(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-293004
(P2005-293004A)
(43)公開日　平成17年10月20日(2005.10.20)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 12/14	G06F 12/14	520B	5B017
G06F 12/00	G06F 12/14	510F	5B082
G06F 15/00	G06F 12/00	537A	5B085
	G06F 15/00	330Z	

審査請求 未請求　請求項の数 5　OL　（全 35 頁）

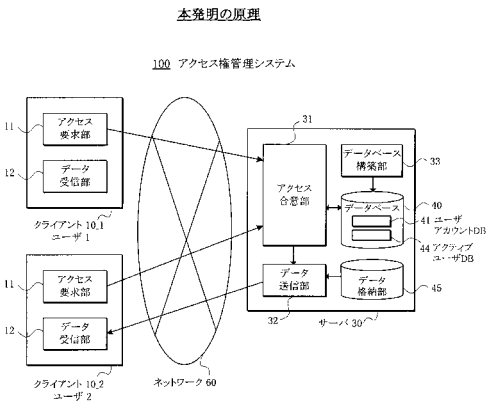
(21)出願番号　特願2004-104521 (P2004-104521)
(22)出願日　平成16年3月31日 (2004.3.31)

(71)出願人　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　100090011
弁理士　茂泉　修司
(72)発明者　久保田　真
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　小島　祐治
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

Fターム(参考)　5B017 AA01　AA07　BA06　BB06　BB07　CA16
5B082 AA01　BA09　EA11　GA11
5B085 AE00　AE02　AE03

(54)【発明の名称】アクセス権管理システム及びアクセス権管理方法

(57)【要約】
【課題】本発明は、データへのアクセスを管理して該データの漏洩を防止するアクセス権管理システム100及びアクセス権管理方法に関し、アクセス権を持つユーザの故意又は過失によるデータ漏洩を防ぐ。
【解決手段】ユーザアカウントデータベース41に、データに対してアクセス権を保有する複数のユーザを関連付けて登録し、アクティブユーザデータベース44に、該アクセス権保有ユーザの内、現在、該データに対するアクセスに合意しているユーザを登録し、該アクセス合意部31が、アクティブユーザデータベース44に登録された該合意しているアクセス権保有ユーザの現在数が複数であるときのみ、該データに対してアクセス要求して来た該アクセス権を保有するユーザに該データへのアクセスを合意する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
データに対してアクセス権を保有する複数のユーザを関連付けたユーザアカウントデータベースと、
該アクセス権保有ユーザの内、現在、該データに対するアクセスに合意しているユーザを示すアクティブユーザデータベースと、
該アクティブユーザデータベースに示された該合意しているアクセス権保有ユーザの現在数が複数であるときのみ、該データに対してアクセス要求して来た該アクセス権を保有するユーザに該データへのアクセスを合意するアクセス合意部と、
で構成されたことを特徴とするアクセス権管理システム。
【請求項２】
請求項１において、
該システムがサーバと１つ以上のクライアントで構成され、
該サーバが、該ユーザアカウントデータベース、該アクティブユーザデータベース、及び該アクセス合意部を備え、
各クライアントが、自分の現在位置を検出する位置情報検出部と、該検出した現在位置及び該ユーザから受け付けたアクセス要求を該アクセス合意部に送信するアクセス要求部とを備え、
該アクセス合意部が、受信した該現在位置を該アクセス権保有ユーザに対応付けて該アクティブユーザデータベースに登録し、所定の範囲内に位置するユーザ数を、該合意しているユーザの現在数とすることを特徴としたアクセス権管理システム。
【請求項３】
請求項１において、
該システムがサーバと１つ以上のクライアントで構成され、
該サーバが、該ユーザアカウントデータベース、該アクティブユーザデータベース、及び該アクセス合意部を備え、
各クライアントが、他のクライアントとの間でネットワークを構築するネットワーク構築部と、ネットワークを構築したクライアントの該アクセス権保有ユーザの識別情報、及び自クライアントのユーザから受け付けたアクセス要求を該アクセス合意部に送信するアクセス要求部とを備え、
該アクセス合意部が、該識別情報の該アクセス権保有ユーザを、該データに対するアクセスに合意している該アクセス権保有ユーザとして該アクティブユーザデータベースに登録することを特徴としたアクセス権管理システム。
【請求項４】
請求項１において、
各クライアントが、該ユーザアカウントデータベース、該アクティブユーザデータベース、及び該アクセス合意部の他に、さらにネットワーク構築部及びアクセス要求部を備え、
該ネットワーク構築部が、他のクライアントとの間でネットワークを構築し、
該アクセス合意部は、該構築されたネットワークに接続されているクライアントのアクセス権保有ユーザを、該データに対するアクセスに合意している該アクセス権保有ユーザとして該アクティブユーザデータベースに登録し、
該アクセス要求部が、該データを保持するクライアントの該アクセス合意部に、自クライアントのユーザから受け付けたアクセス要求を与えることを特徴としたアクセス権管理システム。
【請求項５】
データに対してアクセス権を保有する複数のユーザを関連付けて登録する第１ステップと、
該アクセス権保有ユーザの内、現在、該データに対するアクセスに合意しているユーザを登録する第２ステップと、

該合意しているアクセス権保有ユーザの現在数が複数であるときのみ、該データに対してアクセス要求して来た該アクセス権を保有するユーザに該データへのアクセスを合意する第３ステップと、
を有することを特徴したアクセス権管理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明はアクセス権管理システム及びアクセス権管理方法に関し、特に、データへのアクセスを管理して該データの漏洩を防止するアクセス権管理システム及びアクセス権管理方法に関する。
【０００２】
近年、通信技術の高度な発達に伴い、ネットワーク上を膨大な、産業秘密情報(設計文書等)やプライバシー情報(名簿等)等の機密情報が転送され、この情報の漏洩が問題になって来ている。機密情報の漏洩の要因には、本来アクセス権限を持たない不正ユーザによる情報流出だけではなく、アクセス権限を持つ正規ユーザによる故意又は過失による情報流出が大きな割合を占めており、アクセス権を管理する技術はますます重要になって来ている。
【背景技術】
【０００３】
機密情報の漏洩の具体例としては、CD/FD等の保存媒体の持ち出し、電子メールによる電子ファイル形式での持ち出し、電車等の公衆の中におけるモバイル端末(ノート型PC/PDA等)によるデータ閲覧等がある。これらの例によれば、アクセス権を持つ一人のユーザの意思次第で自由に機密情報にアクセス可能であることが、情報漏洩の主な要因と言える。
【０００４】
このような漏洩問題を解決するため、各種認証システムや、ファイルを暗号化して文書管理サーバと暗号鍵の交換が可能な通信環境でのみアクセス可能とするシステムが開発、導入されている。
【０００５】
図24は、従来の機密情報漏洩防止システム(アクセス権管理システム)例を示しており、このシステムは、ネットワーク60で接続された管理サーバ70及びクライアント10a_1～10a_3(以下、符号10aで総称する。)で構成されている。管理サーバ70は、文書管理DB(データベース)81、鍵管理DB82、ユーザ管理DB83、及びユーザ操作管理DB84、並びにこれらのデータベースを管理する管理ソフトウェアを備えている。各クライアント10aはユーザ専用操作制御ソフトウェアを備えている。
【０００６】
各クライアント10aに対応したユーザ1～3は、専用操作制御ソフトウェアを介して、例えば文書Jの編集要求900を管理サーバ70に送信し、管理サーバ70の管理ソフトウェアから認証を受けた後、編集許可901とともに暗号化文書J及び鍵Kを管理サーバ70からダウンロードする。クライアント10aは、暗号化文書Jを鍵Kで通常文書Jに復号化する。なお、ユーザ1～3(各クライアント10a)は、ユーザ管理DB83及びユーザ操作管理DB84に設定されたアクセス権の範囲内で文書に対して操作を行うことができる。この文書操作には、例えば、閲覧84a、保存84b、編集84c、印刷84d、コピー＆ペースト84e、及び画面キャプチャ84fがある。
【０００７】
クライアント10aは、システム専用のユーザ操作制御ソフトウェアを経由しないと、復号化した文書に対して操作を行うことができないので、許可されたアクセス権以外の操作を行うことはできない。例えば、ユーザ1は、文書名Jの閲覧及び編集操作のみのアクセス権を持っている。なお、対象となる文書の種類(Word,Excel, Acrobat, ...等)は、ユーザ制御ソフトウェアの実装レイヤに応じて、その幅に差がある。一般的にOSのカーネルレイヤに近いレイヤに実装した方が、より幅広い文書が対象となり得る。また、ユーザ管理、

ユーザ操作管理、及びこれに必須の鍵管理を行う管理サーバと、文書管理を行うコンテンツサーバを別サーバとして構成する実装例もある。(例えば、非特許文献１参照。)。

【０００８】

しかし、アクセス権を持つ１ユーザの意思次第で不正が可能であること、特にVPN(VirtualPrivate Network)接続等の技術により社外からの社内ネットワークのデータアクセスを許可した場合、データが社外に漏洩する可能性が高まり問題となる。一方、社外からのアクセスを許可しない場合、近年のモバイル社会においては利便性を損なう問題となる。

【０００９】

この問題を解決するための従来のシステムとして、GPS等によりシステムがユーザの位置を管理可能としておき、この位置情報を用いてデータ読み出しの可否を制御する例がある。これらはいずれも、データベースに登録されたアクセス許可位置と実際の位置が一致した場合のみ閲覧許可することで漏洩への耐性を高めるシステムである。

【００１０】

また、ユーザの位置情報と端末の位置情報を管理し、コンピュータ資源に対して所定のアクセス権を有するユーザがアクセス要求して来たとき、ユーザの位置情報とアクセス要求を行って来た端末の位置情報が所定の関係にあるときのみ、アクセス要求を許可するアクセス権管理システムがある(例えば、特許文献１参照。)。

【００１１】

しかしながら、これらのシステムは、結局はアクセス権を持つ1ユーザの意思次第で不正が可能な点は変わらず、問題は残る。

【特許文献１】特開2001-175601号公報

【非特許文献１】ReEncryption：http://www.reencryption.com/frame_j2.html

【発明の開示】

【発明が解決しようとする課題】

【００１２】

さらに、上記の問題を解決するための従来のシステムとして、コンテンツサーバによる文書の集中管理の脆弱性に注目して、文書を複数のサーバへ分散して格納してセキュリティを向上させる例もある。しかしながら、サーバ管理を行うのが一人の管理者(ユーザ)であるため、該管理者の意思次第で不正が可能であることから、やはり問題が残る。

【００１３】

したがって本発明は、データへのアクセスを管理して該データの漏洩を防止するアクセス権管理システム及びアクセス権管理方法において、アクセス権を持つユーザの故意又は過失によるデータ漏洩を防ぐことを課題とする。

【課題を解決するための手段】

【００１４】

上記の課題を解決するため、本発明のアクセス権管理システムは、データに対してアクセス権を保有する複数のユーザを関連付けたユーザアカウントデータベースと、該アクセス権保有ユーザの内、現在、該データに対するアクセスに合意しているユーザを示すアクティブユーザデータベースと、該アクティブユーザデータベースに示された該合意しているアクセス権保有ユーザの現在数が複数であるときのみ、該データに対してアクセス要求して来た該アクセス権を保有するユーザに該データへのアクセスを合意するアクセス合意部とで構成されていることを特徴している。

【００１５】

図１は、本発明に係るアクセス権管理システム100の原理を示している。このシステム100は、ユーザアカウントデータベース41、アクティブユーザデータベース44、及びアクセス合意部31を備えている。

【００１６】

ユーザアカウントデータベース41には、データ(例えば、設計文書等の産業上の機密情報、名簿等のプライバシー情報等)に対して、このデータに対するアクセス権を有する複数のアクセス権保有ユーザが関連付けられている。アクティブユーザデータベース44には

、ユーザアカウントデータベース41で関連付けられた複数のアクセス権保有ユーザの内、現在、該データに対するアクセスに合意しているアクセス権保有ユーザが示されている。この場合の合意は、例えば、アクセス権保有ユーザが同一範囲内の位置にいる場合である。

【００１７】

アクセス合意部31は、アクティブユーザデータベース44に示された該合意しているアクセス権保有ユーザの現在数が複数であるときのみ、該データに対してアクセス要求して来た該アクセス権保有ユーザに該データへのアクセスを合意する。

【００１８】

これにより、一人のアクセス権保有ユーザの故意又は過失によるデータの漏洩を防ぐことが可能になり、従来システムと比較して、データ漏洩への耐性を強化したデータアクセス環境(システム)を提供することが可能になる。

【００１９】

また、本発明は、上記の発明において、該システムがサーバと１つ以上のクライアントで構成され、該サーバが、該ユーザアカウントデータベース、該アクティブユーザデータベース、及び該アクセス合意部を備え、各クライアントが、自分の現在位置を検出する位置情報検出部と、該検出した現在位置及び該ユーザから受け付けたアクセス要求を該アクセス合意部に送信するアクセス要求部とを備え、該アクセス合意部が、受信した該現在位置を該アクセス権保有ユーザに対応付けて該アクティブユーザデータベースに登録し、所定の範囲内に位置するユーザ数を、該合意しているユーザの現在数とすることが可能である。

【００２０】

図１において、アクセス権管理システム100は、複数のクライアント10_1，10_2(以下、符号10で総称することがある。)、及びサーバ30で構成されている。各クライアント10は、自分の現在位置を検出する位置情報検出部(図示せず。例えば、位置情報送信装置から位置情報を受信する位置情報受信部。)と、例えば、検出した現在位置、又はデータに対する、ユーザから受け付けたアクセス要求をアクセス合意部31に送信するアクセス要求部11とを備えている。

【００２１】

サーバ30は、ユーザアカウントデータベース41、アクティブユーザデータベース44、及びアクセス合意部31を備えている。このアクセス合意部31は、各クライアント10から受信した現在位置をユーザに対応付けてアクティブユーザデータベース44に登録する。そして、アクセス合意部31は、クライアント(アクセス権保有ユーザ)10から、データに対するアクセス要求があったとき、アクティブユーザデータベース44を参照して、所定の範囲内に位置するユーザ数、を該合意しているアクセス権保有ユーザの現在数とし、この現在数が複数以上であるときのみ、アクセスを合意(許可)する。

【００２２】

これにより、所定の範囲内に位置する各アクセス権保有ユーザの合意により、各アクセス権保有ユーザはデータにアクセス可能になる。

【００２３】

なお、クライアントとユーザは、必ずしも１対１に対応する必要はなく、同一のクライアントを複数のユーザが用いてもよい。

【００２４】

また、「必要人数」の設定を追加し、上記で「複数以上であるときのみアクセス合意」の代わりに、アクティブなユーザが、該必要人数以上であることを以って、アクセス合意とみなしても良い。

【００２５】

また、本発明は、上記の発明において、該システムがサーバと１つ以上のクライアントで構成され、該サーバが、該ユーザアカウントデータベース、該アクティブユーザデータベース、及び該アクセス合意部を備え、各クライアントが、他のクライアントとの間でネ

