(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3576008号
(P3576008)
(45)発行日　平成16年10月13日(2004.10.13)　(24)登録日　平成16年7月16日(2004.7.16)

(51)Int.Cl.[7]　F I
G06F 15/00　G06F 15/00　330B
G06F 12/00　G06F 12/00　537A

請求項の数 10　(全 24 頁)

(21)出願番号　特願平10-288106
(22)出願日　平成10年10月9日(1998.10.9)
(65)公開番号　特開2000-112891(P2000-112891A)
(43)公開日　平成12年4月21日(2000.4.21)
審査請求日　平成13年2月6日(2001.2.6)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100084618
弁理士　村松　貞男
(74)代理人　100068814
弁理士　坪井　淳
(74)代理人　100092196
弁理士　橋本　良郎
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠

最終頁に続く

(54)【発明の名称】アクセス制御設定システム及び記憶媒体

(57)【特許請求の範囲】
【請求項１】
分散した複数の計算機上のリソースに対するアクセス権の設定を行うためのアクセス制御設定システムであり、
前記リソースへのアクセス許諾を受ける抽象的なユーザ名及びそのアクセス権内容を記述したアクセス権設定パターンを１以上格納するアクセス権設定パターン格納部と、
前記アクセス権の設定を行うために、前記アクセス権設定パターンの何れかを選択する選択手段と、
前記抽象的なユーザ名に対応したグループ毎の実ユーザ名群からなるユーザ情報を、１グループ以上について格納するユーザ情報格納部と、
前記選択手段にて選択されたアクセス権設定パターンに、前記ユーザ情報格納部に格納されかつアクセス権設定対象となるグループの実ユーザ名群を当てはめて、前記アクセス権の設定を行うために用いられるアクセスコントロールリストを生成するアクセスコントロールリスト生成手段と
を具備し、
前記アクセスコントロールリスト生成手段は、前記リソースによって異なるフォーマット情報を保持しており、前記リソースで使用できるように前記フォーマット情報にしたがって、前記リソースにそれぞれ対応して前記アクセスコントロールリストを作成する
ことを特徴とするアクセス制御設定システム。
【請求項２】

分散した複数の計算機上のリソースに対するアクセス権の設定を行うためのアクセス制御設定システムであり、
前記リソースへのアクセス許諾を受ける抽象的なユーザ名及びそのアクセス権内容を記述したアクセス権設定パターンを１以上格納するアクセス権設定パターン格納部と、
前記アクセス権の設定を行うために、前記アクセス権設定パターンの何れかを選択する選択手段と、
前記抽象的なユーザ名からなるアクセス権設定パターンに基づいて、前記アクセス権の設定を行うために用いられるアクセスコントロールリストを生成するアクセスコントロール生成手段と
を具備し、
前記アクセスコントロールリスト生成手段は、前記リソースによって異なるフォーマット情報を保持しており、前記リソースで使用できるように前記フォーマット情報にしたがって、前記リソースにそれぞれ対応して前記アクセスコントロールリストを作成する
ことを特徴とするアクセス制御設定システム。
【請求項３】
分散した複数の計算機上のリソースに対するアクセス権の設定を行うためのアクセス制御設定システムであり、
前記リソースへのアクセス許諾を受ける抽象的なユーザ名及びそのアクセス権内容を記述したアクセス権設定パターンを１以上格納するアクセス権設定パターン格納部と、
前記アクセス権の設定を行うために、前記アクセス権設定パターンの何れかを選択する選択手段と、
前記抽象的なユーザ名に対応したグループ毎の実ユーザ名群からなるユーザ情報を、１グループ以上について格納するユーザ情報格納部と、
前記選択手段にて選択されたアクセス権設定パターンに、前記ユーザ情報格納部に格納されかつアクセス権設定対象となるグループを当てはめて、前記アクセス権の設定を行うために用いられるアクセスコントロールリストを生成するアクセスコントロールリスト生成手段と
を具備し、
前記アクセスコントロールリスト生成手段は、前記リソースによって異なるフォーマット情報を保持しており、前記リソースで使用できるように前記フォーマット情報にしたがって、前記リソースにそれぞれ対応して前記アクセスコントロールリストを作成する
ことを特徴とするアクセス制御設定システム。
【請求項４】
請求項１乃至請求項３のいずれか１項に記載のアクセス制御設定システムにおいて、
前記アクセス権設定対象となるリソースを直接管理する計算機上に設けられ、かつ、前記アクセスコントロールリスト生成手段が生成したアクセスコントロールリストを当該リソースについて設定することでアクセス権設定を実行するアクセスコントロールリスト設定手段をさらに具備することを特徴とするアクセス制御設定システム。
【請求項５】
請求項１乃至請求項４のいずれか１項に記載のアクセス制御設定システムにおいて、
前記アクセス権設定対象となるリソースを直接管理する計算機上に設けられ、かつ、前記アクセスコントロールリストを作成するのに用いる前記リソースの所属情報を収集するリソース情報収集手段をさらに具備し、
前記選択手段は、前記リソース情報収集手段に指令して情報収集させるとともに、この情報収集対象となるリソースを前記アクセス権設定対象として指定する
ことを特徴とするアクセス制御設定システム。
【請求項６】
請求項１乃至請求項５のいずれか１項に記載のアクセス制御設定システムにおいて、
前記選択手段は、前記リソースを直接管理する計算機とは異なる計算機上に設けられ、両計算機の情報の授受はネットワークを介して行うことを特徴とするアクセス制御設定シ

ステム。
【請求項７】
分散した複数の計算機上のリソースに対するアクセス権を設定させるためのアクセス制御設定システムを制御するプログラムを記憶したコンピュータ読み取り可能な記憶媒体であって、
コンピュータを、
前記リソースへのアクセス許諾を受ける抽象的なユーザ名及びそのアクセス権内容を記述したアクセス権設定パターンを１以上格納させたアクセス権設定パターン格納部から当該パターンを読み出させるアクセス権設定パターン管理手段、
前記アクセス権の設定を行うために、前記アクセス権設定パターンの何れかを選択させる選択手段、
前記抽象的なユーザ名に対応したグループ毎の実ユーザ名群からなるユーザ情報を、１グループ以上について格納させたユーザ情報格納部からユーザ情報を読み出させるユーザ情報管理手段、
前記選択手段にて選択されたアクセス権設定パターンに、前記ユーザ情報格納部に格納されかつアクセス権設定対象となるグループの実ユーザ名群を当てはめさせて、前記アクセス権の設定を行うために用いられるアクセスコントロールリストを生成させるアクセスコントロールリスト生成手段
として機能させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体であり、
前記アクセスコントロールリスト生成手段は、前記リソースによって異なるフォーマット情報にしたがって、前記リソースで使用できるように前記リソースにそれぞれ対応して前記アクセスコントロールリストを作成させる
ことを特徴とする記憶媒体。
【請求項８】
分散した複数の計算機上のリソースに対するアクセス権を設定させるためのアクセス制御設定システムを制御するプログラムを記憶したコンピュータ読み取り可能な記憶媒体であって、
コンピュータを、
前記リソースへのアクセス許諾を受ける抽象的なユーザ名及びそのアクセス権内容を記述したアクセス権設定パターンを１以上格納させたアクセス権設定パターン格納部から当該パターンを読み出させるアクセス権設定パターン管理手段、
前記アクセス権の設定を行うために、前記アクセス権設定パターンの何れかを選択させる選択手段、
前記抽象的なユーザ名からなるアクセス権設定パターンに基づいて、前記アクセス権の設定を行うために用いられるアクセスコントロールリストを生成させるアクセスコントロール生成手段
として機能させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体であり、
前記アクセスコントロールリスト生成手段は、前記リソースによって異なるフォーマット情報にしたがって、前記リソースで使用できるように、前記リソースにそれぞれ対応して前記アクセスコントロールリストを作成させる
ことを特徴とする記憶媒体。
【請求項９】
分散した複数の計算機上のリソースに対するアクセス権を設定させるためのアクセス制御設定システムを制御するプログラムを記憶したコンピュータ読み取り可能な記憶媒体であって、
コンピュータを、
前記リソースへのアクセス許諾を受ける抽象的なユーザ名及びそのアクセス権内容を記述したアクセス権設定パターンを１以上格納させたアクセス権設定パターン格納部から当該

