示）に記憶される。
【００５２】
図６（Ａ）及び（Ｂ）は、この動作例において端末装置２に表示されるＩＤ使用結果の一例であり、ページＡがＩＤ２を使用してアクセスされ、さらにＩＤ３を使用してもアクセス可能であることを表している。ここでは、ＩＤ使用結果が画面の下端及びポップアップに表示される例を示す。なお、後述する説明の便宜上、ページＡはページＢへのリンクを含むものする。
【００５３】
ここまでに述べたように、アクセス制御装置４は、一人の利用者が兼任する複数の役割それぞれに対応してログインＩＤ及びパスワードを記憶しており、そのうちの任意のログインＩＤ及びパスワードが与えられることによってその利用者を識別する。そして、端末装置から受け取るアクセスリクエストを、識別された利用者の全ての役割に対応するログインＩＤ及びパスワードを順次使用しながらサーバ装置へと転送するので、利用者は一つのログインＩＤ及びパスワードを入力するだけで、自らが兼任する役割のうち何れか一つのアクセス権を得ることができる。

【００５４】
しかも、アクセスに成功したログインＩＤが表示されるので、利用者は自らがどの役割のアクセス権を得たかを、確実かつ容易に知ることができる。
【００５５】
次に、前述の動作に引き続いて、利用者がページＢをリクエストする場合の動作について説明する。
【００５６】
図７は、その場合の、端末装置２、アクセス制御装置４、及びサーバ装置６の連携動作の一例を示すフローチャートである。この動作は、図４の動作に引き続いて、アクセス制御装置４がページＢリクエスト情報を端末装置２から受信すると開始される。ページＢリクエスト情報は、例えば、ページＡに含まれるページＢへのリンク（図６（Ａ）及び（Ｂ）を参照）を、利用者がクリックすることによって送信される。
【００５７】
以下、図４の動作と同様の事項については説明を省略し、相違点を主に説明する。
端末装置２は、ページＢリクエスト情報を送信後、記憶しているチケットを、ＩＤ及びパスワードに代えて、アクセス制御装置４へ送信する（Ｓ２２）。
【００５８】
利用者識別部２０は、チケットを受信すると、例えばそのチケットで索引されるログインＩＤと認証情報記憶部４０に記憶されているログインＩＤとを照合し、そのチケットで索引されるログインＩＤが認証情報記憶部４０に含まれる場合に、端末装置２の利用者がそのログインＩＤに対応するグループＩＤによって示される利用者であると識別する。
【００５９】
利用者が識別された後、図４と同様の動作が進行する。端末装置２は新たなチケットを受信すると、受信されたチケットで古いチケット情報を更新する（Ｓ９１）。
【００６０】
図８（Ａ）及び（Ｂ）は、この動作例において端末装置２に表示されるＩＤ使用結果の一例であり、ページＢがＩＤ３を使用してアクセスされ、さらにＩＤ１を使用してもアクセス可能であることを表している。ここでは、ＩＤ使用結果が画面の下端及びポップアップに表示される例を示す。なお、後述する説明の便宜上、ページＢはページＣへのリンクを含むものとする。
【００６１】
ここまでに述べたように、アクセス制御装置４は、アクセスに使用したログインＩＤを示すチケットを端末装置２に記憶させ、次のアクセスのときに端末装置２から受信されるチケットによってログインＩＤを特定することによって利用者を識別するので、アクセスの都度利用者がログインＩＤ及びパスワードを入力する必要がなくなり処理の迅速性が向上する。
【００６２】
しかも、前述したように、ひとたび利用者が識別されるとその利用者の全ての役割に対応するログインＩＤ及びパスワードを使用してアクセスリクエストが転送されるので、利用者にとって、単にページ（情報資源）をリクエストするだけで自らが兼任する役割のうち何れか一つのアクセス権が得られるという優れた利便性及び迅速性が発揮される。
【００６３】
次に、前述の動作に引き続いて、利用者がページＣをリクエストする場合の動作について説明する。
【００６４】
図９は、その場合の、端末装置２、アクセス制御装置４、及びサーバ装置６の連携動作の一例を示すフローチャートである。この動作は、図７の動作に引き続いて、アクセス制御装置４がページＣリクエスト情報を端末装置２から受信すると開始される。ページＣリクエスト情報は、例えば、ページＢに含まれるページＣへのリンク（図８（Ａ）及び（Ｂ）を参照）を、利用者がクリックすることによって送信される。