ットワークを構築するネットワーク構築部と、ネットワークを構築したクライアントの該アクセス権保有ユーザの識別情報、及び自クライアントのユーザから受け付けたアクセス要求を該アクセス合意部に送信するアクセス要求部とを備え、該アクセス合意部が、該識別情報の該アクセス権保有ユーザを、該データに対するアクセスに合意している該アクセス権保有ユーザとして該アクティブユーザデータベースに登録することができる。

【００２６】

すなわち、アクセス権管理システム100は、１つ以上のクライアント10及びサーバ30で構成されている。各クライアント10は、ネットワーク構築部(図示せず。)及びアクセス要求部11を備えている。ネットワーク構築部は他のクライアント10とネットワーク(例えば、アドホックネットワーク、図示せず。)を構築し、アクセス要求部11はネットワークを構築したクライアント10のアクセス権保有ユーザの識別情報及び自クライアントのユーザから受け付けた、データに対するアクセス要求をアクセス合意部31に送信する。

【００２７】

サーバ30は、ユーザアカウントデータベース41、アクティブユーザデータベース44、及びアクセス合意部31を備えている。このアクセス合意部31は、各クライアント10から受信した識別情報のアクセス権保有ユーザを、該データに対するアクセスに合意している該アクセス権保有ユーザとして該アクティブユーザデータベース44に登録する。

【００２８】

そして、アクセス合意部31は、クライアント10からデータに対するアクセス要求があったとき、アクティブユーザデータベース44を参照して、合意しているアクセス権保有ユーザの現在数が、複数であるときのみ、アクセスに合意する。

【００２９】

これにより、例えば、アドホックネットワークが接続されたことで示される所定の範囲内に位置する各アクセス権保有ユーザの合意により、各アクセス権保有ユーザはデータにアクセスすることが可能になる。

【００３０】

なお、アドホックネットワークの代わりに、クライアントを適当な長さの有線で接続したネットワークとすることもできる。

【００３１】

また、本発明は、上記の発明において、各クライアントが、該ユーザアカウントデータベース、該アクティブユーザデータベース、及び該アクセス合意部の他に、さらにネットワーク構築部及びアクセス要求部を備え、該ネットワーク構築部が、他のクライアントとの間でネットワークを構築し、該アクセス合意部は、該構築されたネットワークに接続されているクライアントのアクセス権保有ユーザを、該データに対するアクセスに合意している該アクセス権保有ユーザとして該アクティブユーザデータベースに登録し、該アクセス要求部が、該データを保持するクライアントの該アクセス合意部に、自クライアントのユーザから受け付けたアクセス要求を与えることができる。

【００３２】

すなわち、アクセス権管理システムは、複数のクライアントのみで構成されている。各クライアントは、ユーザアカウントデータベース、アクティブユーザデータベース、及びアクセス合意部の他に、さらにネットワーク構築部及びアクセス要求部を備えている。

【００３３】

ネットワーク構築部は、他のクライアントと、例えば、アドホックネットワークを構築する。アクセス合意部は、構築されたネットワークに現在接続されているクライアントのアクセス権保有ユーザを、該データに対するアクセスに合意している該アクセス権保有ユーザとして該アクティブユーザデータベースに登録する。

【００３４】

該アクセス要求部は、該データを保持するクライアントのアクセス合意部に、自クライアントのユーザから受け付けたアクセス要求を行い、このアクセス要求を受信したアクセス合意部は、アクティブユーザデータベースを参照して、合意しているアクセス権保有ユ

ーザの現在数が、複数のときのみアクセスを合意する。
【００３５】
このようにアクセス合意部を各クライアントに分散することにより、サーバを必要とせずに、複数ユーザの合意を判定し、データ漏洩に対する耐性を向上させることが可能になる。
【００３６】
また、本発明は、上記の発明において、各クライアントが、データベース構築部をさらに有し、該データベース構築部が、該ユーザアカウントデータベースに、該データに対してアクセス権を保有する複数のユーザを関連付けて登録又は削除することができる。
【００３７】
すなわち、各クライアントが、データベース構築部を分散して備えている。このデータベース構築部は、該ユーザアカウントデータベースに該データに対してアクセス権を保有する複数のユーザを関連付けて登録又は削除することが可能である。
【００３８】
これにより、サーバ30無しでシステムを構築することが可能になり、特権的なサーバ管理者からの情報漏洩を防ぎ、複数ユーザが相互に監視するため、システムの漏洩防護への耐性を高めることが可能になる。
【００３９】
また、本発明は、上記の発明において、該サーバが該データを保持してもよい。
【００４０】
また、本発明は、上記の発明において、該クライアントが、該データを分散して保持するデータ格納部と、該データを他のクライアントとの間で送受信するためのデータ送信部及びデータ受信部とをさらに備えることできる。
【００４１】
すなわち、クライアントは、上記の他、データ格納部、データ送信部、及びデータ受信部をさらに備えている。例えば、１つの文書ファイル(データ)は、分散して各クライアントのデータ格納部に格納される。或るクライアントが要求した該文書ファイルに対するアクセスが合意されたとき、他のクライアントのデータ送信部は、データ格納部に格納された分割されて文書ファイルを、この文書ファイルを要求したクライアントに送信する。このクライアントのデータ受信部は、他のクライアントから送信されて来たデータを受信し、１つの文書ファイルを形成する。
【００４２】
これにより、例え個別のクライアントのセキュリティが破られた場合においても、全データの漏洩がないため、漏洩防護への耐性を高めることが可能になる。なお、データの送受信は、例えば、サーバとクライアントを接続するネットワークであってもよいし、クライアント同士を接続するアドホックネットワークであってもよい。
【００４３】
また、本発明は、上記の発明において、該ユーザアカウントデータベースに該データに対してアクセス権を保有する複数のユーザを関連付けて登録又は削除するデータベース構築部をさらに備えることができる。これにより、ユーザアカウントデータベースに該データに対してアクセス権を保有する複数のユーザを関連付けて登録又は削除できる。
【００４４】
さらに、上記の課題を解決するために、本発明に係るアクセス権管理方法は、データに対してアクセス権を保有する複数のユーザを関連付けて登録する第１ステップと、該アクセス権保有ユーザの内、現在、該データに対するアクセスに合意しているユーザを登録する第２ステップと、該合意しているアクセス権保有ユーザの現在数が複数であるときのみ、該データに対してアクセス要求して来た該アクセス権を保有するユーザに該データへのアクセスを合意する第３ステップとを有することができる。
【発明の効果】
【００４５】

以上説明したように、本発明に係るアクセス権管理システムによれば、アクセス可否に複数ユーザの合意が必要とするように構成したので、１ユーザ単位でアクセスの可否判断をする従来のシステムと比較して、データ漏洩に対する耐性が向上する。

【００４６】

また、アクセス権管理システムが、複数ユーザの位置情報に基づき、複数ユーザの合意を判定するようにしたので、各ユーザのデータアクセス時のシステム操作及び手続きの容易性は従来のシステムと同じであり、システム使用時のユーザの手間をかけることなくデータ漏洩に対する耐性が向上する。

【００４７】

また、アクセス権管理システムが、複数ユーザが同一範囲内の位置に近接してネットワークを構成したことで、複数ユーザのアクセスの合意を判定するようにしたので、各ユーザの絶対位置を取得できないような状況においても、データ漏洩に対する耐性が向上する。

【００４８】

また、アクセス権管理システムが、データを各クライアントに分散して保有するようにしたので、サーバとクライアントとの間のネットワークの使用帯域を節約するとともに、データ漏洩に対する耐性を向上する。さらに、データの分散保有により、例え個別のクライアントのセキュリティが破られた場合においても、全データの漏洩がないため、漏洩防護への耐性を高める。

【００４９】

また、クライアントが、アクセス合意部を分散保有することにより、サーバを必要とせずに、複数ユーザの合意を判定し、データ漏洩に対する耐性が向上する。

【００５０】

さらに、クライアントが、データベース構築部を分散保有することにより、サーバなしでシステムを構築することができ、特権的なサーバ管理者からの情報漏洩を防ぎ、複数メンバでクロスチェックするため、システムの漏洩防護への耐性を高めることができる効果がある。

【発明を実施するための最良の形態】

【００５１】

実施例(1)：位置情報に基づくアクセス合意

図２は、本発明の実施例(1)におけるアクセス権管理システム100wの構成例を示している。このアクセス権管理システム100wは、サーバ30及びクライアント10_1, 10_2(以下、符号10で総称することがある。)で構成され、これらのサーバ30及びクライアント10はネットワーク60で接続されている。また、同図には、アクセス権管理システム100wの他に位置情報送信装置50が示されている。サーバ30は、アクセス合意部31、データ送信部32、データベース構築部33、データベース40w、及びデータ格納部45wを備え、各クライアント10は、アクセス要求部11、データ受信部12、及び位置情報受信部13を備えている。

【００５２】

この内の位置情報受信部13は、位置情報送信装置50との通信により、クライアント10の現在位置を検出する。位置情報送信装置50としては、例えば、GPS(GlobalPositioning System)があり、このGPSは、衛星から発信される情報を利用してクライアント10と衛星の位置関係を測定しクライアント10の現在位置の緯度・経度を計算するシステムである。各クライアント10は、位置情報受信部13を用いて自分自身の現在位置を検出することができる。なお、本実施例(1)では、現在位置検出手段としてGPSを用いているが、現在位置検出手段はGPSに限定されない。

【００５３】

サーバ30のデータベース40wは、ユーザアカウントデータベース41w及びアクティブユーザデータベース44wで構成されている。この内のデータベース41wは、グループデータベース42w及び文書ファイルアクセス権管理データベース43wで構成されている。

【００５４】

実施例(1)では、例えば、ネットワーク60に企業Aの社内ネットワーク61(図１参照。)を経由してサーバ30が接続され、ユーザ(社員)1及びユーザ(社員)2（図示せず。）が出張先において、それぞれ、クライアント10_1，10_2を用いてサーバ30のデータ格納部45wに格納されている社内秘の文書ファイルにアクセスする場合を示す。このようなシステム運用に当たり、サーバ30のデータベース構築部33から、予め、ユーザ1及びユーザ2のアカウントを格納したユーザアカウントデータベース41wのグループデータベース42w及び文書ファイルアクセス権管理データベース43wを作成しておく。

【００５５】

図3(1)及び(2)は、それぞれ、ユーザアカウントデータベース41w(図２参照。)を構成するグループデータベース42w及び文書ファイルアクセス権管理データベース43wを示している。同図(1)に示されたグループデータベース42wは、グループ識別子(以下、IDと略称することがある。)42wa、ユーザ識別子42wb、及びパスワード42wcで構成されている。データベース42wには、例えば、ユーザ識別子42wb＝“ユーザ1～ユーザ3”が、グループID42wa＝“グループA”に属し、それぞれのパスワード42wc＝“パスワードP1～パスワードP3”であることが登録されている。

【００５６】

同図(2)に示された文書ファイルアクセス権管理データベース43wは、データ43wa、アクセス可能とする位置情報43wb、及びグループID/ユーザID43wcで構成されている。データベース43wには、例えば、アクセス可能とする位置情報43wb＝“○県△町1-1”又は“○県△町1-2”に位置するグループID/ユーザID＝“グループA”に属するユーザ(ユーザ1～3(同図(1)参照。)のみが、データ43wa＝“文書ファイル0”にアクセス可能であることが登録されている。

【００５７】

また、上記のように、文書ファイルに対してユーザグループ(グループID)を対応付ける他に、ユーザIDだけを単位として対応付けや、グループID及びユーザIDを単位として対応付けすることも可能である。

【００５８】

データベース42w及び43wへのデータ登録/削除は、データベース構築部33を介して行うことが可能であり、例えば、サーバ30の管理者からの手動登録であってもよいし、又は各ユーザ(社員)からのアカウント作成依頼をトリガとした自動登録であってもよい。

【００５９】

なお、この実施例(1)及び後述する実施例(2)～実施例(4)では、文書ファイルへのアクセスとして、閲覧のみを示すが、文保存、編集、印刷、コピー＆ペースト、及び画面キャプチャ等のアクセスも可能である。

【００６０】

図４は、図２に示したアクティブユーザデータベース44wの構成例を示している。このデータベース44wは、データ44wa、ユーザID44wb、及びユーザの現在位置44wcで構成されている。図4(1)は、ユーザ1のみが、クライアント10_1を起動している場合のデータベース44wを示し、同図(2)は、ユーザ1，2が、それぞれ、クライアント10_1，10_2を起動している場合のデータベース44wを示している。

【００６１】

図５は、図２に示した実施例(1)のアクセス権管理システム100wの動作例を示している。この動作例を以下に説明する。

【００６２】

ユーザ(社員)1，2(図示せず。)は、それぞれ、予め、クライアント10_1，10_2(クライアント10_2は図示せず。図２参照、)にサーバ30のアドレスを設定しておく。

【００６３】

ステップS200，S100：サーバ30は稼働中であり、ユーザ1が、例えば、出張先において、クライアント10_1を起動する。このとき、ユーザ2のクライアント10_2は未起動とする。クライアント10_1の位置情報受信部13は、位置情報送信装置からの位置情報700_1，700_2

，…を受信し、検出したクライアント10_1の現在位置701_1，701_2，…をアクセス要求部11に通知する。

【００６４】

ステップS101，S201：クライアント10_1とサーバ30との間で、接続のネゴシエーション710が行われ、クライアント10_1とサーバ30との間にネットワーク60を経由したコネクション60aが設定される。

【００６５】

ステップS102，S103：クライアント10_1において、ユーザ1は、起動コマンドを入力してアクセス要求部11を起動する。このアクセス要求部11は、例えば、OS上で動作する１アプリケーションであり、ユーザ1がユーザID及びパスワードを入力するための入力画面インタフェースを持つ。アクセス要求部11は、ユーザ1が入力したユーザID711a及びパスワード711bをサーバ30に送信する。

【００６６】

ステップS202：サーバ30において、アクセス合意部31は、データベース42wを参照721してパスワード711bが正当であるか否かを判断し、正当である場合“認証OK712a”、正当でない場合“認証NG712b”を示すユーザ認証結果712をクライアント10_1に送信する。

【００６７】

ステップS104，S103：クライアント10_1において、アクセス要求部11は、ユーザ認証結果712が“認証NG”を示すとき、ステップS103のユーザID及びパスワード入力画面に戻る。

【００６８】

ステップS104，S105：アクセス要求部11は、ユーザ認証結果712が“認証OK”を示すとき、恒常的又は定期的に(例えば、10秒毎若しくは現在位置が数ｍ移動する毎に)、サーバ30に対して、位置情報受信部13が受信したユーザID713a及び位置情報(現在位置)713bをアクセス合意部31に送信するように設定した後、ステップS106に進む。

【００６９】

ステップS203：サーバ30において、アクセス合意部31は、受信したユーザID713a及び位置情報713bをアクティブユーザデータベース44wに登録723する。

【００７０】

すなわち、アクセス合意部31は、受信したユーザID713aと位置情報713bにより、ユーザアカウントデータベース44wを検索し、この検索により、ユーザ1が対応付けられた各文書ファイルについて、データベース中でアクセス可能とされた位置と現在位置とが一致するか否かを判断する。一致した場合、アクセス合意部31は、例えば、文書ファイル0に対してアクティブなユーザ1と認識し、アクティブユーザデータベース44wにユーザ1を登録する。このとき、ユーザIDが登録済みであれば、現在位置44wcを上書する。