パターンを読み出させるアクセス権設定パターン管理手段、
前記アクセス権の設定を行うために、前記アクセス権設定パターンの何れかを選択する選択手段、
前記抽象的なユーザ名に対応したグループ毎の実ユーザ名群からなるユーザ情報を、１グループ以上について格納させたユーザ情報格納部からユーザ情報を読み出させるユーザ情報管理手段、
前記選択手段にて選択されたアクセス権設定パターンに、前記ユーザ情報格納部に格納されかつアクセス権設定対象となるグループを当てはめさせて、前記アクセス権の設定を行うために用いられるアクセスコントロールリストを生成させるアクセスコントロールリスト生成手段
として機能させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体であり、
前記アクセスコントロールリスト生成手段は、前記リソースによって異なるフォーマット情報にしたがって、前記リソースで使用できるように、前記リソースにそれぞれ対応して前記アクセスコントロールリストを作成させる
ことを特徴とする記憶媒体。
【請求項１０】
請求項７乃至請求項９のいずれか１項に記載の記憶媒体において、
コンピュータを、
前記アクセス権設定対象となるリソースを直接管理する計算機上に設けられ、かつ、前記アクセスコントロールリスト生成手段が生成したアクセスコントロールリストを当該リソースについて設定することでアクセス権設定を実行させるアクセスコントロールリスト設定手段
として機能させるプログラムをさらに記憶したことを特徴とする記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
この発明はアクセス制御設定システム及び記憶媒体、特に複数の部門あるいはサイトに分散した計算機上のリソースに対するアクセス権の設定を行うのに適したアクセス制御設定システム及び記憶媒体に関するものである。
【０００２】
【従来の技術】
近年は計算機同士が接続されてネットワークが形成され、ある計算機から他の計算機にアクセスすることが容易となり、また、単一の計算機を複数人が使用することもある。したがって、計算機上のリソース（ファイルシステム上のファイル、ＷＷＷサーバ上のＷＷＷコンテンツ、各種デバイス等）に対するアクセスを管理することが重要になってきている。
【０００３】
このような計算機上のリソースに対するアクセス権を設定する場合には、そのリソースを管理するサーバあるいはＯＳ（オペレーティングシステム）等に対して、それぞれ個別にその権限を設定する必要がある。この設定を行うには、設定対象の計算機にログインして設定作業を行うのが一般的である。
【０００４】
具体的には、各サーバ等に対し、「ユーザ１に対しては読み出しと書き込みを許可し、ユーザ２、ユーザ３、ユーザ４に対しては読み出しのみを許可する」というような形式でアクセス権情報（以下、ＡＣＬ（アクセスコントロールリスト）ともいう）が個別に設定される。
【０００５】
【発明が解決しようとする課題】
設定されるアクセス権情報は「システム管理者には読み出しと書き込みを許可するが、一

般ユーザには読み出しのみ許可する」等のような一定のパターンに当てはまる場合が多い。

【０００６】

しかし、「システム管理者」や「一般ユーザ」に対応する実際のユーザは、部門あるいはサイトごとに異なっている。例えば、部門Ａでは「システム管理者＝ユーザａ，一般ユーザ＝ユーザｂ，ユーザｃ，ユーザｄ」であり、部門Ｂでは「システム管理者＝ユーザα，一般ユーザ＝ユーザβ，ユーザγ」であるかのごとくである。

【０００７】

従来のアクセス権設定方法では、各部門等でその構成メンバが異ることからして当然に、アクセス権設定対象のリソース毎にそれぞれ個別のアクセス権を設定する必要がある。

【０００８】

上記例に当てはめれば、部門Ａが保有する計算機上のリソースに対しては、「ユーザａに対しては読み出しと書き込みを許可し、ユーザｂ、ユーザｃ、ユーザｄに対しては読み出しのみを許可する」というアクセス権を設定する。また、部門Ｂが保有する計算機上のリソースに対しては、「ユーザαに対しては読み出しと書き込みを許可し、ユーザβ、ユーザγに対しては読み出しのみを許可する」というアクセス権を設定する。

【０００９】

このように、設定されるべきアクセス権情報のパターンが同一であっても、実際にはそれぞれ異なるアクセス権情報に対応した権限設定を行う必要があるため、アクセス権設定者の負担を軽減するのが困難である。

【００１０】

また、複数の部門あるいはサイトに分散した計算機が連携して処理を行うような分散処理システムにおいては、各計算機上のリソースに対してアクセス権を設定してアクセス制御を行い得るようにするために、アクセス権設定者の負担は過大なものとなる。アクセス権設定者は、この設定のために各計算機に一々ログインする等し、ログインした計算機上で個別のアクセス権設定処理を行う必要があるからである。

【００１１】

本発明は、このような実情を考慮してなされたもので、部門やサイトに依存せず効率的にリソースへのアクセス権を設定することを可能にし、また、設定対象の計算機にその都度ログインすることなしに当該設定を可能として、ひいては設定の手間を軽減し設定ミスを防止できるアクセス制御設定システム及び記憶媒体を提供することを目的とする。

【００１２】

【課題を解決するための手段】

上記課題を解決するために、請求項１に対応する発明は、計算機上のリソースに対するアクセス権の設定を行うためのアクセス制御設定システムについてなされたものである。

【００１３】

このシステムは、分散した複数のリソースへのアクセス許諾を受ける抽象的なユーザ名及びそのアクセス権内容を記述したアクセス権設定パターンを１以上格納するアクセス権設定パターン格納部と、アクセス権の設定を行うために、アクセス権設定パターンの何れかを選択する選択手段と、抽象的なユーザ名に対応したグループ毎の実ユーザ名群からなるユーザ情報を、１グループ以上について格納するユーザ情報格納部と、選択手段にて選択されたアクセス権設定パターンに、ユーザ情報格納部に格納されかつアクセス権設定対象となるグループの実ユーザ名群を当てはめて、アクセス権の設定を行うために用いられるアクセスコントロールリストを生成するアクセスコントロールリスト生成手段とを具備する。

【００１４】

アクセスコントロールリスト生成手段は、リソースによって異なるフォーマット情報を保持しており、リソースで使用できるようにフォーマット情報にしたがって、リソースにそれぞれ対応して前記アクセスコントロールリストを作成する。

このように、アクセス権設定パターンを用いることで、部門やサイトに依存せず効率的に

リソースへのアクセス権を設定することができる。

【００１５】

また、部門等における役職名等を抽象的なユーザ名に対応させることで、より一層、部門やサイトに依存しないアクセス権設定が容易なものとなる。

【００１８】

また、設定者は一々アクセスコントロールリストを記述する必要がなく、アクセス権設定が一層容易なものとなり設定者の負担が低減される。特に、アクセス権設定対象となるリソースが多数の場合に、設定者の負荷低減効果が大きい。

【００１９】

次に、請求項２に対応する発明は、分散した複数の計算機上のリソースに対するアクセス権の設定を行うためのアクセス制御設定システムであり、リソースへのアクセス許諾を受ける抽象的なユーザ名及びそのアクセス権内容を記述したアクセス権設定パターンを１以上格納するアクセス権設定パターン格納部と、アクセス権の設定を行うために、アクセス権設定パターンの何れかを選択する選択手段と、抽象的なユーザ名からなるアクセス権設定パターンに基づいて、アクセス権の設定を行うために用いられるアクセスコントロールリストを生成するアクセスコントロール生成手段とを具備し、アクセスコントロールリスト生成手段は、リソースによって異なるフォーマット情報を保持しており、リソースで使用できるようにフォーマット情報にしたがって、リソースにそれぞれ対応して前記アクセスコントロールリストを作成するアクセス制御設定システムである。

【００２０】

したがって、設定者は一々アクセスコントロールリストを記述する必要がなく、アクセス権設定が一層容易なものとなり設定者の負荷が低減される。

次に、請求項３に対応する発明は、分散した複数の計算機上のリソースに対するアクセス権の設定を行うためのアクセス制御設定システムであり、リソースへのアクセス許諾を受ける抽象的なユーザ名及びそのアクセス権内容を記述したアクセス権設定パターンを１以上格納するアクセス権設定パターン格納部と、アクセス権の設定を行うために、アクセス権設定パターンの何れかを選択する選択手段と、抽象的なユーザ名に対応したグループ毎の実ユーザ名群からなるユーザ情報を、１グループ以上について格納するユーザ情報格納部と、選択手段にて選択されたアクセス権設定パターンに、ユーザ情報格納部に格納されかつアクセス権設定対象となるグループを当てはめて、アクセス権の設定を行うために用いられるアクセスコントロールリストを生成するアクセスコントロールリスト生成手段とを具備し、アクセスコントロールリスト生成手段は、リソースによって異なるフォーマット情報を保持しており、リソースで使用できるようにフォーマット情報にしたがって、リソースにそれぞれ対応してアクセスコントロールリストを作成するアクセス制御設定システムである。

したがって、人事異動等でグループ内のメンバが変更された場合でも、アクセス権設定の実質内容を容易に対応させることができる。

次に、請求項４に対応する発明は、請求項１～３に対応する発明において、アクセス権設定対象となるリソースを直接管理する計算機上にアクセスコントロールリスト設定手段が設けられる。

【００２１】

このアクセスコントロールリスト設定手段により、アクセスコントロールリスト生成手段が生成したアクセスコントロールリストが当該リソースについて設定されアクセス権設定が実行される。

【００２２】

したがって、リソース管理計算機上にて自動的にアクセスコントロールリストを設定させることができる。これにより、アクセス権設定のために当該計算機に一々ログインする必要をなくすことができ、ひいてはアクセス権設定者の労力を低減させることができる。

【００２４】

次に、請求項５に対応する発明は、請求項１～４に対応する発明において、アクセス権設

定対象となるリソースを直接管理する計算機上にリソース情報収集手段が設けられている。

【００２５】

このリソース情報収集手段によって、アクセスコントロールリストを作成するのに用いる前記リソースの所属情報が収集される。

さらに、選択手段からは、リソース情報収集手段に対して情報収集させる旨が指令され、この情報収集対象となるリソースがアクセス権設定対象として指定される。

【００２６】

したがって、アクセス権設定について選択手段からの集中管理を行うことができる。

次に、請求項６に対応する発明は、請求項１～５に対応する発明において、選択手段は、リソースを直接管理する計算機とは異なる計算機上に設けられ、両計算機間の情報の授受はネットワークを介して行われる。

【００２７】

したがって、アクセス権設定者は選択手段が設けられた計算機から、全てのリソースに対するアクセス権設定をリソース管理計算機にログインすることなく容易に行うことができる。これにより、設定者の負担は低減される。