【００６５】
図９の動作は、チケットを利用する点で、図７の動作と実質的に同様である。
図１０（Ａ）及び（Ｂ）は、この動作例において端末装置２に表示されるＩＤ使用結果の一例であり、ページＣがＩＤ２を使用してアクセスされ、ページＣのアクセスに使用できるＩＤがこのＩＤ２のみであることを表している。ここでは、ＩＤ使用結果が画面の下端及びポップアップに表示される例を示す。
（変形例）
なお、本発明を実施の形態に基づいて説明してきたが、本発明は、前述した実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。
【００６６】
実施の形態では、履歴情報記憶部６０は利用者ごとにアクセスに使用されたログインＩＤを所定個数まで時系列順に保持し、試行順序決定部５０は履歴情報記憶部６０を参照して利用者のログインＩＤをより新しく使用された順に並べるとしたが、次のような変形を考えることもできる。
【００６７】
例えば、履歴情報記憶部６０は、履歴情報として、利用者ごとログインＩＤごとの使用回数（頻度）を保持し、試行順序決定部５０は利用者のログインＩＤを使用回数順に並べてもよい。
【００６８】
図１１（Ａ）は、そのような履歴情報の一具体例である。この履歴情報は履歴情報テーブル６１０に格納され、グループＩＤ欄６１１には利用者のＩＤが保持され、ＩＤ欄６１２にはその利用者が兼任する各役割に対応するログインＩＤが保持され、使用回数欄６１３にはその利用者がそのログインＩＤを使用した回数が保持される。
【００６９】
この構成によれば、実施の形態に比べて履歴情報のデータ量を削減できる。そして、長期的に見て使用回数の多い順にログインＩＤが使用されることとなるので、ログインＩＤの使用傾向の時間変動が少ない状況においてメモリ量を削減したい場合に好適である。
【００７０】
また、例えば、履歴情報記憶部６０は、履歴情報として、利用者ごと情報資源ごとログインＩＤごとの使用回数を保持し、試行順序決定部５０は利用者のログインＩＤを、リクエストする情報資源についての使用回数順に並べてもよい。
【００７１】
図１１（Ｂ）は、そのような履歴情報の一具体例である。この履歴情報は履歴情報テーブル６２０に格納され、グループＩＤ欄６２１には利用者のＩＤが保持され、情報資源欄６２２にはその利用者が少なくとも一つの役割でアクセス可能な情報資源のアドレスが保持され、ＩＤ欄６２３にはその情報資源をアクセスできるログインＩＤが保持され、使用回数欄６２４にはその利用者がその情報資源をそのログインＩＤを使用してアクセスした回数が保持される。
【００７２】
この構成によれば、情報資源ごとに使用回数の多い順にログインＩＤが使用されることとなるので、ログインＩＤの使用傾向が情報資源ごとに大きく異なる状況において使用傾向をより忠実に反映したい場合に好適である。
【００７３】
また、実施の形態では、アクセス試行部７０は、試行順序決定部５０によって並べられた順に全てのログインＩＤを使用してアクセスリクエストを転送する（図４のＳ５０を参照）としたが、リクエストに応じた情報が得られた場合、それ以降のログインＩＤを用いる転送を抑止してもよい。
【００７４】
図１２は、そのような動作の一例を示すフローチャートである。アクセス試行部７０は、並べられた順にログインＩＤを一つ選択し（Ｓ５１）、そのログインＩＤを使用してア