【００７１】

不一致の場合、アクセス合意部31は、文書ファイル0に対して非アクティブなユーザと認識し、例えば、アクティブユーザデータベース44wにユーザ1が登録済みの場合、ユーザIDの関連付けデータを削除する。

【００７２】

ここでは、ユーザ1の現在位置＝“○県△町1-1”は、文書ファイルアクセス権管理データベース43wの位置情報43wbと、文書ファイル0について一致し、一方で文書ファイル1については不一致である。この結果、アクティブユーザデータベース44wは図6(1)示したデータベースとなる。このように、恒常的もしくは定期的にアクティブユーザデータベース44wを更新することにより、サーバ30は、クライアント10_1の現在位置を把握しておくことが可能となる。

【００７３】

ステップS106：アクセス要求部11は、受信したい(閲覧したい)ファイル名及びユーザIDを含んだアクセス要求714をサーバ30に送信する。すなわち、アクセス要求部11は、上記ユーザ認証結果712の“OK通知”及びユーザ1による文書ファイル0の閲覧希望の意思をト

リガとして、アクセスしたいファイル名＝“文書ファイル0”、及びユーザID＝“ユーザ1”を含めたアクセス要求714をサーバ30に送信する。なお、閲覧希望のトリガのかけ方、及びファイル名の特定の方式は特に限定しないが、例えば、クライアント10_1上に専用データフォルダを用意し、フォルダ上のファイル名をクリックすると、アクセス要求部11がファイル名＝“文書ファイル0”及び“ユーザ1”をサーバ30に通知するようにしてもよい。

【００７４】

ステップS204，S205：サーバ30において、アクセス合意部31は、アクティブユーザデータベース44wを参照して、当該ファイル名＝“文書ファイル0”に対応付けられた(すなわち、アクティブな)ユーザID44wb及び現在位置44wcを獲得し、ユーザと現在位置が同一なユーザが(ユーザ1も含めて)2人以上、データベース44w上に登録されているか否かを判別する。

【００７５】

登録されていない場合、アクセス合意部31は、アクセス要求に対して“未合意715b”を示す判定結果(メッセージ)715をクライアント10_1に送信し、データファイルは送信せず、ステップS203のクライアントからの現在位置の受信待ち状態に戻る。登録済みの場合、アクセス合意部31は、“合意715a”を示す判定結果715をクライアント10_1に返信し、さらに、データ送信部32に対して“文書ファイル0”の送信指示719を与える。

【００７６】

図4(1)に示すように現在、データベース44wにはユーザ1のみしか登録されていないので、アクセス合意部31は、アクセス要求714に対して“未合意715b”を示す判定結果715をクライアント10_1に返信し、データ送信部32に対して送信指示719を与ない。

【００７７】

ステップS107：クライアント10_1において、アクセス要求部11は、“未合意”を示す判定結果715を受信して、ステップS106に戻り、ファイル名及びユーザIDの入力待状態になる。

【００７８】

この後、同じ出張先において、ユーザ(社員)2が、クライアント10_2(共に図示せず。)を起動したものとする。クライアント10_2とサーバ30の間で、上述したクライアント10_1のステップS101～S106及びサーバ30のステップS201～S203と同様の動作が行われ、ユーザ2がアクティブユーザデータベース44wに登録される。図4(2)は、ユーザ2がさらに登録されたアクティブユーザデータベース44wを示している。

【００７９】

この後のクライアント10_2とサーバ30との間の動作は、クライアント10_1に示したステップS106～S110、及びサーバ30のステップS204～ステップS208を参照して説明する。

【００８０】

ステップS106：クライアント10_2(図5のクライアント10_1参照。)において、アクセス要求部11は、受信したい(閲覧したい)ファイル名＝“文書ファイル0”及びユーザID＝“ユーザ2”を含んだアクセス要求714をサーバ30に送信する。

【００８１】

ステップS204，S205：サーバ30において、アクセス合意部31は、アクティブユーザデータベース44wを参照して、ファイル名＝“文書ファイル0”に対応付けられた(すなわち、アクティブな)ユーザID44wb及び現在位置44wcを獲得し、ユーザと現在位置が同一なユーザが(ユーザ2も含めて)2人以上、データベース44w上に登録されているか否かを判別する。

【００８２】

図4(2)に示すように現在、同図(1)に示したクライアント10_1の時と異なり、データベース44wには、“文書ファイル0”にアクセス権を有するユーザでユーザ2と現在位置が同一なユーザ1が(ユーザ2を含めて)２人登録されているので、アクセス合意部31は、クライアント10_2からのアクセス要求714に対して“合意715a”を示した判定結果715を応答する

。さらに、アクセス合意部31は、データ送信部32に対して、クライアント10_2への“文書ファイル0”の送信指示719を与える。

【００８３】

ステップS107：クライアント10_2において、“合意”を示す判定結果715を受信したアクセス要求部11は、データ受信部12にファイルの受信準備指示718を与える。

【００８４】

ステップS206，S108：サーバ30において、データ送信部32は、データ格納部45の文書ファイルデータベース46wに格納されたデータファイル(＝“文書ファイル0”)716を、クライアント10_2のデータ受信部12に送信する。データ受信部12はデータファイル716を受信し、クライアント10_2のユーザ2は、“文書ファイル0”の閲覧が可能になる。

【００８５】

なお、このとき、クライアント10_1が文書ファイル0に対するアクセス要求714をサーバ30に行った場合、クライアント10_2と同様に、クライアント10_1は、文書ファイル0にアクセスすることが可能である。

【００８６】

ステップS109，S110，S207，S208：クライアント10_1，10_2が“文書ファイル0”の閲覧を終了した後、各クライアント10は、サーバ30との間でコネクション60aの切断のネゴシエーション717を交換してコネクション60aを切断し、さらにクライアント10及びサーバ30は停止する。

【００８７】

以上説明したように実施例(1)では、文書ファイル0へのアクセス権を持つユーザが、文書ファイル0へのアクセスを希望したとき、このユーザの近隣の位置に、同じ文書ファイル0へのアクセス権を持つ他のユーザがいることをアクセス合意とみなし、アクセスを許可することが可能となる。

【００８８】

これにより、複数の社員(ユーザ)が出張した場合は、既存の認証システム等と同等の手続きで、文書の閲覧が可能になる一方、或るユーザが不正なデータ持ち出しを図った場合、閲覧できないこととなり、データ漏洩の防護耐性を高めることができる。

【００８９】

なお、「必要人数」の設定を追加し、例えば「必要人数」＝5の場合、アクティブなユーザが5人以上であることを以って、アクセス合意とみなしてもよい。

【００９０】

また、実施例(1)では、位置情報をGPSによる絶対位置(例では住所)で獲得した。このGPSは、屋外での使用には向くが、屋内での使用には難がある。したがって、実施例(1)は、例えば、複数社員の顧客訪問時、交通機関における移動中や顧客の玄関先における使用に向いている。

【００９１】

この実施例(1)を変形した実施例として、以下の形態であってもよい。

【００９２】

データ種別が、顧客/住民台帳等、各顧客/住民に対して住所及び各種情報が対応付けられたデータである場合、各顧客にもクライアント(端末)を予め貸し出しておき、１人の社員が顧客宅を訪問した際に、顧客宅において、社員と顧客が、各クライアントにユーザID及びパスワードを入力することで、位置情報に基づく複数人の合意とみなしてもよい。

【００９３】

また、クライアント(端末)自体は、１台であり、該クライアント上で各ユーザが、それぞれ、ユーザID及びパスワードを入力する形態であってもよい。

【００９４】

また、位置情報の取得は、GPSの代わりに、携帯電話によるアクセスポイント単位の位置情報取得や、普及が始まりつつある無線LANによるアクセスポイント単位の位置情報取得であってもよい。この内の携帯電話による位置情報の取得は、位置情報の単位はGPSよ

りも荒く、セキュリティは低いが、その代わりに、屋外はもとよりビル内等の屋内での使用も可能であり、柔軟な適用形態である。

【００９５】

また、一つのクライアントは、位置情報の取得部として、上記のどれか一つだけ対応していてもよいし、すべてを具備しておき使用環境(屋外／屋内、回線の速さ)に応じて使い分けられてもよい。さらに、クライアントーサーバ間の接続は、IPsec(SecurityArchitecture for the Internet Protocol)等の技術により暗号化されていることがセキュリティ上好ましいが、必須ではない。

【００９６】

また、上記の各データベース及びデータベース構築部33において、例えば、文書ファイル毎にアクセス種別(閲覧、編集、印刷等)を指定可能としておき、文書・ユーザ毎にアクセス種別を制御してもよい。

【００９７】

また、アクセス要求部11は、セキュリティ向上のため、サーバ30からNG通知を受信したクライアント10は、次に接続可能となるまでの時間を一定時間あけるか、或いは固定回数のNG通知を受けると暫く接続できなくする仕組みがあることが好ましい。

【００９８】

さらに、アクセス合意部31は、クライアント10_1にOK通知を送信した後、上述のように以後定期的にクライアント10から現在位置が通知される形態とする代わりに、クライアントからユーザ2によるアクセス要求を受けたことをトリガとして他のユーザの現在位置を取得し、アクティブユーザデータベースの位置情報を最新情報に更新する形態であってもよい。また、アクセス合意部31は、アクティブユーザデータベース上のユーザ数に基づき自動的に合意・非合意を判断する代わりに、他のユーザにユーザ2のアクセス可否を打診して、他のユーザの許可を以って合意となしてもよい。

【００９９】

実施例(2)：アドホックネットワーク接続に基づくアクセス合意

上述した実施例(1)では、各ユーザの絶対位置を基づき合意の可否を判定した。本実施例(2)では、近接する範囲内に位置するユーザ同士がネットワーク(例えば、アドホックネットワーク)を構築したか否かで、データへのアクセスに合意したか否かを判定する。

【０１００】

したがって、(1)GPS/携帯電話/無線LANからの電波が受信できない、(2)携帯電話/無線LANとの接続状況に基づき絶対位置を推定することができない、或いは(3)推定できたとしても十分な粒度が得られない等の理由で、各ユーザの絶対位置を取得できないような状況においても、本実施例(2)では、各ユーザが合意することができる効果がある。

【０１０１】

図６は、本発明の実施例(2)におけるアクセス権管理システム100xの構成例を示している。このアクセス権管理システム100xは、実施例(1)で示したアクセス権管理システム100wと同様に、アクセス権管理システム100xはネットワーク60で接続された複数のクライアント10及びサーバ30で構成されているが、実施例(1)と異なり位置情報送信装置50を必要としない代わりにクライアント10同士がアドホックネットワーク62で接続される。

【０１０２】

サーバ30の構成は、実施例(1)のサーバ30と基本的に同様であるが、データベース40xが異なっている。クライアント10の構成は、実施例(1)のクライアント10の位置情報受信部13の代わりにアドホックネットワーク構築部14を備えている。

【０１０３】

ユーザ(クライアント)が同一範囲内の位置に近接しネットワークを構築する一般的な従来技術としては、アドホックネットワークがある。アドホックネットワークとは、広くコンピュータ等の無線接続に用いられているIEEE802.11x、Bluetoothなどの技術を用いながら多数の端末をアクセスポイントの介在なしに相互に接続する形態をとるネットワークである。アドホックネットワークでは、基地局やアクセスポイント等のインフラがない場所

で、相互の端末のみでネットワークを構成することができる。逆にいえば、使用無線技術に応じた距離に相互の端末が近接しない限り、相互の端末は、ネットワークを構築することができない。なお、アドホックネットワークよりも利便性は劣るものの、ユーザが同一範囲内の位置に近接しネットワークを構築する手段として、端末同士を適時、妥当な長さの有線によって、相互に接続しても良い。

【０１０４】

図７は、図６に示したクライアント10_1，10_2における一般的なアドホックネットワーク構築部14の構成をより詳細に示している。各アドホックネットワーク構築部14は、それぞれ、ARP(AddressResolution Protocol)テーブル27_1，27_2(以下、符号27で総称することがある。)、論理インタフェース(以下、論理IFと略称することがある。)の属性テーブル28_1，28_2(以下、符号28で総称することがある。)、及び論理インタフェース14f_1，14f_2(以下、符号14fで総称することがある。)を備えている。

【０１０５】

なお、アドホックネットワーク構築部14の技術は、従来のアドホックネットワーク技術であり、テーブル27及び28は、IEEE802.11xの無線LAN技術におけるテーブル例を示している。すなわち、ARPテーブル27は、アドホックネットワーク62内のクライアント情報として、IPアドレス27a、MACアドレス27b、及び出力論理IF27cで構成されている。論理IFの属性テーブル28は、アドホックネットワークのグループ単位の情報として、論理インタフェース14fの付帯情報である、ESS-ID(ExtendedService Set Identifier)28b、チャネル番号(周波数)28c、及び暗号鍵28dで構成されている。なお、ESS-IDは、IEEE802.11xシリーズで規定する無線LANにおける識別子であり、本実施例(2)ではアドホックネットワークの識別子として利用する。

【０１０６】

アドホックネットワーク62上で、例えばクライアント10_1は、クライアント10_2にデータを送信する際には、テーブル27_1及び28_1を参照して宛先IPアドレス＝“ip#1”に対応するMACアドレス＝“MAC#1”等のパラメタを取得し、IEEE802.11の無線LAN技術を使いデータをエンコードした後、クライアント10_2に送信する。クライアント10_2は、受信したデータを、テーブル27_2，28_2に基づきデコードする。これにより、アドホックネットワーク62内でデータ通信が行われる。

【０１０７】

本実施例(2)では、アドホックネットワーク62で接続可能な範囲内に複数のクライアント10が存在し、接続されているときのみ、サーバ30のアクセス合意部31は、クライアント10がデータにアクセスすることに合意する。このクライアント10の接続状態の管理はデータベース40xで行われる。

【０１０８】

図８は、図６に示したデータベース40xにおけるユーザアカウントデータベース41xを示している。同図(1)及び(2)は、それぞれ、データベース41xの内のグループデータベース42x及び文書ファイルアクセス権管理データベース43xを示している。データベース42xは、図3(1)に示した実施例(1)のデータベース42wと同様であり、データベース43xは、アクセス可能とする位置情報43wbが無いことが図3(2)に示したデータベース43wと異なっている。

【０１０９】

図９は、図６に示したアクティブユーザデータベース44x示している。このデータベース44xは、図４で示した実施例(1)のアクティブユーザデータベース44wと異なり、ユーザID44xa及びアドホックネットワーク接続ユーザIDリスト44xbで構成されている。アドホックネットワーク接続ユーザIDリストとは、ユーザID44xaを持つユーザがアドホックネットワーク62を介して現在通信可能な対向ユーザの識別子のリストである。