【００２８】

次に、請求項７に対応する発明は、請求項１に対応する発明を１乃至複数のコンピュータに実現させるプログラムを記憶した記憶媒体である。

この記憶媒体から読み出されたプログラムにより制御されるコンピュータは、請求項１のアクセス制御設定システムとして機能する。

【００２９】

次に、請求項８に対応する発明は、請求項２に対応する発明を１乃至複数のコンピュータに実現させるプログラムを記憶した記憶媒体である。

この記憶媒体から読み出されたプログラムにより制御されるコンピュータは、請求項２のアクセス制御設定システムとして機能する。

【００３０】

次に、請求項９に対応する発明は、請求項３に対応する発明を１乃至複数のコンピュータに実現させるプログラムを記憶した記憶媒体である。

この記憶媒体から読み出されたプログラムにより制御されるコンピュータは、請求項３のアクセス制御設定システムとして機能する。

【００３１】

次に、請求項１０に対応する発明は、請求項４に対応する発明を１乃至複数のコンピュータに実現させるプログラムを記憶した記憶媒体である。

この記憶媒体から読み出されたプログラムにより制御されるコンピュータは、請求項４のアクセス制御設定システムとして機能する。

【００３２】

【発明の実施の形態】

以下、本発明の実施の形態について説明する。

（発明の第１の実施の形態）

図１は本発明の第１の実施の形態に係るアクセス制御設定システムを適用する計算機システムの構成例を示すブロック図である。

【００３３】

この計算機システムは、ネットワーク１を介して設定・管理部門２、Ａ部門３、Ｂ部門４、Ｃ部門５、．．．の各部門のＬＡＮが接続されて構成されている。設定・管理部門２のＬＡＮは、ルータ６を介してネットワーク１に接続されるとともに、そのデータ伝送路７に設定管理サーバ８とディレクトリサーバ９とが接続されて構成されている。この設定・管理部門２は、アクセス権の設定や管理を行う部門である。

【００３４】

各部門３、４、５、．．例えばＡ部門３のＬＡＮは、ルータ１０を介してネットワーク１

に接続されるとともに、そのデータ伝送路１１に複数の計算機１２が接続されて構成されている。ＬＡＮに接続された各計算機１２には、ＷＷＷサーバ１３、コンテンツ情報送信部１４及びＡＣＬ設定部１５が設けられている。本実施形態では、各部門３、４、５、．．．の各計算機１２におけるリソースがアクセス権設定される対象となる。

【００３５】

図２は本実施形態におけるアクセス制御設定システムの機能構成を示すブロック図である。

このアクセス制御設定システムは、設定・管理部門２に設けられたアクセス権設定部２１、ＡＣＬ変換部２２、アクセス権設定パターン管理部２３、記憶装置（図示せず）に格納されたアクセス権設定パターン群２４、ユーザ情報管理部２５及び記憶装置（図示せず）に格納されたユーザ情報２６と、各部門の計算機１２に設けられたコンテンツ情報送信部１４及びＡＣＬ設定部１５をその主要構成としている。

【００３６】

設定・管理部門２における上記構成のうち、本実施形態では、設定管理サーバ８に、アクセス権設定部２１、ＡＣＬ変換部２２、アクセス権設定パターン管理部２３及びアクセス権設定パターン群２４が設けられている。また、ディレクトリサーバ９には、ユーザ情報管理部２５及びユーザ情報２６が設けられている。なお、これらの各構成は、設定・管理部門２に配置されるのであれば、同一の計算機上に設けても構わないし、さらに多数の計算機上に分散して設けてもよい。

【００３７】

アクセス権設定部２１は、入力装置２７を介してアクセス権設定者の入力を受け付け、各部門３等における計算機１２上のＷＷＷサーバ１３に対し、設定・管理部門２からのアクセス権設定処理を可能とする。

【００３８】

このためにアクセス権設定部２１は、計算機１２上のコンテンツ情報送信部１４からコンテンツ情報を受信すると共に、アクセス権設定パターン管理部２３を介してアクセス権設定パターン群２４からアクセス権設定パターンを取得する。さらに取得した設定パターン及び権限設定対象情報をＡＣＬ変換部２２に与えて、同変換部２２にＡＣＬ作成を依頼する。

【００３９】

アクセス権設定パターン管理部２３は、アクセス権設定パターン群２４を管理し、アクセス権設定部２１の要求に応じてアクセス権設定パターンを登録、検索、削除等する。

【００４０】

アクセス権設定パターン群２４は、図３に示すようなアクセス権の設定パターンの集合である。

図３はアクセス権設定パターン群の一例を示す図である。

【００４１】

同図には二つの設定パターンが例示されている。パターン＃１は、「部長と課長に読み出し権限を与え、システム管理者には読み出し権限と実行権限を与える。」というパターンである。また、パターン＃２は、「部長と課長に読み出し権限と実行権限を与え、一般部員には読み出し権限のみを与える。」というパターンである。

【００４２】

ここで、図３における「部長」「課長」「システム管理者」及び「一般部員」は、抽象的なユーザ名であり実際にアクセス権限を設定する対象となるユーザではない。この抽象的なユーザ名から実際のユーザ名への変換は、ユーザ情報２６に基づいて行われるようになっている。

【００４３】

ユーザ情報管理部２５は、ユーザ情報２６を管理し、同情報を登録、検索又は削除等する。本実施形態では同管理部２５の機能は、ＬＤＡＰ（Ｌｉｇｈｔｗｅｉｇｈｔ　Ｄｉｒｅｃｔｏｒｙ　Ａｃｃｅｓｓ　Ｐｒｏｔｏｃｏｌ）に準拠したディレクトリサーバ機能で実

現される。なお、同様な機能であれば他の方法で実現してもよい。また、ディレクトリサーバとは、ＬＤＡＰ等により会社や研究機関等における人員の情報を集中的に管理するための計算機であり、特に図示しない他の入出力手段により、常時最新の部門情報や個人情報が登録更新されている。

【００４４】

ユーザ情報２６は、図４に示すようなユーザ名（ユーザＩＤ）と抽象的なユーザ名（役職など）の対応表に相当する情報がディレクトリサーバに管理されたものである。

【００４５】

図４はある部門（Ａ部門）のユーザ情報の例を示す図である。

図５は他の部門（Ｂ部門）のユーザ情報の例を示す図である。

次に、ＡＣＬ変換部２２は、アクセス権設定部２１からのＡＣＬ作成指令を受けると、アクセス権設定部２１から取得した部門名により、ユーザ情報管理部２５に依頼して対応するユーザ情報を取り出す。さらに、当該ユーザ情報をアクセス権設定部２１より取得した設定パターンに当てはめ、ＷＷＷコンテンツ２８に実際に設定するアクセス権情報（アクセスコントロールリスト：ＡＣＬ）を生成する。

【００４６】

図６はＡＣＬ変換部により生成されるＡＣＬの例を示す図である。

同図（ａ）は、ＡＣＬファイルの具体的な内容例を示している。ここで”ｐａｔｈ”は、アクセス権設定対象となる計算機上のパス情報を示し、”ａｌｌｏｗ”は読出や書込、実行等の許可の内容を示す。さらに”ｕｓｅｒ”は、ある”ａｌｌｏｗ”の対象となる具体的なユーザ名を示している。

【００４７】

図６（ｂ）及び図６（ｃ）には、図３に示すアクセス権設定パターン群２４のパターン＃１に対し、ＡＣＬ変換部２２によりそれぞれ図４及び図５のユーザ情報が当てはめられた例が示されている。なお、同図（ｂ）、（ｃ）に示す内容が同図（ａ）のような情報に変換されてＡＣＬファイルとなる。

【００４８】

例えば図６（ｂ）の場合では、設定パターン＃１がＡ部門３が保有するＷＷＷサーバ１３ａ上のＷＷＷコンテンツ２８ａに設定する場合が想定されている。すなわちアクセス権

部長＝読み出し権限

課長＝読み出し権限

システム管理者＝読み出し権限、実行権限

に対して、「部長→鈴木」「課長→佐藤」「システム管理者→高橋、田中」という変換がＡＣＬ変換部２２にて施され、図６（ｂ）に示す内容のＡＣＬファイルが作成されて、Ａ部門に送信される。このＡＣＬは後述するように計算機１２上のＡＣＬ設定部１５によって、ＷＷＷコンテンツ２８ａに設定される。

【００４９】

同様に、設定パターン＃１を、Ｂ部門４が保有するＷＷＷサーバ１３ｂ上のＷＷＷコンテンツ２８ｂに設定した場合には、図６（ｃ）に示す内容のＡＣＬファイルが作成されて、Ｂ部門４に送信される。

【００５０】

このＡＣＬファイルが送信される各計算機１２に設けられた構成要素について説明する。ＷＷＷサーバ１３（１３ａ、１３ｂを含む）は、各計算機１２に設けられ、動作するワールドワイドウェブ用のサーバソフトウエアである。ＷＷＷサーバ１３は、一つの計算機１２上に一つに限らず複数設けられてもよい。また、各ＷＷＷサーバ１３は、リソースとしてのＷＷＷコンテンツ２８（２８ａ、２８ｂを含む）を１以上保持している。なお、本実施形態ではアクセス権の設定対象をＷＷＷサーバ上のＷＷＷコンテンツの場合で説明しているが、アクセス権の設定手段を持つリソース（例えばあるＯＳ上のコンテンツ）であれば、対象は特に限定しない。

【００５１】

コンテンツ情報送信部１４は、アクセス権設定部２１から指定されたＷＷＷサーバ１３上のコンテンツ２８のコンテンツ情報として、ファイル名や現在設定されているアクセス権等を送信する。