クセスリクエストを転送し（Ｓ５２）、アクセス拒否された場合のみ（Ｓ５３：ＹＥＳ）、次のログインＩＤを使用してさらにリクエストを転送する。

【００７５】

この構成によれば、リクエストした情報が得られた時点以降のリクエストの転送が抑止されるので、通信トラフィック量の削減と処理時間の短縮とが実現される。

【００７６】

また、実施の形態では、利用者は、自らを識別する識別情報として認証情報記憶部４０に記憶されているログインＩＤ及びパスワードの何れか一組を入力するとしたが、この識別情報は、認証情報記憶部４０に記憶されているログインＩＤ及びパスワードの組に限定されるものでない。例えば、認証情報記憶部４０に記憶されているグループＩＤと図示しない一つのパスワードとの組が、利用者を識別する識別情報として利用できることは明らかである。さらには、高度に偽装困難な本人証明性を持つＰＫＩ（Public Key Infrastructure）情報を識別情報として用いることも考えられる。

【００７７】

また、実施の形態では、兼任する役割ごとにアクセス権を使い分ける利用者の例を用いたが、本発明のアクセス制御装置が優れた効果を発揮する場面は、この例に限られるものではない。例えば、コンピュータシステムごとにアクセス権を使い分ける利用者が行うアクセスについても、本発明のアクセス制御装置によって効果的な制御が可能である。すなわち、それらのコンピュータシステムが、それぞれ具体的にネットワークバンキングシステム、航空券予約システム、ネットワーク通販システム等として機能している場合を考えれば、利用者は、それらのシステムごとのログインＩＤ及びパスワードの組のうち何れか一つ（例えば、最も覚えやすい一つ、又はたまたま思い出した一つ）を用いてひとたび識別を受けた後は、どのシステムにもログインできるという、極めて優れた利便性を享受できる。

【００７８】

実施の形態、及びこの変形例で説明した機能は、プログラムと、ＣＰＵ、ＲＡＭ、ＲＯＭ、不揮発性メモリ等のハードウェア資源との組み合わせにより、集積回路であるＬＳＩ（Large Scale Integration）として実現されてもよい。各機能は、個別に１チップ化されてもよいし、複数の機能の全部又は一部が１チップ化されてもよい。

【００７９】

集積回路化の一例として、図１におけるアクセス制御装置４が集積回路であるとしてもよい。集積回路は、集積度の違いにより、ＩＣ（Integrated Circuit）、システムＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩと呼称されることもある。

【００８０】

集積回路、ＬＳＩに限るものではなく、専用回路又は汎用プロセサにより実現されてもよい。ＬＳＩ製作後にプログラムを格納することが可能なＦＰＧＡ（Field Programmable Gate Array）や、ＬＳＩ内部の回路セルの接続や設定を再構成することが可能なリコンフィギュラブル・プロセサが利用されてもよい。

【００８１】

更には、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然その技術を用いて上記機能の集積回路化が行われてもよい。バイオ技術の適用等が可能性としてあり得る。

【産業上の利用可能性】

【００８２】

本発明に係るアクセス制御装置は、複数のアクセス権を使い分ける利用者が行うアクセスを効率的に制御する装置、例えば、ワークフローシステムにおける利用者の識別とアクセス要求の転送とを行うゲートウェイサーバ等として利用できる。