【０１１０】

図９のデータベース44xでは、例えば、“ユーザ1”の対向ユーザ＝“ユーザ2”：１名、ユーザ3の対向ユーザ＝“ユーザ4及び5：2名(複数名によるリスト)”で相互にアドホッ

クネットワークを構築していることがわかる。

【０１１１】

図10は、図６に示した実施例(2)のアクセス権管理システム100xの動作例を示している。この動作例を以下に説明する。

【０１１２】

ステップS130，S131：サーバが稼働し、クライアント10_1が、ユーザ1(図示せず。)によって起動され、アドホックネットワーク構築部14が、他のクライアント10_2にアドホックネットワーク接続依頼730_1を送信する。アドホックネットワークが他のクライアントを発見する機構は、従来のアドホックネットワーク技術に依るものとする。クライアント10_1のアドホックネットワーク構築部14は、他クライアント10_2からアドホックネットワーク接続依頼可否731_1を受信する。クライアント10_1のアドホックネットワーク構築部14は、アドホックネットワーク接続依頼可否731_1＝“可”のとき、クライアント10_2との間でアドホックネットワーク62を構築し、“否”のとき、クライアント10_2との間でアドホックネットワーク62を構築しない。

【０１１３】

アドホックネットワーク構築部14は、イベント、定期的な、又は新たな他クライアントを発見したイベントによって継続的にアドホックネットワーク構築を試みる。

【０１１４】

ステップS131～S134，S231，S232：サーバ30及びクライアント10_1の間で接続のネゴシエーション740及びユーザ認証は、実施例(1)のステップS101～S104、及びS201，S202と同様である。

【０１１５】

ステップS233：クライアント10_1において、ステップS130とは逆に、アドホックネットワーク構築部14は、他クライアント10_2からクライアント10_2のユーザID及びパスワードを含むアドホックネットワーク接続依頼730_2を受信する。そして、アドホックネットワーク構築部14は、受信したユーザID及びパスワードを含むアドホックネットワーク接続ユーザ認証依頼743をサーバ30のアクセス合意部31に与える。

【０１１６】

アクセス合意部31は、グループデータベース42x(図８参照。)を参照して、受信したアドホックネットワーク接続ユーザ認証依頼743が正当(認証可)なとき、アクティブユーザデータベース44xのユーザID＝“ユーザ1”のアドホックネットワーク接続ユーザIDリスト44xbにユーザID＝“ユーザ2”を登録又は更新し、正当でない(認証否)とき、更新しない。さらに、アクセス合意部31は、クライアント10_1のアドホックネットワーク構築部14にユーザ認証依頼743の発信元のクライアント10_2宛てのアドホックネットワーク接続ユーザ認証結果744を返信する。

【０１１７】

クライアント10_1において、アドホックネットワーク構築部14は、受信したユーザ認証結果744が認証可を示すとき、認証可を示すアドホックネットワーク接続依頼可否731_2をクライアント10_2に返信すると共に、クライアント10_2との間で、アドホックネットワーク62を構築する。認証否を示すときアドホックネットワーク構築部14は、認証否を示すアドホックネットワーク接続依頼可否731_2をクライアント10_2に返信し、クライアント10_2との間でアドホックネットワークを構築しない。

【０１１８】

上述のように、クライアント10_1は、サーバ30へ他のクライアント10_2(ユーザ2)の認証を問い合わせ、認証されたとき、このクライアント10_2との間でアドホックネットワークを構築する。そして、サーバ30は、アクティブユーザデータベース44xにクライアント10_1(ユーザ1)がアドホックネットワークを構築しているユーザ2(クライアント10_1)を登録/更新する。

【０１１９】

なお、アクティブユーザデータベース44xからユーザ2の削除は、クライアント10_1とク

ライアント10_2との間のアドホックネットワークが切断された場合に行われる。

【０１２０】

ステップS135，S234～S235：クライアント10_1のユーザ1が、例えば、文書ファイル0の閲覧を希望し、ユーザID＝“ユーザ1”及び受信したいファイル名＝“文書ファイル0”を含むアクセス要求745をサーバ30に送信する。サーバ30において、アクセス合意部31は、文書ファイルアクセス権管理データベース43xを参照して、文書ファイル0に対応付けられているグループID/ユーザID43xb＝“グループA”を取得し、さらに、データベース42xを参照して“グループA”を展開したユーザID42xb＝“ユーザ1、ユーザ2、ユーザ3”を取得する。

【０１２１】

また、アクセス合意部31は、アクティブユーザデータベース44xから閲覧を要求しているユーザ1に対応するアドホックネットワーク接続ユーザIDリスト44xb＝“ユーザ2”を取得し、すなわち、ユーザ1とアドホックネットワークで相互接続コネクションを形成しているユーザ2を取得する。そして、アクセス合意部31は、ユーザ2が文書ファイル0にアクセス権を有しているグループAに属しているので、ユーザ1の文書ファイル0に対するアクセスに合意746aし、合意746aを示す合意判定結果746をクライアント10_1へ返信する。相互接続コネクションが形成していない場合は、アクセス合意部31は、未合意746bを示す合意判定結果746をクライアント10_1に返信する。

【０１２２】

クライアント10_1(＝ユーザ1)が、文書ファイル0の閲覧希望を要求した場合において、アドホックネットワーク62の相互接続コネクションを形成しているか否かのより詳細な判断方法を、図８及び図９のデータ内容に基づき以下に説明する。

【０１２３】

(1)文書ファイルアクセス権管理データベース43xを参照し、文書ファイル0に対応付けられているユーザIDに閲覧要求をしたユーザIDが含まれているか否か確認する。なければ、アドホックネットワークの相互接続コネクションなしと判定する。ここでは、グループA＝ユーザ1が含まれている。

【０１２４】

(2)文書ファイル0に対応付けられているユーザIDを抽出する。ここでは、ユーザ1～ユーザ3。

【０１２５】

(3)アクティブユーザデータベース44xを参照して、閲覧要求をしたユーザ1のアドホックネットワーク接続ユーザIDリスト44xbからユーザIDを抽出する。ここでは、ユーザ2が抽出される。

【０１２６】

(4)上記(2)及び(3)で抽出したユーザIDのAND演算する。ここでは、演算結果はユーザ2である。

【０１２７】

(5)上記(4)のそれぞれのユーザIDのアドホックネットワーク接続ユーザIDリスト44xbに閲覧要求をしたユーザのID＝“ユーザ1”があるか否かを判定する。ここでは、ユーザ2のアドホックネットワーク接続ユーザIDリスト44xbにユーザ1があるので、「有り」と判定する。

【０１２８】

(6)上記(5)において、一つでも「有り」があった場合、アドホックネットワークの相互接続コネクションがあると判定する。「有り」が一つもなかった場合、アドホックネットワークの相互接続コネクションがないと判定する。ここでは、アドホックネットワークの相互接続コネクションがある。

【０１２９】

なお、上記(5)では、一つでも「有り」があった場合、「アドホックネットワークの相互接続コネクションがある」と判定したが、例えば、図８(2)の文書ファイルアクセス権

管理データベース43xに文書ファイルの属性として、さらに、“必要コネクション数”を追加し、この“必要コネクション数”以上のアドホックネットワークの相互接続コネクションがあった場合、「相互接続コネクションがある」と判定すれば、より多くの複数ユーザによる合意を実現することができる。

【０１３０】

ステップS136，S137，S235，S236：クライアント10_1において、アクセス要求部11は、合意判定結果746が“未合意”を示すときステップS135に戻り、“合意”を示すとき、データ(文書ファイル0)の受信準備指示749をデータ受信部12に与える。一方、サーバ30において、アクセス合意部31は、アドホックネットワークの相互接続コネクションがあった場合、データ送信部32に対して文書ファイル0の送信指示750を与え、アドホックネットワークの相互接続コネクションがなかった場合、文書ファイル0の送信指示をデータ送信部32に与えない。

【０１３１】

送信指示750を受信したデータ送信部32は、データ格納部45に格納された文書ファイル0(データファイル747)をクライアント10_1に送信する。閲覧要求したクライアント10_1において、データ受信部12は、文書ファイル0(データファイル747)を受信する。

【０１３２】

これにより、ユーザ1はクライアント10_1上で文書ファイル0の閲覧が可能になる。

【０１３３】

ステップS138，S237：データ転送終了後、サーバ30とクライアント10_1の間でコネクション切断のネゴシエーション748が行われ、コネクション60aが切断される。

【０１３４】

さらに、アドホックネットワーク構築部14は、アドホックネットワーク62を構築しておく必要がなくなった場合は、アドホックネットワーク切断依頼を他クライアント10_2へ送信する。アドホックネットワーク切断依頼を受信したアドホックネットワーク構築部14は、切断依頼元のユーザID、パスワードを内包するアドホックネットワーク切断ユーザ認証依頼をサーバ30へ送信する(図示せず。)。

【０１３５】

アドホックネットワーク切断ユーザ認証依頼を受信したサーバ30のアクセス合意部31は、認証OKならば、アクティブユーザデータベース44xを更新し、認証OKを示すアドホックネットワーク接続ユーザ認証結果をクライアント10_2へ送信する。認証NGのとき、アクセス合意部31は、アクティブユーザデータベース44xを更新せずに、認証NGをクライアント10_2に送信する(図示せず。)。

【０１３６】

上記のアドホックネットワーク接続ユーザ認証結果を受信したクライアント10_2のアドホックネットワーク構築部14は、認証OKならば、該当の他クライアント10_1とのアドホックネットワーク62の接続を切断し、認証NGならば、アドホックネットワーク62の接続を切断しない。

【０１３７】

また、アドホックネットワーク構築部14が、従来のアドホックネットワーク技術として、他クライアントが発見できなくなった場合も、他のクライアントのアドホックネットワーク切断依頼をサーバ30へ送信する。このとき、クライアント10のアドホックネットワーク構築部14は、他のクライアントの認証情報(パスワード等)を送信することはできないが、すでに、通信が不可能な状態、例えば、クライアント相互の距離が離れ過ぎている状況になっているので、サーバ30のアクセス合意部31は、上記の他クライアント10の認証無しで、アクティブユーザデータベース44xを更新する。

【０１３８】

以上のように、実施例(2)のアクセス権管理システム100xによれば、複数のユーザがアドホックネットワーク構築可能範囲内の位置に近接しアドホックネットワークを構成することで、アクセス権を保有するユーザの合意とみなし、データにアクセスすることを可能

にする。これによって、実施例(1)と同様の漏洩防護への耐性を高めることができることに加えて、各ユーザが絶対位置を取得できないような状況においても、アクセス権を保有するユーザの合意を実現することができる効果がある。

【０１３９】

実施例(3)：クライアントによるデータ分散保持

上述した実施例(2)では、データがサーバ30のデータ格納部45のみに保持されていたのと異なり、本実施例(3)では、複数のクライアント10が暗号化したデータ及びこのデータの暗号化/復号化のための鍵を分散して保持する。

【０１４０】

図11は、本発明の実施例(3)におけるアクセス権管理システム100yの構成例を示している。このアクセス権管理システム100yが、図６に示した実施例(2)のアクセス権管理システム100xと異なる点は、実施例(2)においてサーバ30が備えていたデータ格納部45が、実施例(3)では、各クライアント10_1，10_2に、それぞれ、データ格納部25_1，25_2(以下、符号25で略称することがある。)として分散されていることである。さらに、アクセス権管理システム100yが、実施例(2)のアクセス権管理システム100xと異なる点は、サーバ30からクライアント10にデータを伝送するためのサーバ30のデータ送信部32及びクライアント10のデータ受信部12の代わりに、分散されたデータ格納部25に格納されたデータをクライアント10相互間で送受信するためのデータ送信部15及びデータ受信部16が、クライアント10に付加されていることである。

【０１４１】

図12は、サーバ30が備えているユーザアカウントデータベース41yを示している。同図(1)及び(2)は、それぞれ、ユーザアカウントデータベース41yの内のグループデータベース42y及び文書ファイルアクセス権管理データベース43yを示している。

【０１４２】

グループデータベース42y及び文書ファイルアクセス権管理データベース43yは、図８の実施例(2)で示したグループデータベース42x及び文書ファイルアクセス権管理データベース43xと同様である

図13は、アクティブユーザデータベース44yを示しており。このデータベース44yは、図９の実施例(2)で示したアクティブユーザデータベース44xと同様である。

【０１４３】

なお、図12及び図13には、図11に示されていないユーザ3，ユーザ4，及びユーザ5(クライアント10_3，クライアント10_4，及びクライアント10_5)のデータが含まれている。

【０１４４】

図14(1)及び(2)は、それぞれ、クライアント10_1及び10_2のデータ格納部25が保持する文書ファイルデータベース26y_1及び26y_2(以下、符号26yで総称することがある。)を示しており、データベース26yは、データ名26ya、データ内容26yb、及び鍵26ycで構成されている。すなわち、データベース26yは、データ名26ya＝文書ファイルnを主キーとして、データ内容26yb＝“暗号化分割文書ファイルn-m”と分割鍵26yc＝“分割鍵n-m”を保持する。暗号化分割文書ファイルn-mは、文書ファイルnを暗号化して分割した分割部分mを意味する。分割鍵n-mは、文書ファイルnの鍵nを分割した分割部分mを意味する。

【０１４５】

例えば、文書ファイル0は、分割されてそれぞれ、データベース26y_1及び26y_2のデータ内容26ybに、暗号化分割文書ファイル0-0，0-1として格納されている。また、各暗号化分割文書ファイル0-0，0-1を暗号化/復号化(解読)するため鍵0の一部である分割鍵0-0，0-1は、それぞれ、データベース26y_1，26y_2の鍵26ycに格納されている。

【０１４６】

暗号化分割文書ファイル0-0，0-1を結合して暗号化文書ファイル0を形成し、分割鍵0-0，0-1を結合して鍵0を形成する。そして、暗号化文書ファイル0を鍵0で復号化することで、閲覧可能な文書ファイル0を得ることができる。

【０１４７】

図15は、実施例(3)におけるアクセス権管理システム100yの動作例を示している。この動作例を以下に説明する。

【０１４８】

ステップS150～S154，S250～S252：実施例(2)のステップS130～S134，S230～S232と同様である。サーバ30とクライアント10_1との間で、接続のネゴシエーション770及びユーザの認証を行う。

【０１４９】

ステップS155，S253～S255：実施例(2)のステップS135，S136，S234～S236と同様である。アドホックネットワーク接続ユーザIDがアクティブユーザデータベース44yに登録され、クライアント10_1とサーバ30との間でユーザID及びファイル名を含むアクセス(閲覧)要求775と、合意/未合意を示す判定結果776が送受信される。

【０１５０】

なお、ステップS255の判断手順は、すなわち、アドホックネットワークの相互接続コネクションを形成しているか否かの判断手順は、実施例(2)のステップS235の判定動作と異なっている。

【０１５１】

データベース41y(42y，43y)，44y，25yのデータ内容が、それぞれ、図12、図13及び図14の場合で、クライアント10_1(＝ユーザ1)が、ファイル名＝文書ファイル0のアクセス(閲覧)要求775を行ったときの実施例(3)における判断手順を以下に説明する。