【００５２】

ＡＣＬ設定部１５は、ＡＣＬ変換部２２より受け取ったアクセス権情報（ＡＣＬ２９）を設定対象のＷＷＷコンテンツに設定する。

なお、請求項における選択手段には、例えばアクセス権設定部２１が対応する。また、アクセス権設定パターン格納部には、例えばアクセス権設定パターン群２４を格納するサーバ８上の記憶手段が対応する。さらに、ユーザ情報格納部には、例えばユーザ情報２６を格納するサーバ９上の記憶手段が対応する。

【００５３】

また、請求項におけるリソース情報収集手段には、例えばコンテンツ情報送信部１４が対応する。

次に、以上のように構成された本実施形態におけるアクセス制御設定システムの動作について図２及び図７を用いて説明する。

【００５４】

図７は本実施形態のアクセス制御設定システムの動作を示す流れ図である。

同図に示すように、まず、設定・管理部門２において、設定者からのアクセス権設定部２１に対する入力により、どのＷＷＷサーバ１３のアクセス権を設定するかが選択される（ｓ１）。ここでは、Ａ部門３が保有するＷＷＷサーバ１３ａが選択されたと仮定する。

【００５５】

次に、Ａ部門３のコンテンツ情報送信部１４に対し、選択されたＷＷＷサーバ１３ａのコンテンツ情報を送信するように、アクセス権設定部２１により司令される（ｓ２）。

【００５６】

この指令を受けたコンテンツ情報送信部１４によって、ＷＷＷサーバ１３ａ上のコンテンツ情報が取得され、アクセス権設定部２１に対して同情報が送信される（ｓ３）。

【００５７】

コンテンツ情報を受け取ったアクセス権設定部１０６からアクセス権設定パターン管理部２３に対し、アクセス権設定パターン一覧を送信するよう司令される（ｓ４）。

【００５８】

アクセス権設定パターン管理部２３によりアクセス権設定パターン群２４が読み込まれ、アクセス権設定部２１に送信される（ｓ５）。

このアクセス権設定パターン一覧は表示装置（図示せず）上に表示される。設定者は、この表示を確認しながらアクセス権設定の対象となるコンテンツ２８ａと、同コンテンツに設定されるべきアクセス権設定パターンとをアクセス権設定部２１に選択入力する（ｓ６）。

【００５９】

ステップｓ６で選択された各情報は、当該入力がなされたアクセス権設定部２１からＡＣＬ変換部２２へ送信される（ｓ７）。なお、どの部門であるかという情報は選択コンテンツの情報に含まれている。

【００６０】

設定対象となるＷＷＷサーバ１３ａはＡ部門３に含まれているため、ＡＣＬ変換部２２からユーザ情報管理部２５に対し、Ａ部門３のユーザ情報を送信する旨の司令がなされる（ｓ８）。

【００６１】

この指令を受けたユーザ情報管理部２５によって、ユーザ情報２６からＡ部門３のユーザ情報が検索され、検索情報がＡＣＬ変換部２２へ送信される（ｓ９）。

【００６２】

次に、ＡＣＬ変換部２２によりアクセス権設定パターンの抽象ユーザ名に受信したユーザ情報が適用され、ＷＷＷコンテンツ１３ａに設定する実際のＡＣＬ（図６（ａ）参照）に

変換される（ｓ１０）。ＡＣＬへの変換は、上記のようにアクセス権設定パターンにユーザ情報を代入することによって実行される。なお、作成されるＡＣＬには、どのアクセス権設定パターンを選択したかを特定できる情報（パターン番号等）がＡＣＬのコメント等の形で含まれるようになっている。

【００６３】

さらに、ステップｓ１０で生成されたＡＣＬは、設定対象のＷＷＷサーバ１３ａで使用できるフォーマットに従っている。ＡＣＬのフォーマットはＷＷＷサーバ製品によって異なるが、各フォーマット情報は、ＡＣＬ変換部２２が保持しており、各ＷＷＷサーバ１３にそれぞれ対応してＡＣＬが生成される。

【００６４】

次に、生成されたＡＣＬ２９はネットワーク１を介してＡＣＬ変換部２２からＡ部門３における計算機１２のＡＣＬ設定部１５に送信される（ｓ１１）。

計算機１２に送信されたＡＣＬ２９は、ＡＣＬ設定部１５によって、対象となるＷＷＷサーバ１３ａのコンテンツ２８ａに対して設定されることとなる（ｓ１２）。

【００６５】

以上のようにしてコンテンツ２８に対してＡＣＬが設定されるが、当該ＡＣＬ設定後、そのコンテンツ２８（例えばコンテンツ２８ａ）に対するアクセス制御は具体的には以下のようにして行われる。ここで、各ユーザの属性情報（ユーザ名やパスワードの惰報など）がディレクトリサーバ９に登録されているものとする。

【００６６】

あるユーザがＷＷＷサーバ１３ａのコンテンツ２８ａへアクセスしようとすると、ＷＷＷサーバ１３ａがユーザに対してユーザ名とパスワードの入力を要求する。ユーザ名とパスワードをＷＷＷサーバ１３ａが受け取ると、ＷＷＷサーバ１３ａがディレクトリサーバ９に当該ユーザのユーザ情報を問い合わせ、ユーザが入カしたユーザ名とパスワードの組が正しく登録されているものであるかどうかを調べる（この処理を一般に「ユーザ認証」と言う）。正しく登録されていることが確認された場合、次に、ＷＷＷサーバ１３ａが、ここで得たユーザ名とＡＣＬで設定されている権限者名を比較し、一致する名前があればＡＣＬに設定されている権限に応じてコンテンツ２８ａへのアクセスを許可する。

【００６７】

上述した本発明の実施の形態に係るアクセス制御設定システムによれば、以下の効果が奏される。

まず、アクセス権設定部２１からの情報に基づき、ＡＣＬ変換部２２によりＡＣＬを自動生成するようにしたので、アクセス権設定パターンを選択するだけでＡＣＬの設定を行うことができ、ＡＣＬを設定するための手間が軽減される。特に、アクセス権の内容を設定のたびに設定者が一々ＡＣＬを記述する必要がないので、記述ミスによる設定不備も防止できる。

【００６８】

また、アクセス権設定パターン群２４における各パターンは抽象的なユーザ名を用いて記述されているので、所属するユーザが異なっている複数の部門あるいはサイトに対しても、同一のアクセス権設定パターンを利用することができる。したがって、システム全体で必要とするアクセス権のパターン数が大幅に減少し、管理コストが軽減され、これによりアクセス権設定コストの軽減も図れる。

【００６９】

さらに、本実施形態における各処理は、アクセス権の設定時のみで完結している。したがって、ＷＷＷサーバ上のコンテンツへのアクセス時に追加的な処理が発生することはなく、実行時（運用時：リソースにアクセスするとき）の性能劣化は起こらない。

【００７０】

また、ＡＣＬ変換部２２から各部門の計算機１２へＡＣＬを配送する機構を備えているので、ネットワーク１上に分散配置されたＷＷＷサーバ１３上のコンテンツに対するアクセス権の設定を、一個所（設定・管理部門２）で集中的に行うことができる。これにより、

アクセス権設定者が設定対象の計算機１２にその都度ログインする等の手間が軽減される。なお、この処理を実現するのに、実行時（コンテンツへのアクセス時）におけるＷＷＷサーバのアクセス権確認機構などは、従来のまま変更や追加を行う必要はない。

【００７１】

また、ディレクトリサーバ９にてユーザ情報を一括管理しているので、人事異動等によりユーザ情報に変更があった場合でも、ＡＣＬに付加されたアクセス権設定パターンに関する情報（パターン番号等）を利用してＡＣＬの再変換を行うのみで、ユーザ情報の変更を容易に反映させることができる。なお、アクセス権設定部２１は、再変換時の選択が可能なように構成され、同選択がなされた場合には、コンテンツ情報に上記パターンに関する情報を含めるようにコンテンツ情報送信部１４に指令する。さらに、このパターンに関する情報を用いて自動的にＡＣＬ変換部２２への付与情報が取得され、ＡＣＬ生成指令がなされる。

（発明の第２の実施の形態）

第１の実施形態ではＡＣＬパターンを設定・管理部門側でＡＣＬに変換してからＷＷＷサーバに配布していたが、本実施形態はＡＣＬパターンからの変換をＷＷＷサーバ側で行うものである。

【００７２】

図８は本発明の第２の実施の形態に係るアクセス制御設定システムの機能構成を示すブロック図であり、図２と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【００７３】

このアクセス制御設定システムにおいては、ユーザ情報管理部２５及びユーザ情報２６ａ，２６ｂ，．．と、ＡＣＬ変換部２２とが各部門３，４，．．に設けられる他、第１の実施形態と同様に構成されている。

【００７４】

各ユーザ情報２６ａ，２６ｂ，．．は、それぞれの部門３，４，．．についての情報である。ユーザ情報及びユーザ情報管理部２５は、部門ＬＡＮにおける各計算機１２、あるいはその部門に関する情報管理や各種処理を行うサーバ計算機（部門管理計算機３１）に設けられている。何れの場合でもＡＣＬ変換部２２は、ユーザ情報管理部２５に依頼してユーザ情報を取得できるように構成される。

【００７５】

次に、以上のように構成された本実施形態におけるアクセス制御設定システムの動作について図８及び図９を用いて説明する。

図９は本実施形態のアクセス制御設定システムの動作を示す流れ図である。

【００７６】

同図に示す処理のうち、ステップｔ１からステップｔ６間での処理は、第１の実施形態の図７におけるステップｓ１からステップｓ６と同様であるので説明を省略する。なお、本実施形態においても、Ａ部門３におけるＷＷＷサーバ１３ａのコンテンツ２８ａについてアクセス権を設定する場合について説明する。