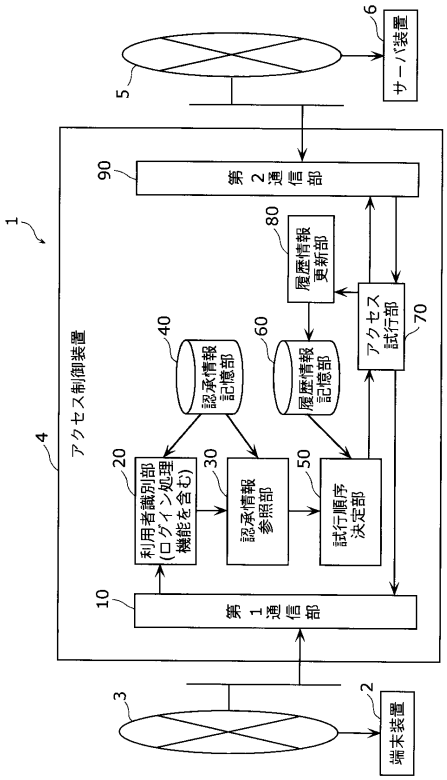
【図面の簡単な説明】

【００８３】

【図１】本発明の一実施の形態に係るアクセス制御装置を含む情報処理システムの全体構

成を示す機能ブロック図である。
【図２】認証情報記憶部に記憶されている認証情報の一具体例を示す図である。
【図３】履歴情報記憶部に記憶されている履歴情報の一具体例を示す図である。
【図４】動作の一例を示すフローチャートである。
【図５】（Ａ）及び（Ｂ）端末装置に表示されるログインプロンプトの一例を示す図である。
【図６】（Ａ）及び（Ｂ）端末装置に表示されるＩＤ使用結果の一例を示す図である。
【図７】動作の一例を示すフローチャートである。
【図８】（Ａ）及び（Ｂ）端末装置に表示されるＩＤ使用結果の一例を示す図である。
【図９】動作の一例を示すフローチャートである。
【図１０】（Ａ）及び（Ｂ）端末装置に表示されるＩＤ使用結果の一例を示す図である。
【図１１】（Ａ）及び（Ｂ）履歴情報の一変形例を示す図である。
【図１２】動作の一変形例を示すフローチャートである。
【図１３】利用者に応じたアクセス制御を行う従来の情報処理システムの典型例を示す図である。
【図１４】利用者に応じたアクセス制御に用いられる従来の利用者情報の一具体例を示す図である。
【符号の説明】
【００８４】
１　情報処理システム
２　端末装置
３　第１通信網
４　アクセス制御装置
５　第２通信網
６　サーバ装置
１０　第１通信部
２０　利用者識別部
３０　認証情報参照部
４０　認証情報記憶部
５０　試行順序決定部
６０　履歴情報記憶部
７０　アクセス試行部
８０　参照履歴更新部
８０　履歴情報更新部
９０　第２通信部
１００　情報処理システム
１０１　端末装置
１０２　サーバ装置
１０４　ネットワーク
２００　利用者情報テーブル
４００　認証情報テーブル
６００、６２０　履歴情報テーブル

【図１】




【図２】

400

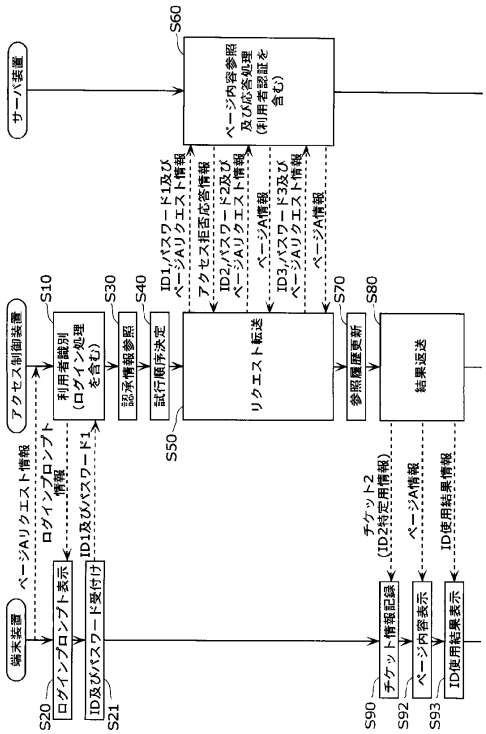
| 401 グループID | 402 ID | 403 パスワード |
|---|---|---|
| G0001234 | 0000001 | jfN2jdG＄ |
| | 0040024 | 9JrnqP45 |
| | 0070523 | Uf03Mfd! |
| G0002955 | 0010312 | 0!&gjoWE |
| | | |