【０１５２】

(1)文書ファイルアクセス権管理データベース43yにおいて、データ43ya＝“アクセス要求された文書ファイル0”に対応するグループID/ユーザID43ybにアクセス要求されたユーザID＝“ユーザ1”が有るか否か確認する。ここでは、ユーザ1が有る。ユーザ1が無い場合、ユーザ1には文書ファイル0に対するアクセス権がないと判定する。

【０１５３】

(2)データベース43yのデータ43ya＝“文書ファイル0”に対応するグループID/ユーザID43ybからアクセス要求をしたユーザID＝“ユーザ1”を除いたユーザIDを抽出する。ここでは、ユーザ2が抽出される。

【０１５４】

(3)アクティブユーザデータベース44yにおいて、ユーザID44ya＝“アクセス要求をしたユーザ1”に対応するアドホックネットワーク接続ユーザIDリスト44ybに登録されたユーザIDに、上記(2)で抽出したユーザが全て含まれているか否かを確認する。ここでは、ユーザ2が含まれている。もし、含まれていなければ、アドホックネットワークの相互接続コネクションなしと判定する。

【０１５５】

(4)上記(2)のすべてのユーザIDに関して、そのアドホックネットワーク接続ユーザIDリスト44ybにアクセス要求をしたユーザのID＝“ユーザ1”があるか否かを判定する。ここでは、ユーザ2のアドホックネットワーク接続ユーザIDリスト44ybにユーザ1があるので、「有り」と判定する。

【０１５６】

(5)上記(4)において、「有り」であった場合、アドホックネットワークの相互接続コネクションがあると判定する。ここでは、アドホックネットワークの相互接続コネクションがある。

【０１５７】

上記(1)～(5)の手順で示したステップS255における判定が、実施例(2)のステップS235における判定と異なる点は、或る文書ファイルに或るユーザがアクセス要求をした場合、アクセスを要求された文書ファイルに対してアクセス権を有する全てのユーザとアドホックネットワークを構築していた場合のみ、「アドホックネットワークの相互接続コネクションがある」と判定していることである。

【０１５８】

このように判定する理由は、本実施例(3)では、文書ファイルに対してアクセス権を有する全てのユーザ(クライアント)間で、文書ファイルを分散保有しているためである。

【０１５９】

なお、例えば、文書ファイル0に対してアクセス権を有するユーザ数が多く、運用上の利便性が下がってしまうような場合には、全てのユーザではなく、特定の2人以上を組み合わせたユーザ同士がアドホックネットワークを構築した場合、アドホックネットワークの相互接続コネクションがあると判定するようにしてもよい。この場合、各クライアント10の文書ファイルデータベース26y(図14参照。)が、各文書ファイルに対して、ユーザの組合わせパターン別に暗号化分割文書ファイル及び分割鍵を保持すればよい。

【０１６０】

ステップS156：クライアント10_1において、アクセス要求部11は、“合意”を示す判定結果776を受信したとき、データ受信部12に受信準備指示779を与える。

【０１６１】

ステップS157，S255：アクセス合意部31において、判定結果776が“合意(アドホックネットワークの相互接続コネクションがある)”のとき、サーバ30は、それぞれ、クライアント10_1及び10_2に対して文書ファイル0の送信指示777_1及び777_2(以下、符号777で総称することがある。)を与える。この送信指示777には、閲覧要求元のクライアント10_1のユーザID＝“ユーザ1”及びファイル名＝“文書ファイル0”が含まれている。

【０１６２】

送信指示777を受信した各クライアント10のデータ送信部15は、それぞれ、データ格納部25_1及び25_2の文書ファイルデータベース26y_1，26y_2から文書ファイル0に対応する暗号化分割文書ファイルと分割鍵を読み出し、自分自身がアクセス要求元であった場合には、自データ受信部12へ暗号化分割文書ファイル762a_1及び分割鍵762b_1を送信し、自身がアクセス要求元でない場合には、送信指示777で指示されたアクセス要求元のクライアント10_1のデータ受信部12に暗号化分割文書ファイル762a_2及び分割鍵762b_2を送信する。

【０１６３】

ステップS158：クライアント10_1において、データ受信部16は、文書ファイル0の全ての暗号化分割文書ファイル及び全ての分割鍵を受信する。そして、データ受信部16は、それぞれ、暗号化分割文書ファイル及び分割鍵を結合して、暗号化文書ファイル0及び鍵0を形成し、暗号化文書ファイル0を鍵0で復号化することにより、閲覧可能な文書ファイル0を作成する。これにより、クライアント10_1のユーザ1は、文書ファイル0を閲覧することが可能となる。

【０１６４】

ステップS159，S160，S255，S256：クライアント10_1及びサーバ30間のコネクション60aの切断のネゴシエーション778の手順は、実施例(2)のステップS138，S139，S237，及びS238で示した切断のネゴシエーション748の手順と同様である。

【０１６５】

このように、クライアント10がデータ(文書ファイル)を分散保持することによって、実施例(1)と同様の漏洩防護への耐性を高めることができる。また、サーバ30とクライアント10間のネットワーク60の使用帯域を節約することが可能になる。すなわち、アドホックネットワーク62よりも帯域が狭い、或いは従量課金のあるクライアント10とサーバ30間とのネットワーク60を使用せずに、容量が多い文書ファイルのデータをクライアント10相互間で送受信することが可能になる。この結果、サーバ30とクライアント10と間のネットワーク60の使用帯域を節約できる効果がある。

【０１６６】

さらに、各クライアント10のセキュリティが例え破られたとしても、完全なデータ(文書ファイル)が漏洩してしまうことはないという、漏洩防護への耐性を高めることができる。

【０１６７】

なお、上述した実施例(3)においては、文書ファイル及び鍵を分散して保有したが、鍵のみを分散して保有することも可能である。鍵のみを分散保有した場合、ある一つのクライアントのセキュリティが破られた場合、完全なファイルが漏洩してしまう危険性があるが、アドホックネットワーク62の使用帯域を節約することができる。

【０１６８】

実施例(4)：各クライアントがアクセス合意部を分散保持

この実施例(4)では、実施例(3)におけるサーバ30のアクセス合意部31の機能は、各クライアント10にアクセス合意部18として分散される。この結果、実施例(4)ではサーバ30を必要としない。

【０１６９】

図16は、本発明の実施例(4)におけるアクセス権管理システム100zの構成例を示している。このアクセス権管理システム100zは、複数の、例えばクライアント10_1～10_3で構成されている。各クライアント10の構成が、実施例(3)に示したクライアント10と異なる点は、サーバ30に対してアクセス要求したアクセス要求部11の代わりにクライアント10間相互にアクセス要求するアクセス要求部17を備えていることである。また、実施例(3)において、サーバ30が保持していたアクセス合意部31、データベース構築部33、及びデータベース40yを、各クライアント10が、アクセス合意部18、データベース構築部19、データベース20z(符号20z_1, 20z_1の総称である。)として備えていることも異なっている。

【０１７０】

本実施例(4)では、[1]「文書に対するアクセス権の合意」に係る実施例、及び[2]「データベース構築部分散時のアクセス権管理」に係る実施例に分けて説明する。

【０１７１】

[1]文書に対するアクセス権の合意

図17は、データベース20zを構成するユーザアカウントデータベース21zを示している。このデータベース21zは、グループデータベース22z及び文書ファイルアクセス権管理データベース23zで構成されている。

【０１７２】

同図(1)は、クライアント10_1及び10_2が，保持するグループデータベース22z_1及び22z_2を示している。このグループデータベース22z_1及び22z_2は、同じデータベースであり、グループID22za、ユーザID22zb、及びパスワード22zcで構成されている。

【０１７３】

同図(2)及び(3)は、それぞれ、クライアント10_1及び10_2の文書ファイルアクセス権管理データベース23z_1及び23z_2(以下、符号23zで総称することがある。)を示しており、データ23za及びグループID/ユーザID23zbで構成されている。データベース23zは、各クライアント10自身がアクセス権を有する文書ファイルに関するデータベースである。例えば、同図(2)のデータベース23z_1では、クライアント10_1は、文書ファイル0と文書ファイル1にアクセス権を有する自分自身を含めたユーザIDを保持し、同図(3)のデータベース23z_2では、クライアント10_2は、文書ファイル0にアクセス権を有するユーザIDを保持している。

【０１７４】

図18(1)及び(2)は、それぞれ、クライアント10_1及び10_2が、保持するアクティブユーザデータベース24z_1及び24z_2を示している。このデータベース24z_1及び24z_2には、それぞれ、クライアント10_1及び10_2がアドホックネットワークを構成しているアドホックネットワーク接続ユーザIDリストを保持している。

【０１７５】

図19(1)及び(2)は、それぞれ、クライアント10_1及び10_2が保持する文書ファイルデータベース26z_1及び26z_2(以下、符号26zで総称することがある。)を示している。文書ファイルデータベース26zは、図14に示した実施例(3)の文書ファイルデータベース26yと同様であり、データ名26za、データ内容26zb、及び鍵26zcで構成されている。

【０１７６】

図20は、実施例(4)における動作手順を示している。この動作手順を以下に説明する。なお、この説明では、２つのクライアント10_1及び10_2のみの場合を説明するが、３つ以上のクライアントがある場合の動作手順も同様である。

【０１７７】

ステップS170，S270：クライアント10_1，10_2がそれぞれ起動する。

【０１７８】

ステップS171，S172，S271，S272：クライアント10_1，10_2のアドホックネットワーク構築部14は、それぞれ、他クライアントとの間で継続的にアドホックネットワーク62を構築する。すなわち、クライアント10_1において、アドホックネットワーク構築部14はアドホックネットワーク接続依頼790をクライアント10_2に送信する。クライアント10_2において、アドホックネットワーク接続依頼790を受信したアドホックネットワーク構築部14は、アドホックネットワーク接続のユーザ認証依頼791をアクセス合意部18に与える。アクセス合意部18は、ユーザアカウントデータベース21z_1を参照811して、実施例(3)と同様に認証を行い、アドホックネットワーク接続のユーザ認証結果792をアドホックネットワーク構築部14に返信する。さらに、認証OKであった場合、アクセス合意部18は、アクティブユーザデータベース24z_2にクライアント10_1(=ユーザ1)を登録813する。

【０１７９】

ユーザ認証結果792を受信したアドホックネットワーク構築部14は、クライアント10_1のアドホックネットワーク構築部14にアドホックネットワーク接続依頼応答793を送信する。この応答793には、クライアント10_2の認証情報(ユーザ2及びパスワードP2)を含んでいる。

【０１８０】

クライアント10_1において、応答793を受信したアドホックネットワーク構築部14は、応答793に含まれる認証情報(ユーザ2及びパスワードP2)を含むユーザ認証依頼794をアクセス合意部18に送信する。このアクセス合意部18は、ユーザアカウントデータベース21z_1を参照802して、認証を行い、ユーザ認証結果795をアドホックネットワーク構築部14へ与える。さらに、認証OKであった場合、アクセス合意部18は、アクティブユーザデータベース24z_1にクライアント10_2(=ユーザ2)を登録803する。

【０１８１】

このアドホックネットワーク構築の一連の動作を行うことで、図18(1)及び(2)のアクティブユーザデータベース24z_1及び24z_2のように、ユーザ2及びユーザ1がユーザIDリストに登録/更新される。

【０１８２】

ステップS173，S273，S274：クライアント10_1において、アクセス要求部17は、ユーザアカウントデータベース21z_1の文書ファイルアクセス権管理データベース23z_1を参照802し、文書ファイル0にアクセス権を有する自身以外のすべてのユーザIDを抽出する。ここでは、ユーザ2が抽出される。さらに、アクセス要求部17は、アクティブユーザデータベース24z_1を参照804し、抽出したユーザID＝ユーザ2が、アドホックネットワーク接続ユーザIDリスト(アクティブユーザデータベース24z_1(図18(1)参照。)にあることを確認する。ここでは、ユーザ2がアドホックネットワーク接続ユーザIDリストにある。アクセス要求部17は、文書ファイル0にアクセス権を有する自身以外のすべてのクライアントへアクセス(閲覧)要求796を送信する。すなわち、アクセス要求部17は、文書ファイル0のアクセス要求796をクライアント10_2に送信する。

【０１８３】

クライアント10_2において、アクセス要求796を受信したアクセス合意部18は、クライアント10_1(ユーザ1)との間で、アドホックネットワークの相互接続コネクションを形成しているか否かをアクティブユーザデータベース24z_2を参照814して判断する。形成していた場合は、アクセス合意部18は、“合意797a”を示す判定結果797を、アクセス要求796を送って来たクライアント10_1に返送し、データ送信部15に対してデータの送信指示807を与える。形成していない場合、“未合意797b”を示す判定結果797を返信する。

【０１８４】
ここで、ステップS274における「アドホックネットワーク62の相互接続コネクションを形成しているか否か」のより詳細な判定動作を以下に説明する。
【０１８５】
(1)文書ファイルアクセス権管理データベース23z_2を参照して、文書ファイル0に対応付けられているユーザIDに、アクセス要求をしたユーザID=ユーザ1が含まれているか否かを確認し、無ければ、アクセス権無しと判定する。ここでは、ユーザ1が有るので、アクセス権有りと判定する。
【０１８６】
(2)アクティブユーザデータベース24z_2を参照してアドホック接続ユーザIDリストにアクセス要求をしたユーザID=ユーザ1があるか否かを確認する。無い場合、アドホックネットワークの相互接続コネクションは無しと判定する。ここでは、ユーザ1が有るので、「有り」と判定する。
【０１８７】
(3)上記(2)において、「有り」と判定した場合、アドホックネットワーク相互接続コネクションが有ると判定する。ここでは、アドホックネットワークの相互接続コネクションがある。
【０１８８】
ステップS174：クライアント10_1において、アクセス要求部17は、アクセス要求796を送信したすべてのクライアント(ここでは、クライアント10_2のみ)から、“合意”を示した合意判定結果797を受信した場合、データ送信部15へ、暗号化分割文書ファイル0-0及び分割鍵0-0の送信を指示するデータ送信指示805aを与え、データ受信部16に受信準備指示805bを与える。
【０１８９】
ステップS175，S176，S275：クライアント10_2において、アクセス合意部18は、データ送信部15に対して、文書ファイルデータベース26z_2に保持されている暗号化分割文書ファイル0-1及び分割鍵0-1の送信指示807を与える。データ送信部15は、それぞれ、文書ファイル0-1及び分割鍵0-1を含む暗号化分割文書ファイル798a及び分割鍵798bをクライアント10_1に送信する。
【０１９０】
クライアント10_2において、データ送信部15から暗号化分割文書ファイル0-1及び分割鍵0-1を受信する。クライアント10_1のデータ送信部15は、文書ファイルデータベース26z_1が保持している暗号化分割文書ファイル0-0及び分割鍵0-0を、それぞれ、暗号化分割文書ファイル806a及び分割鍵806bに含めてデータ受信部16に与える。データ受信部16は、受信した暗号化分割文書ファイル0-0，0-1及び分割鍵0-0，0-1を結合して、暗号化文書ファイル0及び鍵0を形成し、暗号化文書ファイル0を鍵0で復号化して文書ファイル0を作成する。
【０１９１】
この結果、クライアント10_1のユーザ1は、文書ファイル0の閲覧が可能となる。
【０１９２】
ステップS177，S276：クライアント10_1及び10_2は、それぞれ、停止する。
【０１９３】
上述したで動作手順によれば、複数のクライアント10がアクセス合意部を分散保有することができる。この結果、実施例(3)と同様の効果を享有しつつ、サーバ30がない状況において、文書ファイルにアクセスすることが可能になる。
【０１９４】
[2]アクセス権分散管理
アクセス権分散時の動作手順を以下に説明する。この説明においては、クライアント10_1及び10_2が、例えば、文書ファイル0分散保有している場合について説明する。
【０１９５】