【００７７】

設定者によるアクセス権設定部２１に対する選択入力が終了すると（ｔ６）、アクセス権設定の対象となるコンテンツ２８ａの指定情報と、同コンテンツについて設定されるべきアクセス権設定パターンの情報と（ＡＣＬパターン３２）が、設定管理サーバ８のアクセス権設定部２１からネットワーク１を介してＡ部門３における計算機１２上のＡＣＬ変換部１５へ送信される（ｔ７）。

【００７８】

このＡＣＬパターン３２を受け取ったＡＣＬ変換部２２からＡ部門３のユーザ情報管理部２５に対し、Ａ部門３のユーザ情報を送信する旨の司令がなされる（ｔ８）。

【００７９】

この指令を受けたユーザ情報管理部２５によるユーザ情報の取得、さらにはユーザ情報及

び設定パターンに基づくＡＣＬ２９の生成が、第１の実施形態における図７のステップｓ８，ｓ９，ｓ１０と同様にして行われる（図９：ｔ８，ｔ９，ｔ１０）。

【００８０】

Ａ部門のＡＣＬ変換部２２にて生成されたＡＣＬ２９は、Ａ部門３内においてＡＣＬ設定部１５に送信される（ｔ１１）。

このＡＣＬ２９を受信したＡＣＬ設定部１５により、第１の実施形態と同様にして、当該ＡＣＬ２９はWWWサーバ１３ａ上のコンテンツ２８ａに設定される（ｔ１２）。

【００８１】

以上のようにしてＡＣＬ設定されたコンテンツ２８に対し、実際のシステム運用時にいかにしてアクセス制御されるかは第１の実施形態の場合と同様であり、その具体的な説明はここでは省略する。

【００８２】

上述した本発明の実施の形態に係るアクセス制御設定システムによれば、第１の実施形態と同様な効果が得られる他、更に以下の効果が奏される。

まず、ネットワーク１を介して送信されるデータがＡＣＬパターン３２のみ（設定パターン情報及びコンテンツ指定情報）となるため、第１の実施形態の場合に比べ、送信データ量の軽減を図ることができる。

【００８３】

また、ＡＣＬ２９への変換処理を各WWWサーバ１３側で行うことにより、第１の実施形態の場合に比べ、ＡＣＬ変換作業の負荷分散を図ることができる。

（発明の第３の実施の形態）

第２の実施形態では、ユーザ情報管理部及びユーザ情報を各部門に設置するようにしたが、本実施形態では、ＡＣＬ変換部は各部門に設置しユーザ情報管理部及びユーザ情報は、設定・管理部門２に一括して設置するものである。

【００８４】

図１０は本発明の第３の実施の形態に係るアクセス制御設定システムの機能構成を示すブロック図であり、図２又は図８と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【００８５】

このアクセス制御設定システムは、ユーザ情報管理部２５及びユーザ情報２６が第１の実施形態と同様に設定・管理部門２のディレクトリサーバ９に設けられる他、第２の実施形態と同様に構成されている。

【００８６】

このように構成された本実施形態のアクセス制御設定システムにおいては、ＡＣＬ変換部２２による対象部門のユーザ情報の問合せがネットワーク１を介して設定・管理部門２のユーザ情報管理部２５に対して行われる点を除けば、第２の実施形態と同様に動作する。

【００８７】

以上のようにしてＡＣＬ設定されたコンテンツ２８に対し、実際のシステム運用時にいかにしてアクセス制御されるかは第１の実施形態の場合と同様であり、その具体的な説明はここでは省略する。

【００８８】

上述した本発明の実施の形態に係るアクセス制御設定システムによれば、第２の実施形態と同様な効果が得られる他、ユーザ情報２６の管理を設定・管理部門２にて集中的に行われるため、第１の実施形態と同様に、各部門３，４，．．におけるユーザ情報管理資源の設置コストやユーザ情報管理コスト自体を削減することができる。

【００８９】

なお、本実施形態では、ＡＣＬを生成するたびに設定・管理部門へユーザ情報の問い合わせを行うオーバヘッドが生じトラフィックが増えることになるが、第１及び第２の実施形態では、このようなトラフィック増加を防止することができる。

（発明の第４の実施の形態）

上記各実施形態では、生成されるアクセス権として、個々のユーザに対するアクセス権の形で表現する場合を説明したが、本実施形態は、単数または複数のユーザから構成されるユーザグループ単位でアクセス権を設定するものである。

【００９０】

図１１は本発明の第４の実施の形態に係るアクセス制御設定システムの機能構成を示すブロック図であり、図２と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【００９１】

このアクセス制御設定システムは、ＡＣＬ変換部２２′の機能が修正される他、第１の実施形態と同様に構成されている。

ＡＣＬ変換部２２′は、設定する権限者としてユーザ名を使用する代わりに、単数または複数のユーザから構成されるユーザグループを使用するようなＡＣＬを生成する点が、第１の実施形態と異なっている。また、第１～第３の実施形態では特に説明しなかったが、ユーザ情報管理部２５は、ユーザグル一プ名と、そのユーザグループにどのユーザが所属しているかの情報も合わせて管理している。

【００９２】

図１２は本実施形態のＡＣＬ変換部により生成されるＡＣＬファイルの例を示す図である。同図に示すように、図６（ａ）ではユーザ名が入る部分にユーザグループ名５２が記述されている。

【００９３】

なお、本実施形態におけるWWWサーバ１３は、ユーザグループ単位でのＡＣＬの設定機能やユーザグループの管理機能を提供するものである。

次に、以上のように構成された本実施形態におけるアクセス制御設定システムの動作について説明する。

【００９４】

ユーザグループ名によるＡＣＬ設定がなされる部分を除けば、本実施形態の動作は第１の実施形態と同様であるので、その点は説明を省略する。

例えばＡ部門３のユーザ情報が図４のとおりであり、Ａ部門３のWWWサーバ１３ａ上のコンテンツ２８ａに対して図３のアクセスパータン＃１を設定する場合を考える。

【００９５】

まず、ユーザ情報管理部２５が、図４に示す情報に対応して、以下のようなユーザグループの定義を管理しているものとする。

・「部門Ａの部長」グループ＝鈴木が所属
・「部門Ａの課長」グループ＝佐藤が所属
・「部門Ａのシステム管理者」グループ＝高橋，田中が所属

ここでは、ユーザグループ名の命名規則として、「抽象ユーザ名の前に対象部門名を付加する」という規則を採用している。命名規則は別の規則を採用しても問題ないが、どのような命名規則を採用するかの情報は、ＡＣＬ変換部２２′とユーザ情報管理部２５で共有されている必要がある。

【００９６】

第１の実施形態ではＡＣＬ変換部２２にてアクセス権設定パターンの抽象ユーザ名が実ユーザ名に展開されるが、本実施形態のＡＣＬ変換部２２′では、上記命名規則に従ってユーザグループ名に展開される。すなわち、

部長＝読み出し権限
課長＝読み出し権限
システム管理者＝読み出し権限、実行権限

というアクセス権設定パターンが、

Ａ部門の部長＝読み出し権限
Ａ部門の課長＝読み出し権限
Ａ部門のシステム管理者＝読み出し権限、実行権限

というＡＣＬに変換される。
【００９７】
同様に、同じアクセス権設定パターン＃１をＢ部門のＷＷＷサーバ１３に設定する場合は、
Ｂ部門の部長＝読み出し権限
Ｂ部門の課長＝読み出し権限
Ｂ部門のシステム管理者＝読み出し権限、実行権限
というＡＣＬに変換される。
【００９８】
この変換されたＡＣＬは計算機１２のＡＣＬ設定部１５によってＷＷＷサーバ１３ａのコンテンツ２８ａに設定される。
以上のようにしてＡＣＬ設定されたコンテンツ２８に対し、実際のシステム運用時にいかにしてアクセス制御されるかは、基本的には第１の実施形態の場合と同様であるが、相違する部分もあるのでその点について説明する。
【００９９】
すなわち、ＷＷＷサーバ１３がユーザ認証を完了した後、ＡＣＬに設定されている権限者を確認する場合、ＡＣＬにはユーザグループ名が記載されているため、このユーザグループにどのユーザが所属しているかを、ディレクトリサーバ９に問い合わせることにより確認する。例えば、「部門Ａのシステム管理者」というユーザグループに対しては、「高橋，田中」というユーザ名のリストが得られる。ユーザ認証の結果確認されたユーザ名（コンテンツにアクセスしようとしているユーザ）が、ここで得られたユーザ名のリストに含まれているかを確認し、含まれていれば権限者であると認定し、ＡＣＬに設定されている権限に応じてコンテンツ２８に対するアクセスを許可する。
【０１００】
上述した本発明の実施の形態に係るアクセス制御設定システムによれば、第１の実施形態と同様な効果が得られる他、アクセス権設定パターンを実ユーザではなくユーザグループに展開するようにしたので、人事異動などによりユーザ情報が変更になった場合でも、ユーザグループの定義を変更するだけでＡＣＬの再生成などの作業は不要とすることができる。
【０１０１】
なお、本実施形態は、第１の実施形態に対応させる場合を説明したが、本実施形態におけるユーザグループ単位でＡＣＬを設定する方法は、他の第２，第３実施形態に対しても同様に適用することができる。
（発明の第５の実施の形態）
上記各実施形態では、実際のアクセス制御処理時（ＡＣＬ設定後の運用時）の処理として、実ユーザ名を確認するためにＷＷＷサーバ１３がディレクトリサーバ９のユーザ情報管理部２５に問い合わせる方法を説明した。これに対して本実施形態では、確認すべきユーザの属性情報（ユーザ名やパスワードの情報など）およびユーザグループ情報（ユーザグループに所属するユーザのリスト）を、あらかじめＷＷＷサーバ１３に登録する方法について説明する。
【０１０２】
図１３は本発明の第５の実施の形態に係るアクセス制御設定システムの機能構成を示すブロック図であり、図２と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。
【０１０３】
このアクセス制御設定システムは、設定管理サーバ８にユーザ情報送信部５４、また各計算機１２にユーザ情報設定部５１が設けられるとともに、ＷＷＷサーバ１３にユーザ情報データベース５３が設けられる他、第１の実施形態と同様に構成されている。ここで、ユーザ情報データベース５３は、一般的なＷＷＷサーバが標準で持っている機構である。
【０１０４】