【図３】

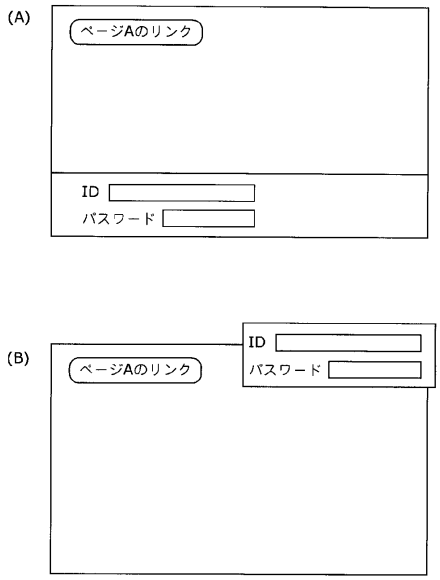
600

| 601 グループID | 602 ID |
|---|---|
| G0001234 | 0070523 |
| | 0040024 |
| | 0000001 |
| | 0000001 |
| | 0070523 |
| | 0000001 |
| | 0000001 |
| | 0040024 |
| | 0040024 |
| | 0070523 |
| | |

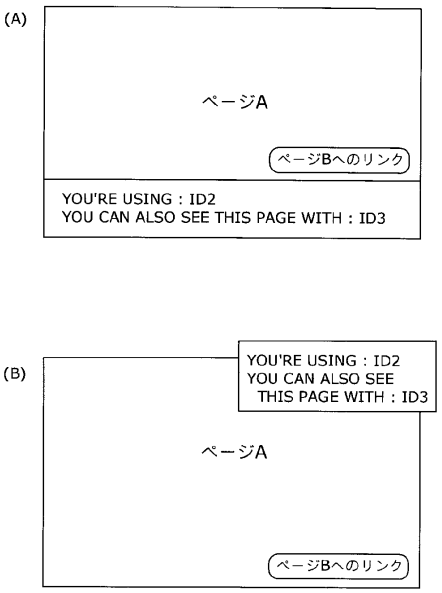
【図４】



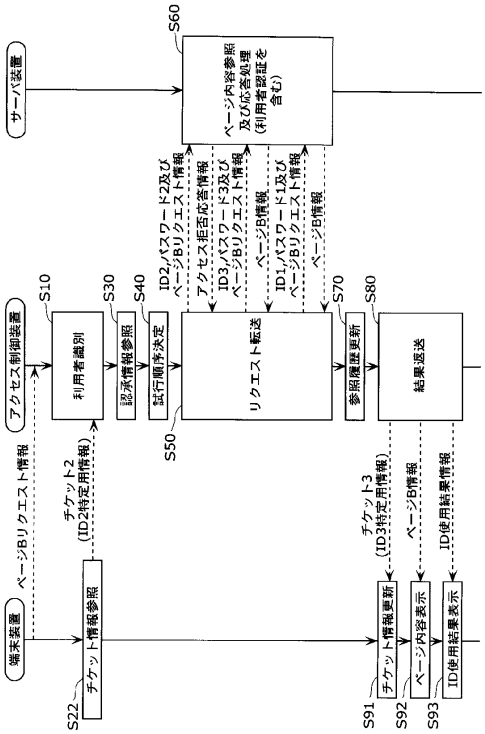
【図５】


(A)
ページAのリンク
ID
パスワード
(B)
ページAのリンク
ID
パスワード

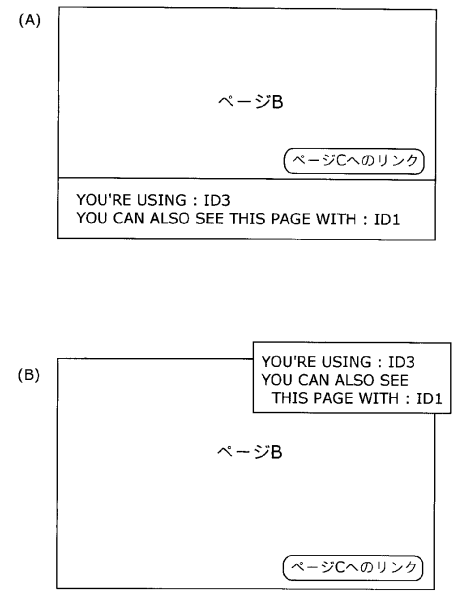
【図６】


(A)
ページA
ページBへのリンク
YOU'RE USING : ID2
YOU CAN ALSO SEE THIS PAGE WITH : ID3
(B)
YOU'RE USING : ID2
YOU CAN ALSO SEE
THIS PAGE WITH : ID3
ページA
ページBへのリンク