まず、クライアント10_1(=ユーザ1)、クライアント10_2(=ユーザ2)、及びクライアント10_3(=ユーザ3)がアドホックネットワーク62を構築する。そして、クライアント10_3が、アクセス権を有していない文書ファイル0に対するアクセス権を要求したとき、各クライアント10_1～10_3において、データベース構築部19_1～19_3のアクセス権管理機能は、文書ファイル0をクライアント10_1～10_3に分散する。

【０１９６】

図21は、実施例(4)：アクセス権分散管理におけるユーザアカウントデータベース21zを示している。このデータベース21zは、同図(1)に示したグループデータベース22zと同図(2)～(4)に示したクライアント毎に異なる文書ファイルアクセス権管理データベース23zとで構成されている。

【０１９７】

同図(1)のグループデータベース22zは全クライアント10_1～10_3に共通であり、実施例(4)のグループデータベース22zと同様である。同図(2)～(4)の文書ファイルアクセス権管理データベース23z_1～23z_3(以下、符号23zで総称することがある。)は、それぞれ、クライアント10_1～10_3が保持しているデータベースであり、図17(2)及び(3)で示した実施例(3)のデータベース23zと同様である。図21(4)のクライアント10_3のデータベース23z_3には、クライアント10_3が、現在、文書ファイル1を管理していることが示されている。

【０１９８】

なお、同図(2)～(4)のデータベース23zの内の(2a)～(4a)は、更新前のデータベース23z_1～23z_3を示し、(2b)～(4b)は更新後のデータベース23z_1～23z_3を示している。

【０１９９】

図22(1)～(3)は、各クライアント10_1～10_3が、それぞれ、保持する文書ファイルデータベース26z_1～26z_3(以下、符号26zで総称することがある。)を示している。このデータベース26z_1及び26z_2は、図19に示し文書ファイルデータベース26z_1，26z_2と同様である。クライアント10_3のデータベース26z_3には、クライアント10_3が文書ファイル1の内の暗号化分割文書ファイル1-2及び鍵0の分割鍵1-2を管理していることを示している。

【０２００】

なお、図22(1)～(3)の内の(1a)～(3a)は更新前のデータベース26z_1～26z_3を示し、(1b)～(3b)は更新後のデータベース26z_1～26z_3を示している。

【０２０１】

図23は、実施例(4)：アクセス権分散管理における動作手順を示している。この動作手順を以下に説明する。なお、アクセス権分散管理機能は、各クライアントのアドホックネットワーク構築部14_1～14が備えている。

【０２０２】

ステップS10，S20，S30：クライアント10_1～10_3において、アドホックネットワーク構築部14_1～14は、アドホックネットワーク62を構築する。クライアント10_3のデータベース構築部19_1は、アドホックネットワーク62を構成している自身以外のすべてのクライアント10_1，10_2に文書検索820，821をブロードキャストする。すなわち、クライアント10_3は、アクセス権を要求する文書ファイルの存在自体を知らないので、存在する文書ファイルの文書検索をする必要がある。なお、この検索条件には、検索用のキーワードを含めてもよい。

【０２０３】

ステップS11，S21：クライアント10_1において、文書検索820を受信したデータベース構築部19は、ユーザアカウントデータベース21z_1を参照822aして、文書検索メッセージの認証を行う。認証OKである場合、データベース構築部19_1は、ユーザアカウントデータベース21z_1を参照822bして、全ての文書名(又は検索条件がある場合は検索条件に合致した文書名)及びこの文書のアクセス権を保有するユーザIDをクライアント10_3へ返信する。同様に、クライアント10_2も文書名及びアクセス権を保有するユーザIDをクライアント10_3へ返信する。

【０２０４】

ステップS31：クライアント10_3において、データベース構築部19_3は、クライアント10_1及び10_2から返信された検索結果のメッセージを、ユーザアカウントデータベース21z_3を参照826して認証し、認証OKであるものを抽出する。ここでは、すべてのメッセージが認証OKであったものとする。

【０２０５】

ステップS32(アクセス権許可要求文書ファイル決定)：さらに、データベース構築部19_3は、アクセス権を要求する文書ファイルを決定する。この決定は、例えば、ユーザ3が手動で行うこととし、ここでは、文書ファイル0を決定した。そして、データベース構築部19_3は、文書ファイル0のアクセス権を有するすべてのクライアント10_1(=ユーザ1)及びクライアント10_2(=ユーザ2)に、それぞれ、アクセス権許可要求827_1，827_2を送信する。

【０２０６】

ステップS12，S21：クライアント10_1において、アクセス権許可要求827_1を受信したデータベース構築部19_1は、アクセス権許可の可否判断を行い、アクセス権許可要求結果830をクライアント10_3へ送信する。アクセス権許可が“可”のとき、データベース構築部19_1は、文書ファイルデータベース26z_1から暗号化分割文書ファイル0-0及び分割鍵0-0をそれぞれ含んだ暗号化分割文書ファイル829a及び分割鍵829bを読み出し、この暗号化分割文書ファイル829a及び分割鍵829bをアクセス権許可要求結果830に含める。上記の可否判断は、例えば、ユーザ1が手動で行ってもよいし、ユーザ1が手動で行う代わりに予めエージェントに可とする条件を与えておき、エージェントが自動で判断してもよいし、さらには、アドホックネットワーク62を構築していることを以って自動で可としてもよい。ここでは、“可”であったとする。

【０２０７】

クライアント10_2においても同様の動作手順で、データベース構築部19_2は、アクセス権許可要求結果(可、暗号化分割文書ファイル0-1及び分割鍵0-1)832をクライアント10_3に返信する。

【０２０８】

ステップS33：クライアント10_3において、データベース構築部19_3は、文書ファイル0のすべての暗号化分割文書ファイル及び鍵0のすべての分割鍵を受信し、文書ファイル0の再分割処理を行う。なお、データベース構築部19_3は、受信したアクセス権許可結果が可でない場合は、以降の処理は行わず、クライアント10_3はアクセス権を得られない。

【０２０９】

ここで、文書ファイルの再分割処理とは、一度、暗号化分割文書ファイルを結合して、復号化して、完全な文書ファイル0を得た後に、再度、新たにアクセス権保有ユーザとなったユーザ3(クライアント10_1)も含めて、3つのユーザ1～3(クライアント10_1～10_3)に再分割する処理である。クライアント10_3のデータベース構築部19_3は、それぞれ、新分割情報833及び834に基づき、ユーザアカウントデータベース21z_3及び文書ファイルデータベース26z_3を更新する。さらに、データベース構築部19_3は、それぞれ、新分割情報835及び836をクライアント10_1及び10_2に送信する。

【０２１０】

クライアント10_1，10_2において、データベース構築部19_1及び19_2は、それぞれ、受信した新分割情報835及び836に基づき、ユーザアカウントデータベース21z_1及び21z_23並びに文書ファイルデータベース26z_1及び26z_2を更新837～840する。

【０２１１】

この結果、各クライアント10において、新分割情報に基づき、ユーザアカウントデータベース21z_1～21z_3及び文書ファイルデータベース26z_1～26z_3が、図21(2)～(4)及び図22(1b)～(3b)に示すように更新されることになる。すなわち、分散保有している文書ファイルアクセス権管理データベースの更新、及びこの更新に対応する文書ファイルデータベースの更新を実現する。

【０２１２】

上述したように本実施例(4)によれば、サーバ30と通信せずに、文書に対するアクセス

権保有ユーザの合意を実現することができる。また、サーバ30と通信しなくて済むということは、サーバとの通信インフラがない状況において、各クライアント10が適宜、アドホックネットワーク62を構築することによって、文書に対するアクセスが実現できる効果がある。また、サーバなしで、システムを構築することができ、特権的なサーバ管理者からの情報漏洩を防ぎ、システムの漏洩防護への耐性を高めることができる効果がある。

【０２１３】

また、グループデータベースの更新、例えば、まったく新しいユーザ6が、本システムに参加する場合には、クライアント10_6(=ユーザ6)が自身の認証情報(ここでは、パスワード)を他のクライアントへ伝達することで、実現できる。

【０２１４】

なお、データベース構築部(アクセス権管理機能)とは、一般的にいうところのユーザ・アドミッションを実現するグループデータベースと文書ファイル毎のアクセス権保有ユーザの管理を実現する文書ファイルアクセス権管理データベースを含むユーザアカウントデータベース、及び、該データベースのデータ内容を構築するデータベース構築部である。

【０２１５】

また、サーバなしで、システムを構築することによるシステムの漏洩防護への耐性を高める効果のみを得る目的ならば、クライアント間のネットワークは、必ずしもアドホックネットワークである必要はなく、一般的な有線のLANでも構わない。

【０２１６】

（付記１）

データに対してアクセス権を保有する複数のユーザを関連付けたユーザアカウントデータベースと、

該アクセス権保有ユーザの内、現在、該データに対するアクセスに合意しているユーザを示すアクティブユーザデータベースと、

該アクティブユーザデータベースに示された該合意しているアクセス権保有ユーザの現在数が複数であるときのみ、該データに対してアクセス要求して来た該アクセス権を保有するユーザに該データへのアクセスを合意するアクセス合意部と、

で構成されたことを特徴とするアクセス権管理システム。

（付記２）上記の付記１において、

該システムがサーバと１つ以上のクライアントで構成され、

該サーバが、該ユーザアカウントデータベース、該アクティブユーザデータベース、及び該アクセス合意部を備え、

各クライアントが、自分の現在位置を検出する位置情報検出部と、該検出した現在位置及び該ユーザから受け付けたアクセス要求を該アクセス合意部に送信するアクセス要求部とを備え、

該アクセス合意部が、受信した該現在位置を該アクセス権保有ユーザに対応付けて該アクティブユーザデータベースに登録し、所定の範囲内に位置するユーザ数を、該合意しているユーザの現在数とすることを特徴としたアクセス権管理システム。

（付記３）上記の付記１において、

該システムがサーバと１つ以上のクライアントで構成され、

該サーバが、該ユーザアカウントデータベース、該アクティブユーザデータベース、及び該アクセス合意部を備え、

各クライアントが、他のクライアントとの間でネットワークを構築するネットワーク構築部と、ネットワークを構築したクライアントの該アクセス権保有ユーザの識別情報、及び自クライアントのユーザから受け付けたアクセス要求を該アクセス合意部に送信するアクセス要求部とを備え、

該アクセス合意部が、該識別情報の該アクセス権保有ユーザを、該データに対するアクセスに合意している該アクセス権保有ユーザとして該アクティブユーザデータベースに登録することを特徴としたアクセス権管理システム。

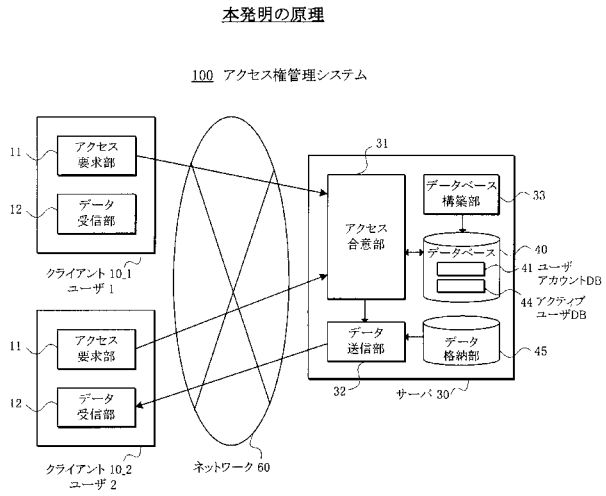
（付記４）上記の付記１において、
　各クライアントが、該ユーザアカウントデータベース、該アクティブユーザデータベース、及び該アクセス合意部の他に、さらにネットワーク構築部及びアクセス要求部を備え、
　該ネットワーク構築部が、他のクライアントとの間でネットワークを構築し、
　該アクセス合意部は、該構築されたネットワークに接続されているクライアントのアクセス権保有ユーザを、該データに対するアクセスに合意している該アクセス権保有ユーザとして該アクティブユーザデータベースに登録し、
　該アクセス要求部が、該データを保持するクライアントの該アクセス合意部に、自クライアントのユーザから受け付けたアクセス要求を与えることを特徴としたアクセス権管理システム。
（付記５）上記の付記４において、
　各クライアントが、データベース構築部をさらに有し、
　該データベース構築部が、該ユーザアカウントデータベースに、該データに対してアクセス権を保有する複数のユーザを関連付けて登録又は削除することを特徴としたアクセス権管理システム。
（付記６）上記の付記２又は３において、
　該サーバが、該データを保持していることを特徴としたアクセス権管理システム。
（付記７）上記の付記２又は３において、
　該クライアントが、該データを分散して保持するデータ格納部と、該データを他のクライアントとの間で送受信するためのデータ送信部及びデータ受信部と、をさらに備えたことを特徴としたアクセス権管理システム。
（付記８）上記の付記１乃至３において、
　該ユーザアカウントデータベースに該データに対してアクセス権を保有する複数のユーザを関連付けて登録又は削除するデータベース構築部をさらに備えたことを特徴とするアクセス権管理システム。
（付記９）
　データに対してアクセス権を保有する複数のユーザを関連付けて登録する第１ステップと、
　該アクセス権保有ユーザの内、現在、該データに対するアクセスに合意しているユーザを登録する第２ステップと、
　該合意しているアクセス権保有ユーザの現在数が複数であるときのみ、該データに対してアクセス要求して来た該アクセス権を保有するユーザに該データへのアクセスを合意する第３ステップと、
　を有することを特徴したアクセス権管理方法。
【図面の簡単な説明】
【０２１７】
【図１】本発明に係るアクセス権管理システム及びアクセス権管理方法の原理を示したブロック図である。
【図２】本発明に係るアクセス権管理システムの実施例(1)におけるシステム構成を示したブロック図である。
【図３】本発明に係るアクセス権管理システムの実施例(1)におけるユーザアカウントデータベースを示した図である。
【図４】本発明に係るアクセス権管理システムの実施例(1)におけるアクティブユーザデータベースを示した図である。
【図５】本発明に係るアクセス権管理システムの実施例(1)における動作手順を示したフローチャート図である。
【図６】本発明に係るアクセス権管理システムの実施例(2)におけるシステム構成を示したブロック図である。
【図７】一般的なアドホックネットワーク構築部が保持するテーブル例を示したブロック