ユーザ情報送信部５４は、入力装置２７から指定された部門に所属するユーザの属性情報とユーザグループ情報を、ユーザ情報管理部２５から取得し、取得情報をネットワーク１を介してユーザ情報設定部５１に送信する。ユーザ情報設定部５１は、ユーザ情報送信部５４から受け取った情報を、ユーザ情報データベース５３に登録する。

【０１０５】

次に、以上のように構成された本実施形態におけるアクセス制御設定システムの動作について説明する。

まず、ＡＣＬ設定処理については、第１の実施形態と同様であるのでその点は説明を省略する。

【０１０６】

次に、アクセス権設定者は適宜のタイミング（例えばＡＣＬ設定前の任意の時点やＡＣＬ設定直後）で、入力装置２７を介してユーザ情報送信部５４に対象ＷＷＷサーバが必要とするユーザの属性情報とユーザグループ情報（例えば部門ＡのＷＷＷサーバには、部門Ａに属するユーザとユーザグループの情報を送信するなどの規則をあらかじめ定めておく。あるいはアクセス権設定者が指定する）を送信するよう指令する。

【０１０７】

この指令を受けたユーザ情報送信部５４により、ユーザ情報管理部２５から必要なユーザの属性情報とユーザグループ情報が読み出され、対象部門のユーザ情報設定部５１に送信される。ユーザ情報設定部５１は、受け取った情報を対象ＷＷＷサーバ１３のユーザ情報データベース５３に格納する。

【０１０８】

次に、ＡＣＬ設定されたコンテンツ２８に対し、実際のシステム運用時にいかにしてアクセス制御するかを説明する。

あるユーザがＷＷＷサーバ１３ａのコンテンツ２８ａへアクセスしようとすると、ＷＷＷサーバ１３ａがユーザに対してユーザ名とパスワードの入力を要求する。ユーザ名とパスワードをＷＷＷサーバ１３ａが受け取ると、ＷＷＷザーバ１３ａは自己に設けられたユーザ情報データベース５３に当該ユーザの属性情報を問い合わせ、ユーザ認証を行う。

【０１０９】

このユーザ情報データベース５３ａから取得された実ユーザ名がＡＣＬと比較され、以下、第１の実施形態と同様にしてアクセス制御が行われることになる。上述した本発明の実施の形態に係るアクセス制御設定システムによれば、第１の実施形態と同様な効果が得られる他、第１～第４の実施形態とは異なる方式でアクセス制御を運用することができる。

【０１１０】

なお、本実施形態は、第１の実施形態に対応させる場合を説明したが、本実施形態におけるユーザの属性情報を自己に設けられたユーザ情報データベース５３から取得する方法は、他の第２，第３，第４実施形態に対しても適用することができる。これら各実施形態において、ユーザ情報送信部５４，ユーザ情報設定部５１及びユーザ情報データベース５３を設けるようにすればよい。

（発明の第６の実施の形態）

上記各実施形態では、アクセス権設定パターン群２４は予め設定されている物として説明したが、アクセス権設定パターンの生成・変更・削除を行うことも可能であり、本実施形態ではこの場合を説明する。

【０１１１】

図１４は本発明の第６の実施の形態に係るアクセス制御設定システムに適用されるアクセス権設定パターンの編集機能の構成を示すブロック図であり、図２～図１３と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【０１１２】

このアクセス制御設定システムは、第１～第５の何れかの実施形態に係るアクセス制御設定システムの設定管理サーバ８においてアクセス権設定パターン管理ＧＵＩ６１が設けられたものである。

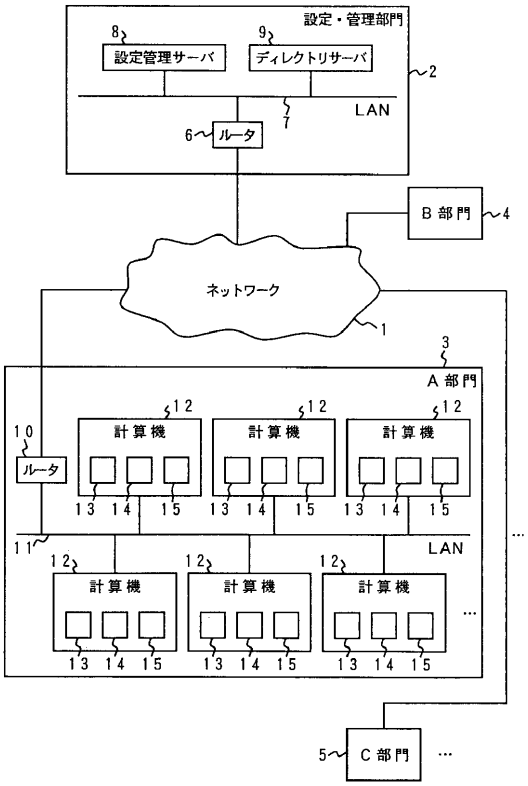
【０１１３】
この管理ＧＵＩ６１は、入力装置２７から情報入力可能に構成され、同入力情報に基づくアクセス権設定パターンの生成・変更・削除をアクセス権設定パターン管理部２３を介して行うようになっている。
【０１１４】
このように構成された本実施形態のアクセス制御設定システムは、アクセス権設定パターンの生成・変更・削除の部分以外については第１～第５の実施形態と同様に動作する。管理ＧＵＩ６１の部分については以下のように動作する。
【０１１５】
入力装置２７から新しいアクセス権設定パターンの情報（内容）が管理ＧＵＩ６１に入力されると、同ＧＵＩ６１によりアクセス権設定パータン群２４に新たにパターンが追加される。
【０１１６】
また、既存のアクセス権設定パターンの変更内容はアクセス権設定パターン管理部２３及び管理ＧＵＩ６１を介して表示出力され、同表示を見ながら設定者６２による変更入力がなされる。この変更入力に基づき、管理ＧＵＩ６１によってアクセス権設定パターン群２４の内容が変更される。
【０１１７】
さらに、入力装置２７から削除指令及び削除対象パターンの指定が入力されると、管理ＧＵＩ６１によって、アクセス権設定パターン群２４から該当パターンが削除される。
【０１１８】
上述した本発明の実施の形態に係るアクセス制御設定システムによれば、第１～第４の実施形態と同様な効果が得られる他、管理ＧＵＩ６１、入力装置２７及びアクセス権設定パターン管理部２３からなるアクセス権設定パターン管理機構を備えるようにしたので、アクセス権設定パターンの生成・修正・削除を容易に行うことができる。
【０１１９】
また、アクセス権設定パターンの管理は、ＣＵＩベースでもＧＵＩベースでも、両者を混合させた形でも行なうことができる。
例えば管理ＧＵＩ６１及び入力装置２７については、設定者６２からのキーボード入力という形態であってもよく、また、表示面に対するマウスクリック及びキーボード入力という形態でもよく、種々の場合が考えられる。
（変形例）
なお、本発明は、上記各実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々に変形することが可能である。以下に変形の例を説明する。
【０１２０】
［変形例１］
実施形態では、ＡＣＬ，ＡＣＬパターン、コンテンツ情報の送受信方法については特に記載していなかったが、これについては次のような形態が考えられる。必要な情報を正しく送受信できれば、何れの手法を用いてもよい。
【０１２１】
・ＪａｖａＲＭＩ、あるいは、ＣＯＲＢＡ（Ｃｏｍｍｏｎ　Ｏｂｊｅｃｔ　Ｒｅｑｕｅｓｔ　Ｂｒｏｋｅｒ　Ａｒｃｈｉｔｅｃｔｕｒｅ）に準拠したＯＲＢ（Ｏｂｊｅｃｔ　Ｒｅｑｕｅｓｔ　Ｂｒｏｋｅｒ）技術などを利用した分散オブジェクト間のメッセージ通信を用いる。
【０１２２】
・ＲＰＣ（Ｒｅｍｏｔｅ　Ｐｒｏｃｅｄｕｒｅ　Ｃａｌｌ）やＳｏｃｋｅｔなどを用いたプロセス間通信を用いる。
・ＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）やＣＧＩ（Ｃｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅ）など、一般的なＷＷＷの機構を利用する。