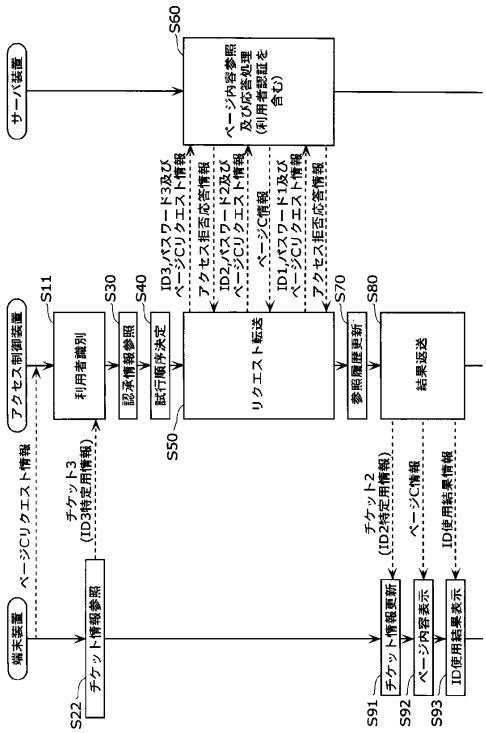
【図７】


サーバ装置
アクセス制御装置
端末装置
S10
S30
S40
S50
S60
S70
S80
S22
S91
S92
S93
利用者識別
認証情報参照
試行順序決定
リクエスト転送
ページ内容参照及び応答処理(利用者認証を含む)
参照履歴更新
結果返送
チケット情報参照
チケット情報更新
ページ内容表示
ID使用結果表示
ページBリクエスト情報
チケット2(ID2特定用情報)
ID2,パスワード2及びページBリクエスト情報
アクセス拒否応答情報
ID3,パスワード3及びページBリクエスト情報
ページB情報
ID1,パスワード1及びページBリクエスト情報
ページB情報
チケット3(ID3特定用情報)
ページB情報
ID使用結果情報

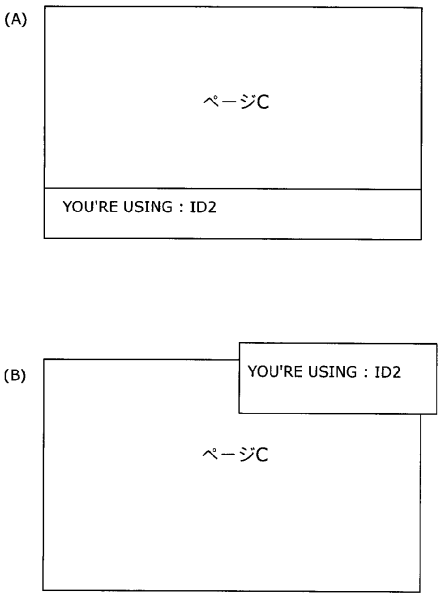
【図８】


(A)
ページB
ページCへのリンク
YOU'RE USING : ID3
YOU CAN ALSO SEE THIS PAGE WITH : ID1
(B)
YOU'RE USING : ID3
YOU CAN ALSO SEE
THIS PAGE WITH : ID1
ページB
ページCへのリンク

【図９】




【図１０】




【図１１】

(A)