図である。
【図８】本発明に係るアクセス権管理システムの実施例(2)におけるユーザアカウントデータベースを示した図である。
【図９】本発明に係るアクセス権管理システムの実施例(2)におけるアクティブユーザデータベースを示した図である。
【図１０】本発明に係るアクセス権管理システムの実施例(2)における動作手順を示したフローチャート図である。
【図１１】本発明に係るアクセス権管理システムの実施例(3)におけるシステム構成を示したブロック図である。
【図１２】本発明に係るアクセス権管理システムの実施例(3)におけるユーザアカウントデータベースを示した図である。
【図１３】本発明に係るアクセス権管理システムの実施例(3)におけるアクティブユーザデータベースを示した図である。
【図１４】本発明に係るアクセス権管理システムの実施例(3)における文書ファイルデータベースを示した図である。
【図１５】本発明に係るアクセス権管理システムの実施例(3)における動作手順を示しフローチャート図である。
【図１６】本発明に係るアクセス権管理システムの実施例(4)におけるシステム構成を示したブロック図である。
【図１７】本発明に係るアクセス権管理システムの実施例(4)：「文書に対するアクセス権の合意」におけるユーザアカウントデータベースを示した図である。
【図１８】本発明に係るアクセス権管理システムの実施例(4)：「文書に対するアクセス権の合意」におけるアクティブユーザデータベースを示した図である。
【図１９】本発明に係るアクセス権管理システムの実施例(4)：「文書に対するアクセス権の合意」における文書ファイルデータベースを示した図である。
【図２０】本発明に係るアクセス権管理システムの実施例(4)：「文書に対するアクセス権の合意」における動作手順を示したフローチャート図である。
【図２１】本発明に係るアクセス権管理システムの実施例(4)：「データベース構築部分散時のアクセス権管理」におけるユーザアカウントデータベースを示した図である。
【図２２】本発明に係るアクセス権管理システムの実施例(4)：「データベース構築部分散時のアクセス権管理」における文書ファイルデータベースを示した図である。
【図２３】本発明に係るアクセス権管理システムの実施例(4)：「データベース構築部分散時のアクセス権管理」の動作手順を示したシーケンス図である。
【図２４】従来のアクセス権管理システムを示したブロック図である。
【符号の説明】
【０２１８】
100，100w～100z　アクセス権管理システム　　1～5　ユーザ
10，10_1～10_3，10a，10a_1～10a_3　クライアント(ユーザ端末)
11　アクセス要求部　　12　データ受信部
13　位置情報受信部　　14，14_1～14_3　アドホックネットワーク構築部
14f，14f_1，14f_2　論理インタフェース
15　データ送信部　　16　データ受信部　　17　アクセス要求部
18　アクセス合意部　　19，19_1～19_3　データベース構築部
20z，20z_1，20z_2　データベース
21z，21z_1～21z_3　ユーザアカウントデータベース
22z，22z_1，22z_2　グループデータベース
23z，23z_1～23z_3　文書ファイルアクセス権管理データベース
24z，24z_1，24z_2　アクティブユーザデータベース
25，25_1，25_2　データ格納部
26y，26y_1，26y_2，26z，26z_1～26z_3　文書ファイルデータベース

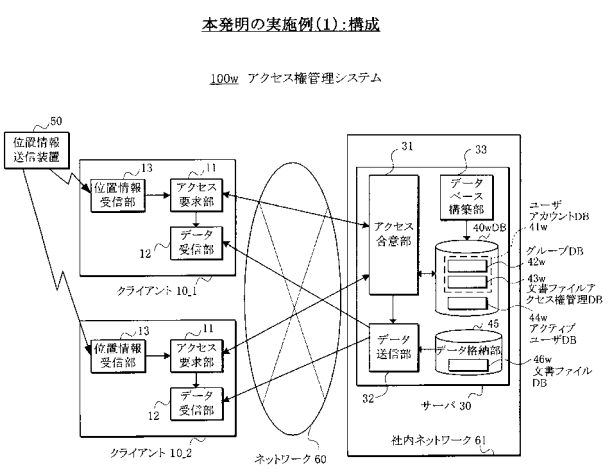
27_1, 27_2 ARPテーブル 28_1, 28_2 論理IFの属性テーブル
30 サーバ 31 アクセス合意部 32 データ送信部
33 データベース構築部 40, 40w, 40y データベース
41, 41w～41y ユーザアカウントデータベース
42w～42y グループデータベース
43w～43y 文書ファイルアクセス権管理データベース
44, 44w～44y アクティブユーザデータベース
45 データ格納部 46 文書ファイルデータベース
50 位置情報送信装置 60 ネットワーク 60a コネクション
60b コネクション 61 社内ネットワーク 62 アドホックネットワーク
62a コネクション 70 管理サーバ 81 文書管理DB
82 鍵管理DB 83 ユーザ管理DB 84 ユーザ操作管理DB
700_1～700_4 位置情報 701_1～701_4 現在位置 710 接続のネゴシエーション
711a ユーザID 711b パスワード 712 ユーザ認証結果
712a 認証OK 712b 認証NG 713a ユーザID
713b 位置情報 714 アクセス要求 715 判定結果
715a 合意 715b 未合意 716 データファイル
717 切断のネゴシエーション 718 受信準備指示
719 送信指示 720 登録/削除 721, 722, 724 参照
723 登録/更新/削除 725 削除
730_1, 730_2 アドホックネットワーク接続/切断依頼
731_1, 731_2 接続依頼可否 740 接続ネゴシエーション
741a ユーザID 741b パスワード 742 ユーザ認証結果
742a 認証OK 742b 認証NG
743 アドホックネットワーク接続ユーザ認証依頼
744 アドホックネットワーク接続ユーザ認証結果
745 アクセス要求 745a ユーザID 745b ファイル名
746 判定結果 746a 合意 746b 未合意
747 データファイル 748 切断のネゴシエーション
749 受信準備指示 750 送信指示 751 登録/削除
752～754, 756 参照 755 登録/更新 758 削除
760_1, 760_2 アドホックネットワーク接続/切断依頼
761_1, 761_2 接続依頼可否
762a_1, 762a_2 暗号化分割文書ファイル 762b_1, 762b_2 分割鍵
770 接続のネゴシエーション 771a ユーザID
771b パスワード 772 ユーザ認証結果 772a 認証OK
772b 認証NG 773 アドホックネットワーク接続/切断依頼
774 ユーザ認証結果 775 アクセス要求 776 判定結果
776a 合意 776b 未合意 777, 777_1, 777_2 送信指示
778 切断のネゴシエーション 779 受信準備指示
780 登録/削除 781～783, 785 参照 784 登録/更新
786 削除 790 アドホックネットワーク接続/切断依頼
790 アドホックネットワーク接続依頼 791 ユーザ認証依頼
792 ユーザ認証結果 793 接続依頼応答 794 ユーザ認証依頼
795 ユーザ認証結果 796 アクセス要求 797 判定結果
797a 合意 797b 未合意 798a 暗号化分割文書ファイル
798b 分割鍵 801, 802, 804 参照 803 登録
805a 送信指示 805b 受信準備指示 806a 暗号化分割文書ファイル
806b 分割鍵 807 送信指示 811, 812, 814 参照
813 登録 820, 821 文書検索

822a，822b，823a，823b，826　参照
824，825　文書検索応答　827_1，827_2　アクセス権許可要求
829a　暗号化分割文書ファイル　829b　分割鍵
830　アクセス権許可要求結果　831a　暗号化分割文書ファイル
831b　分割鍵　832　アクセス権許可要求結果
833～836　新分割情報　837～840　更新　900　編集要求
901　編集許可
図中、同一符号は同一又は相当部分を示す。

【図１】



【図２】



【図３】

ユーザアカウントデータベース 41w

(1)グループデータベース 42w

グループ ID (42wa)	ユーザ ID (42wb)	パスワード (42wc)
グループ A	ユーザ 1	パスワード P1
	ユーザ 2	パスワード P2
	ユーザ 3	パスワード P3
グループ B	ユーザ 3	パスワード P3
	ユーザ 4	パスワード P4
	ユーザ 5	パスワード P5

(2)文書ファイルアクセス権管理データベース 43w

データ (43wa)	アクセス可能とする位置情報 (43wb)	グループ ID／ユーザ ID (43wc)
文書ファイル 0	○県△町1－1 ◎県▽町1－2	グループ A
文書ファイル 1	×県△町3－1	グループ B ユーザ 1

【図４】

アクティブユーザデータベース 44w

(1)ユーザ 1 のみがクライアント 10_1 を起動している場合

44w

データ (44wa)	ユーザ ID (44wb)	現在位置 (44wc)
文書ファイル 0	ユーザ 1	○県△町1－1

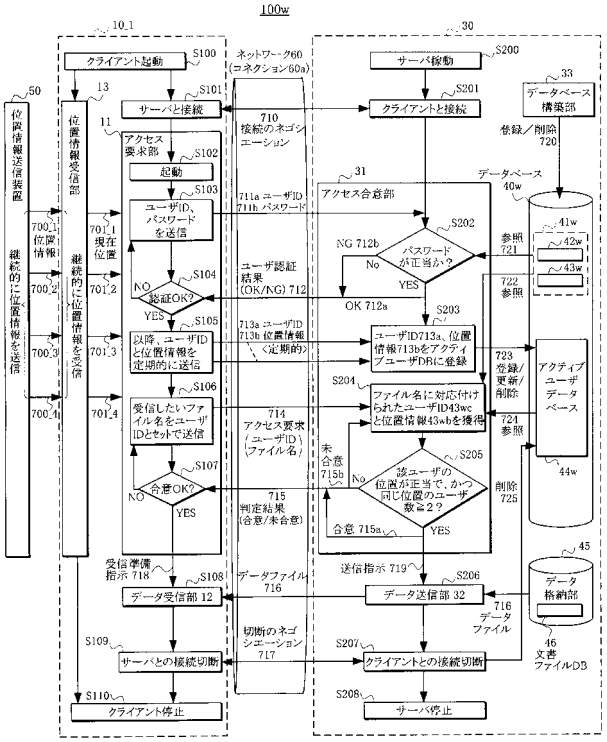
(2)ユーザ 1、2 がそれぞれクライアント 10_1,10_2 を起動している場合

44w

データ (44wa)	ユーザ ID (44wb)	現在位置 (44wc)
文書ファイル 0	ユーザ 1	○県△町1－1
	ユーザ 2	○県△町1－1

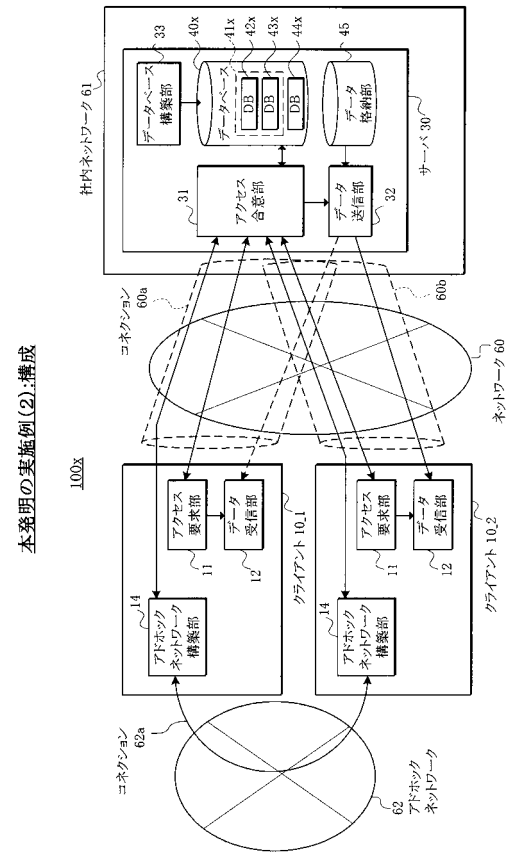
【図５】

本発明の実施例(1):動作手順



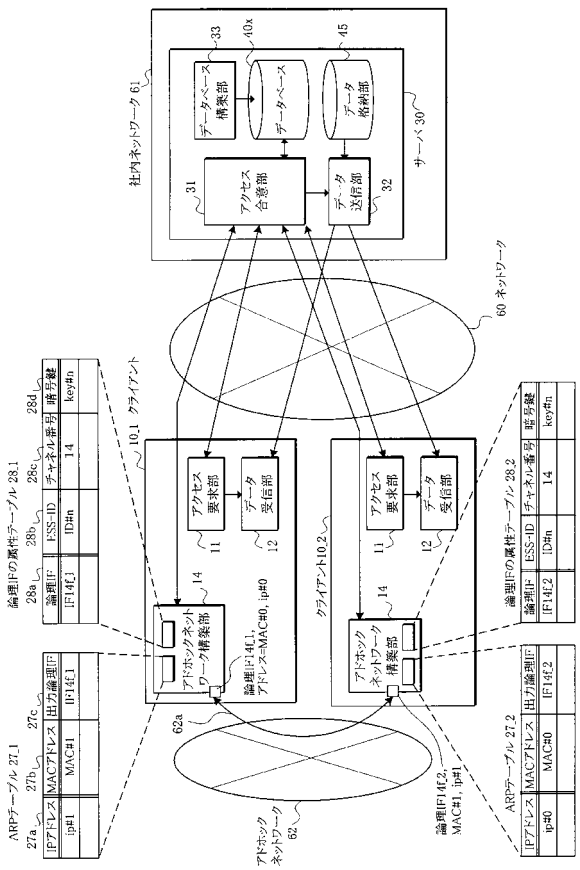
【図６】

本発明の実施例(2):構成



【図７】

一般的なアドホックネットワーク構築部におけるテーブル例



【図８】

ユーザアカウントデータベース 42x

(1)グループデータベース 42x

グループ ID (42xa)	ユーザ ID (42xb)	パスワード (42xc)
グループ A	ユーザ 1	パスワード P1
	ユーザ 2	パスワード P2
	ユーザ 3	パスワード P3
グループ B	ユーザ 3	パスワード P3
	ユーザ 4	パスワード P4
	ユーザ 5	パスワード P5

(2)文書ファイルアクセス権管理データベース 43x

データ (43xa)	グループ ID／ユーザ ID (43xb)
文書ファイル 0	グループ A
文書ファイル 1	グループ B
	ユーザ 1

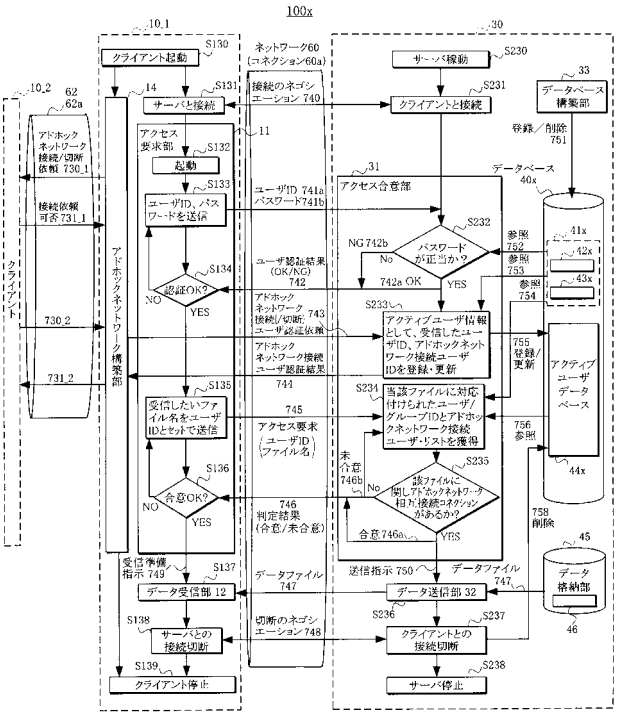
【図９】

アクティブユーザデータベース 44x

ユーザ ID (44xa)	アドホックネットワーク接続ユーザ ID リスト (44xb)
ユーザ 1	ユーザ 2
ユーザ 2	ユーザ 1
ユーザ 3	ユーザ 4, ユーザ 5
ユーザ 4	ユーザ 2, ユーザ 5
ユーザ 5	ユーザ 2, ユーザ 4