【０１２３】
・エージェントが必要な情報を保持し、配布して回る、等である。
［変形例２］
実施形態では、アクセス権設定パターンにユーザ情報を適用することによりＡＣＬを生成しているが、すでに完成しているＡＣＬに相当するものをアクセス権設定パターンとして含めることもできる。この場合、ＡＣＬ変換部２２，２２′では、選択されたアクセス権設定パターンをそのままＡＣＬとしてＡＣＬ設定部１５に送信することになる。
【０１２４】
［変形例３］
一つのアクセス権設定パターンの中に、抽象的なユーザ名と実ユーザ名（あるいはユーザグループ名）を混在させることもできる。この場合、抽象的なユーザ名のみがユーザ情報により変換され、はじめから実ユーザ名の部分はそのままの形のＡＣＬが生成される。
【０１２５】
［変形例４］
抽象的なユーザ名として、「部長」や「課長」など企業内の職制に関する例示を行ったが、抽象ユーザ名に特に制限はない。
【０１２６】
［変形例５］
実施形態では、アクセス権設定対象のリソースとして、ＷＷＷサーバ上のコンテンツについて記載したが、ファイルシステム上のファイルやデータベース上のデータ等、アクセス権の設定を行える計算機上のリソースであれば、対象となるリソースに関しての制限はない。
【０１２７】
［変形例６］
実施形態においては、アクセス権の設定・管理部門２を独立して設定したが、これをある部門、例えばＡ部門３が兼任するような形態にしてもよい。
【０１２８】
［変形例７］
図２～図１１では、Ａ部門３とＢ部門４の二つの部門が存在する形態で説明したが、図１に示すように部門数には特に制限はない。
【０１２９】
［変形例８］
第１の実施形態と、第２又は第３の実施形態を適宜組み合わせ、あるいは何れの実施形態を用いるかを適宜選択するようにすれば、アクセス権設定パターンからＡＣＬへの変換を設定・管理部門２で行なうか、設定対象の各部門３，４，．．で行なうかを、システムの設計思想や負荷状況などによって選択することができる。
【０１３０】
なお、本発明における記憶媒体としては、磁気ディスク、フロッピーディスク、ハードディスク、光ディスク（ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ等）、光磁気ディスク（ＭＯ等）、半導体メモリ等、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であってもよい。
【０１３１】
また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているＯＳ（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のＭＷ（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行してもよい。
【０１３２】
さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶又は一時記憶した記憶媒体も含まれる。

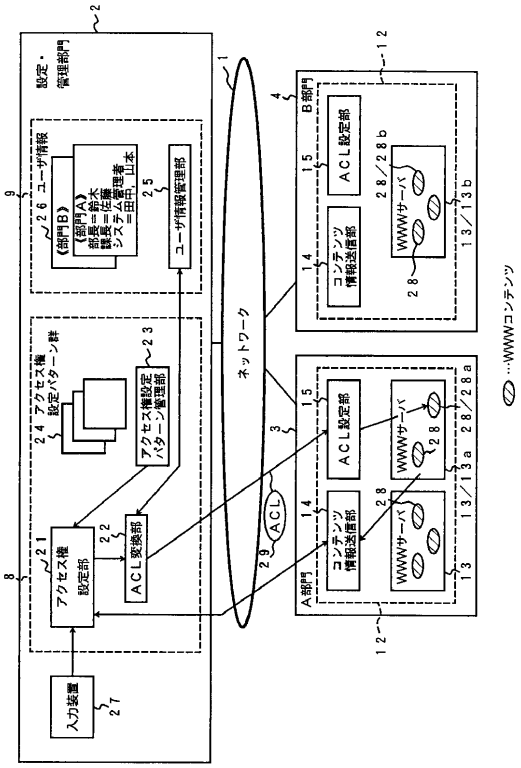
【０１３３】
また、記憶媒体は１つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何らの構成であってもよい。
【０１３４】
なお、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の１つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であってもよい。
【０１３５】
また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。
【０１３６】
【発明の効果】
以上詳記したように本発明によれば、アクセス権設定パターンを予め設け、これを選択することでアクセスコントロールリストを生成するようにしたので、部門やサイトに依存せず効率的にリソースへのアクセス権を設定することを可能にし、ひいては設定の手間を軽減し設定ミスを防止できるアクセス制御設定システム及び記憶媒体を提供することができる。
【０１３７】
また、アクセス権設定部に対する入力のみでアクセスコントロールリストを生成するとともに、生成したアクセスコントロールリストをリソースを管理する計算機側の設定手段でアクセス権設定できるようにしたので、設定対象の計算機にその都度ログインすることなしに当該設定を可能として、ひいては設定の手間を軽減し設定ミスを防止できるアクセス制御設定システム及び記憶媒体を提供することができる。
【図面の簡単な説明】
【図１】本発明の第１の実施の形態に係るアクセス制御設定システムを適用する計算機システムの構成例を示すブロック図。
【図２】同実施形態におけるアクセス制御設定システムの機能構成を示すブロック図。
【図３】アクセス権設定パターン群の一例を示す図。
【図４】ある部門（Ａ部門）のユーザ情報の例を示す図。
【図５】他の部門（Ｂ部門）のユーザ情報の例を示す図。
【図６】ＡＣＬ変換部により生成されるＡＣＬの例を示す図。
【図７】同実施形態のアクセス制御設定システムの動作を示す流れ図。
【図８】本発明の第２の実施の形態に係るアクセス制御設定システムの機能構成を示すブロック図。
【図９】同実施形態のアクセス制御設定システムの動作を示す流れ図。
【図１０】本発明の第３の実施の形態に係るアクセス制御設定システムの機能構成を示すブロック図。
【図１１】本発明の第４の実施の形態に係るアクセス制御設定システムの機能構成を示すブロック図。
【図１２】同実施形態のＡＣＬ変換部により生成されるＡＣＬファイルの例を示す図。
【図１３】本発明の第５の実施の形態に係るアクセス制御設定システムの機能構成を示すブロック図。
【図１４】本発明の第６の実施の形態に係るアクセス制御設定システムに適用されるアクセス権設定パターンの編集機能の構成を示すブロック図。
【符号の説明】
１…ネットワーク
２…設定・管理部門
３…Ａ部門
４…Ｂ部門

５…Ｃ部門
６…ルータ
７…データ伝送路
８…設定管理サーバ
９…ディレクトリサーバ
１０…ルータ
１１…データ伝送路
１２…計算機
１３，１３ａ，１３ｂ…ＷＷＷサーバ
１４…コンテンツ情報送信部
１５…ＡＣＬ設定部
２１…アクセス権設定部
２２，２２′…ＡＣＬ変換部
２３…アクセス権設定パターン管理部
２４…アクセス権設定パターン群
２５…ユーザ情報管理部
２６…ユーザ情報
２７…入力装置
２８，２８ａ，２８ｂ…ＷＷＷサーバ上のコンテンツ
２９…生成されたＡＣＬ
３１…部門管理計算機
３２…ＡＣＬパターン
５１…ユーザ情報設定部
５２…ユーザグループ名
５３…ユーザ情報データベース
５４…ユーザ情報送信部
６１…管理ＧＵＩ
６２…設定者

【図１】



【図２】



【図３】

アクセス権 設定パターン＃１：	部長=読み出し権，課長=読み出し権， システム管理者=読み出し権・実行権
アクセス権 設定パターン＃２：	部長=読み出し権・実行権，課長=読み出し権・実行権， 一般部員=読み出し権

【図４】

部長	鈴木
課長	佐藤
システム管理者	高橋，田中
一般部員	渡辺，小林，伊藤

【図５】

部長	中村
課長	加藤
システム管理者	斎藤
一般部員	佐々木，山本

【図６】

（a）ＡＣＬファイルの例（XXX.acl）

```
path="/opt/www/docs/file1.html"
allow (read, write)
    user="yamada, tanaka"
path="/opt/www/docs/file2.html"
allow ( ····· )
    user=( ····· )
  ⋮
```