610

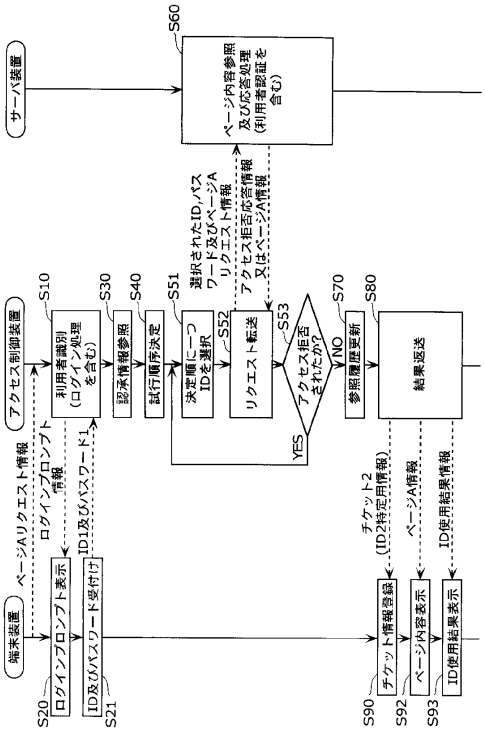
| 611 IDグループ | 612 ID | 613 使用回数 |
|---|---|---|
| G0001234 | 0000001 | 394 |
| | 0040024 | 72 |
| | 0070523 | 15 |

(B)

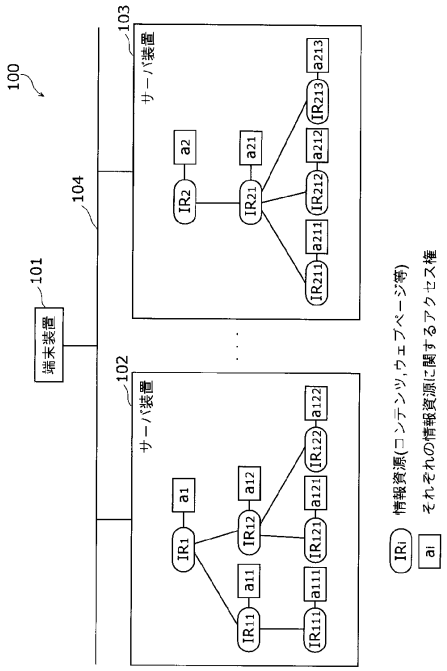
620

| 621 IDグループ | 622 情報資源(WEBページ) | 623 ID | 624 使用回数 |
|---|---|---|---|
| G0001234 | ページA | 0000001 | 21 |
| | | 0040024 | 210 |
| | ページB | 0000001 | 185 |
| | | 0040024 | 4 |
| | | 0070523 | 72 |
| | ページC | 0070523 | 103 |
| | ページD | 0000001 | 321 |
| | | 0040024 | 184 |
| | | 0070523 | 15 |

【図１２】



【図１３】




【図１４】

200

| 201 グループID | 202 ID | 203 パスワード | 204 情報資源 |
|---|---|---|---|
| G0001234 | 0000001 | jfN2jdG$ | IR1, IR2 |
| | 0040024 | 9JrnqP45 | IR2, IR21, IR211 |
| | 0070523 | Uf03Mfd! | IR1, IR12, IR121, IR122 |
| | | | |

フロントページの続き

(56)参考文献 特開２００２－２７８９３０（ＪＰ，Ａ）
特開２００２－２１５５８６（ＪＰ，Ａ）
特開２００４－０２９８９０（ＪＰ，Ａ）
特開２００４－２３４３２９（ＪＰ，Ａ）
特開２００２－０７３５６２（ＪＰ，Ａ）
特開２００１－０７５６６７（ＪＰ，Ａ）
特開平０６－０６０２３５（ＪＰ，Ａ）
特開平０２－０６４８８８（ＪＰ，Ａ）
特開平０２－００２４７５（ＪＰ，Ａ）
特開昭６３－０２０６８０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１
Ｇ０９Ｃ
Ｈ０４Ｌ　９