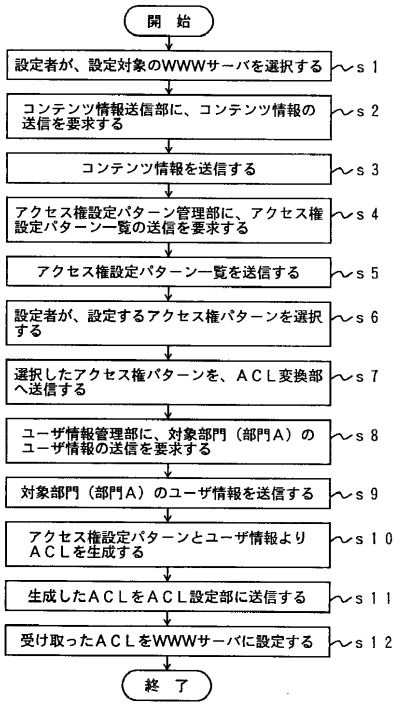
（b）

対象パス＝○○○○
鈴木＝読み出し権限
佐藤＝読み出し権限
高橋＝読み出し権限，実行権限
田中＝読み出し権限，実行権限

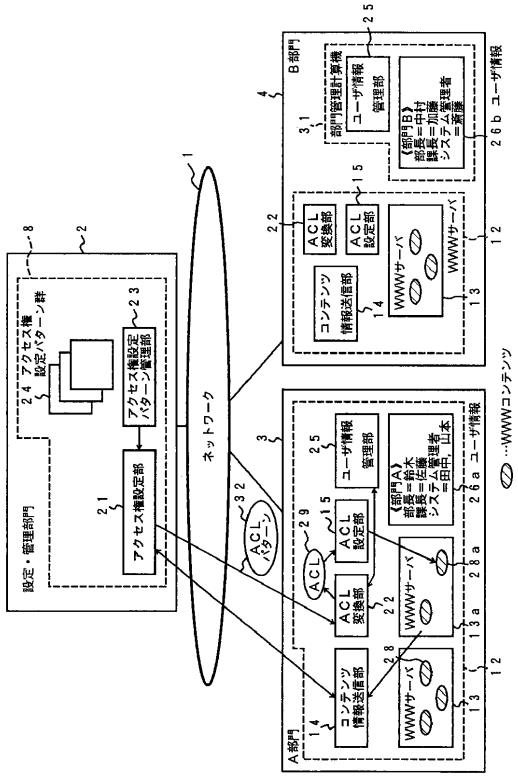
（c）

対象パス＝××××
中村＝読み出し権限
加藤＝読み出し権限
斎藤＝読み出し権限，実行権限

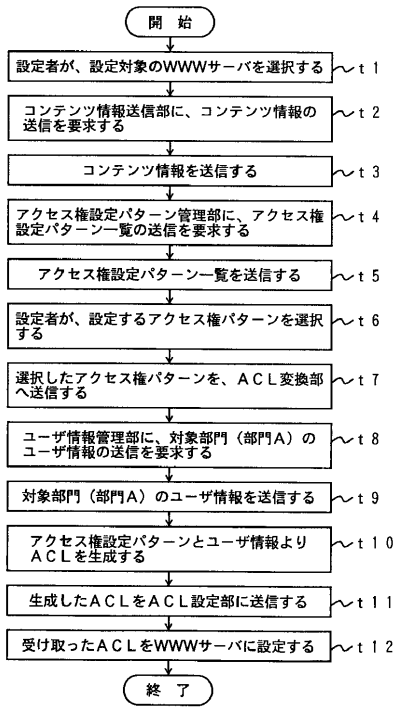
【図７】


開　始
設定者が、設定対象のWWWサーバを選択する
ｓ１
コンテンツ情報送信部に、コンテンツ情報の送信を要求する
ｓ２
コンテンツ情報を送信する
ｓ３
アクセス権設定パターン管理部に、アクセス権設定パターン一覧の送信を要求する
ｓ４
アクセス権設定パターン一覧を送信する
ｓ５
設定者が、設定するアクセス権パターンを選択する
ｓ６
選択したアクセス権パターンを、ＡＣＬ変換部へ送信する
ｓ７
ユーザ情報管理部に、対象部門（部門Ａ）のユーザ情報の送信を要求する
ｓ８
対象部門（部門Ａ）のユーザ情報を送信する
ｓ９
アクセス権設定パターンとユーザ情報よりＡＣＬを生成する
ｓ１０
生成したＡＣＬをＡＣＬ設定部に送信する
ｓ１１
受け取ったＡＣＬをWWWサーバに設定する
ｓ１２
終　了

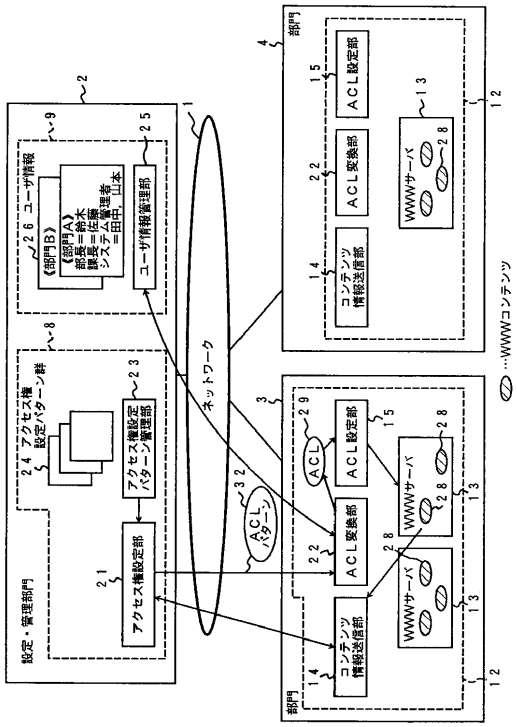
【図８】


設定・管理部門
アクセス権設定パターン群
アクセス権設定パターン管理部
アクセス権設定部
ネットワーク
ACLパターン
B部門
部門管理計算機
ユーザ情報管理部
〈部門B〉
部長＝中村
課長＝加藤
システム管理者＝斎藤
ACL変換部
ACL設定部
コンテンツ情報送信部
WWWサーバ
A部門
ユーザ情報
〈部門A〉
部長＝鈴木
課長＝佐藤
システム管理者＝田中、山本
…WWWコンテンツ

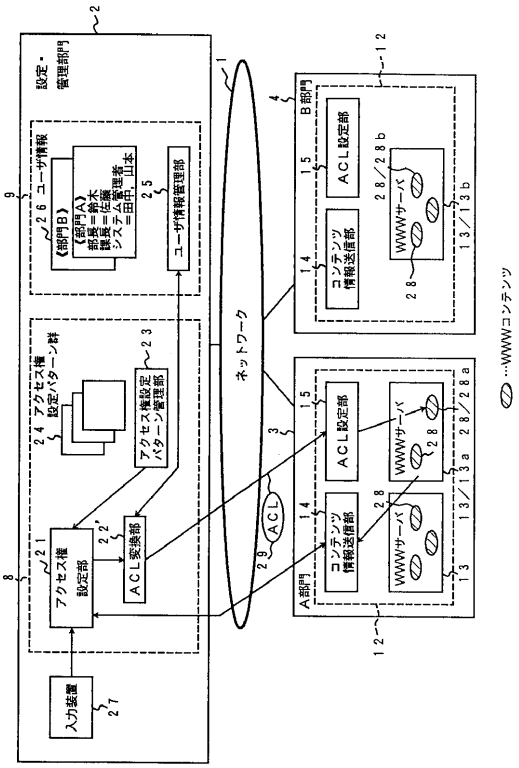
【図９】


開　始
設定者が、設定対象のWWWサーバを選択する
ｔ１
コンテンツ情報送信部に、コンテンツ情報の送信を要求する
ｔ２
コンテンツ情報を送信する
ｔ３
アクセス権設定パターン管理部に、アクセス権設定パターン一覧の送信を要求する
ｔ４
アクセス権設定パターン一覧を送信する
ｔ５
設定者が、設定するアクセス権パターンを選択する
ｔ６
選択したアクセス権パターンを、ＡＣＬ変換部へ送信する
ｔ７
ユーザ情報管理部に、対象部門（部門Ａ）のユーザ情報の送信を要求する
ｔ８
対象部門（部門Ａ）のユーザ情報を送信する
ｔ９
アクセス権設定パターンとユーザ情報よりＡＣＬを生成する
ｔ１０
生成したＡＣＬをＡＣＬ設定部に送信する
ｔ１１
受け取ったＡＣＬをWWWサーバに設定する
ｔ１２
終　了

【図１０】


設定・管理部門
アクセス権設定パターン群
アクセス権設定パターン管理部
アクセス権設定部
ユーザ情報管理部
〈部門B〉
〈部門A〉
部長＝鈴木
課長＝佐藤
システム管理者＝田中、山本
ネットワーク
ACLパターン
部門
ACL設定部
ACL変換部
コンテンツ情報送信部
WWWサーバ
…WWWコンテンツ

【図１１】

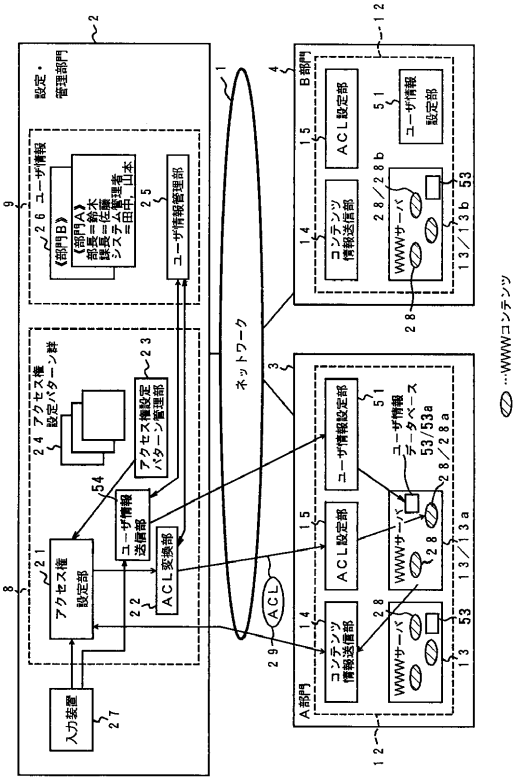


【図１２】

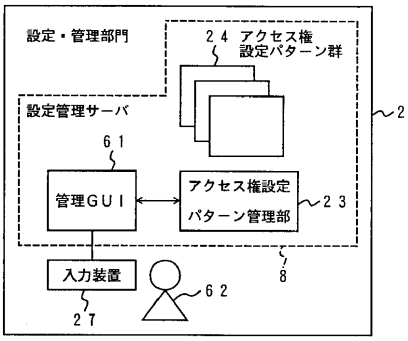
ＡＣＬファイルの例（XXX.acl）

```
path="/opt/www/docs/file1.html"
allow (read, write)
    user="ユーザグループ名"
path="/opt/www/docs/file2.html"
allow ( ····· )
    user=( ····· )
  ⋮
```

【図１３】



【図１４】



フロントページの続き

(74)代理人　100070437
　　弁理士　河井　将次
(72)発明者　橋本　圭介
　　東京都府中市東芝町１番地　株式会社東芝府中工場内
(72)発明者　長谷川　義朗
　　東京都府中市東芝町１番地　株式会社東芝府中工場内

審査官　後藤　和茂

(56)参考文献　特開平０６－１０３２３６（ＪＰ，Ａ）
　　特開平０９－２３３４５３（ＪＰ，Ａ）
　　特開平０９－２１８８２７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.^{7}，ＤＢ名)
　　G06F12/00
　　G06F15/00