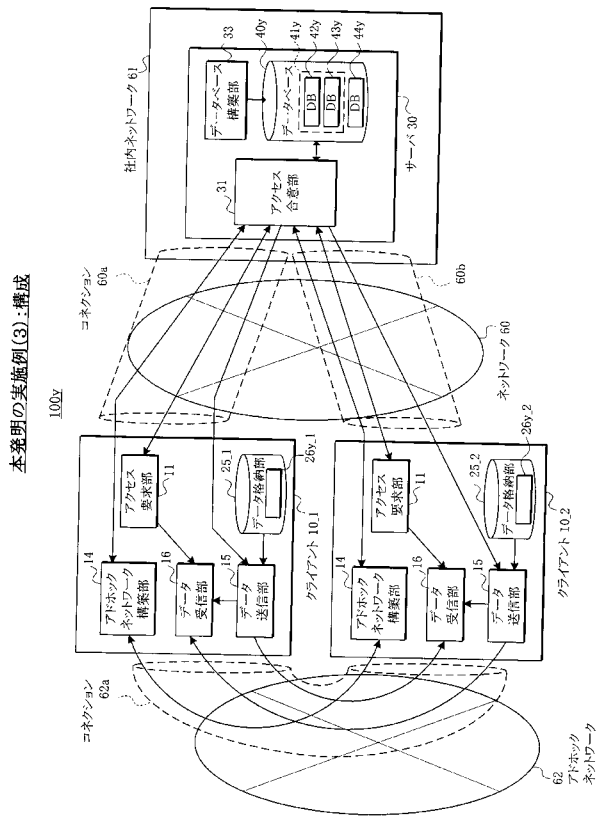
【図１０】

本発明の実施例(2):動作手順



【図１１】

本発明の実施例(3):構成



【図１２】

ユーザアカウントデータベース 41y

(1)グループデータベース 42y

グループ ID (42ya)	ユーザ ID (42yb)	パスワード (42yc)
グループ A	ユーザ 1	パスワード P1
	ユーザ 2	パスワード P2
	ユーザ 3	パスワード P3
グループ B	ユーザ 3	パスワード P3
	ユーザ 4	パスワード P4
	ユーザ 5	パスワード P5

(2)文書ファイルアクセス権管理データベース 43y

データ (43ya)	グループ ID／ユーザ ID (43yb)
文書ファイル 0	ユーザ 1
	ユーザ 2
文書ファイル 1	グループ B
	ユーザ 1

【図１３】

アクティブユーザデータベース 44y

ユーザ ID (44ya)	アドホックネットワーク接続ユーザ ID リスト (44yb)
ユーザ 1	ユーザ 2
ユーザ 2	ユーザ 1
ユーザ 3	ユーザ 4, ユーザ 5
ユーザ 4	ユーザ 3, ユーザ 5
ユーザ 5	ユーザ 3, ユーザ 4

【図１４】

文書ファイルデータベース 26y

(1) クライアント 10_1 のデータベース 26y_1

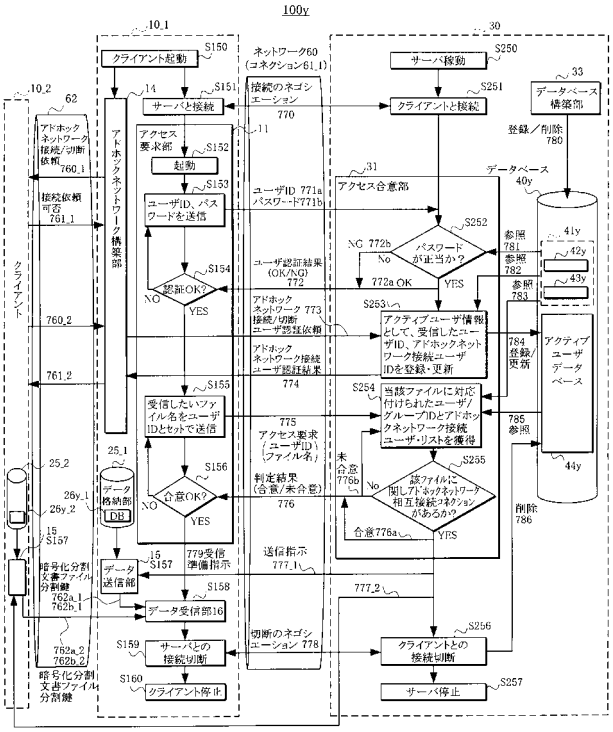
データ名 (26ya)	データ内容 (26yb)	鍵 (26yc)
文書ファイル 0	暗号化分割文書ファイル 0-0	分割鍵 0-0
文書ファイル 1	暗号化分割文書ファイル 1-0	分割鍵 1-0

(2) クライアント 10_2 のデータベース 26y_2

データ名 (26ya)	データ内容 (26yb)	鍵 (26yc)
文書ファイル 0	暗号化分割文書ファイル 0-1	分割鍵 0-1

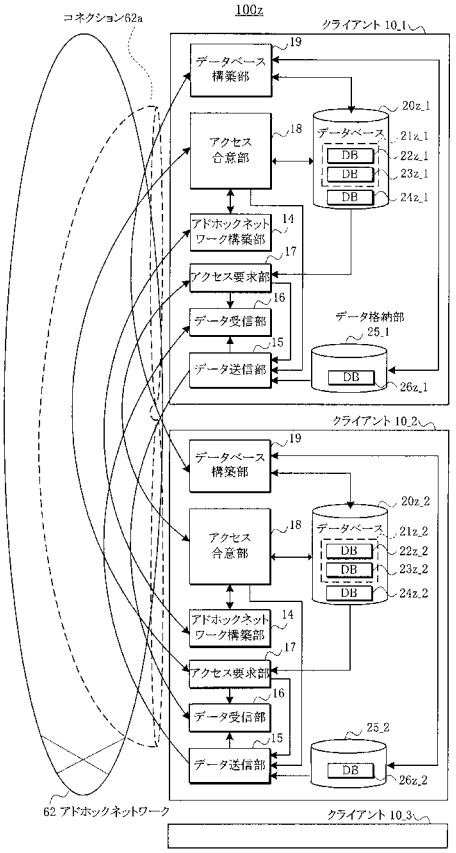
【図１５】

本発明の実施例(3):動作手順



【図１６】

本発明の実施例(4):構成



【図１７】

ユーザアカウントデータベース 21z

(1)クライアント 10_1,10_2 のグループデータベース 22z_1, 22z_2

グループ ID (22za)	ユーザ ID (22zb)	パスワード (22zc)
グループ A	ユーザ 1	パスワード P1
	ユーザ 2	パスワード P2
	ユーザ 3	パスワード P3
グループ B	ユーザ 3	パスワード P3
	ユーザ 4	パスワード P4
	ユーザ 5	パスワード P5

(2)クライアント 10_1 の文書ファイルアクセス権管理データベース 23z_1

データ (23za)	グループ ID／ユーザ ID (23zb)
文書ファイル 0	ユーザ 1
	ユーザ 2
文書ファイル 1	グループ B
	ユーザ 1

(3)クライアント 10_2 の文書ファイルアクセス権管理データベース 23z_2

データ (23za)	グループ ID／ユーザ ID (23zb)
文書ファイル 0	ユーザ 1
	ユーザ 2

【図１８】

アクティブユーザデータベース 24z

(1) クライアント 10_1 のデータベース 24z_1

アドホックネットワーク接続ユーザ ID リスト
ユーザ 2

(2) クライアント 10_2 のデータベース 24z_2

アドホックネットワーク接続ユーザ ID リスト
ユーザ 1

【図１９】

文書ファイルデータベース 26z

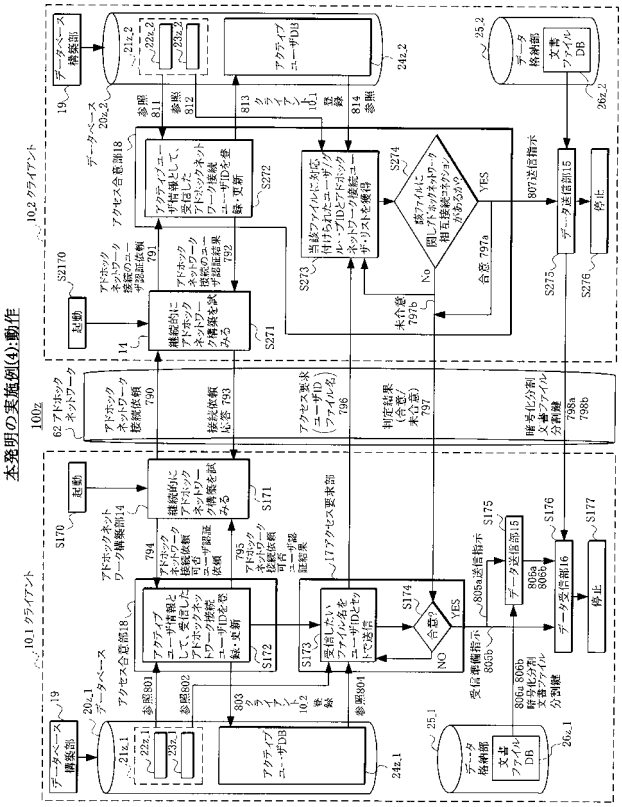
(1) クライアント 10_1 のデータベース 26z_1

26za データ名	26zb データ内容	26zc 鍵
文書ファイル 0	暗号化分割文書ファイル 0-0	分割鍵 0-0
文書ファイル 1	暗号化分割文書ファイル 1-0	分割鍵 1-0

(2) クライアント 10_2 のデータベース 26z_2

26za データ名	26zb データ内容	26zc 鍵
文書ファイル 0	暗号化分割文書ファイル 0-1	分割鍵 0-1

【図２０】



【図２１】

ユーザアカウントデータベース 21z

(1) 全クライアントのグループデータベース 22z_1,22z_2,22z_3

22za グループ ID	22zb ユーザ ID	22zc パスワード
グループ A	ユーザ 1	パスワード P1
	ユーザ 2	パスワード P2
	ユーザ 3	パスワード P3
グループ B	ユーザ 3	パスワード P3
	ユーザ 4	パスワード P4
	ユーザ 5	パスワード P5

(2) クライアント 10_1 の文書ファイルアクセス権管理データベース 23z_1

(2a)

23za データ	23zb グループ ID／ユーザ ID
文書ファイル 0	ユーザ 1
	ユーザ 2
文書ファイル 1	グループ B
	ユーザ 1

⇨

(2b)

データ	グループ ID／ユーザ ID
文書ファイル 0	ユーザ 1
	ユーザ 2
	ユーザ 3
文書ファイル 1	グループ B
	ユーザ 1

(3) クライアント 10_2 の文書ファイルアクセス権管理データベース 23z_2

(3a)

23za データ	23zb グループ ID／ユーザ ID
文書ファイル 0	ユーザ 1
	ユーザ 2

⇨

(3b)

データ	グループ ID／ユーザ ID
文書ファイル 0	ユーザ 1
	ユーザ 2
	ユーザ 3

(4) クライアント 10_3 の文書ファイルアクセス権管理データベース 23z_3

(4a)

23za データ	23zb グループ ID／ユーザ ID
文書ファイル 1	グループ B
	ユーザ 1

⇨

(4b)

データ	グループ ID／ユーザ ID
文書ファイル 0	ユーザ 1
	ユーザ 2
	ユーザ 3
文書ファイル 1	グループ B
	ユーザ 1

【図２２】

文書ファイルデータベース 26z

(1) クライアント 10_1 のデータベース 26z_1

(1a)

26za データ名	26zb データ内容	26zc 鍵
文書ファイル 0	暗号化分割文書ファイル 0-0	分割鍵 0-0
文書ファイル 1	暗号化分割文書ファイル 1-0	分割鍵 1-0

⇩

(1b)

データ名	データ内容	鍵
文書ファイル 0	新暗号化分割文書ファイル 0-0	新分割鍵 0-0
文書ファイル 1	暗号化分割文書ファイル 1-0	分割鍵 1-0

(2) クライアント 10_2 のデータベース 26z_2

(2a)

データ名	データ内容	鍵
文書ファイル 0	暗号化分割文書ファイル 0-1	分割鍵 0-1

⇩

(2b)

データ名	データ内容	鍵
文書ファイル 0	新暗号化分割文書ファイル 0-1	新分割鍵 0-1

(3) クライアント 10_3 のデータベース 26z_3

(3a)

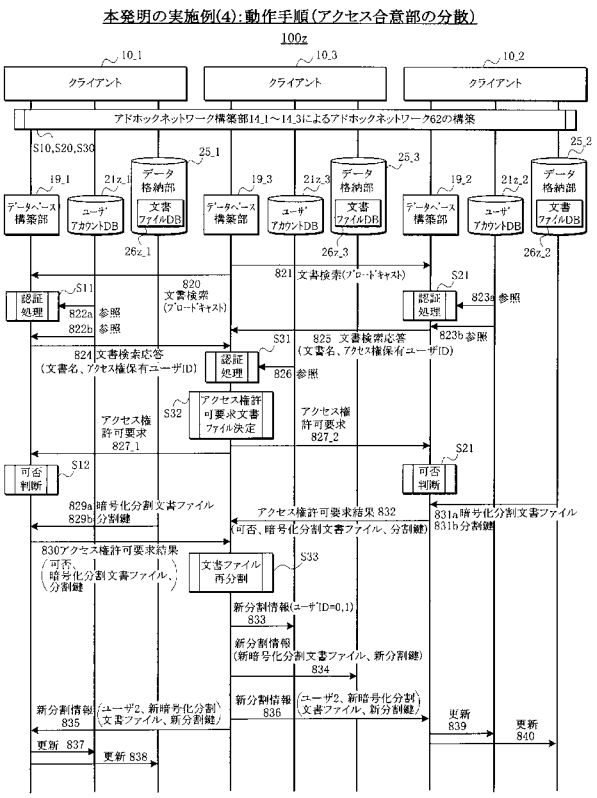
データ名	データ内容	鍵
文書ファイル 1	暗号化分割文書ファイル 1-2	分割鍵 1-2

⇩

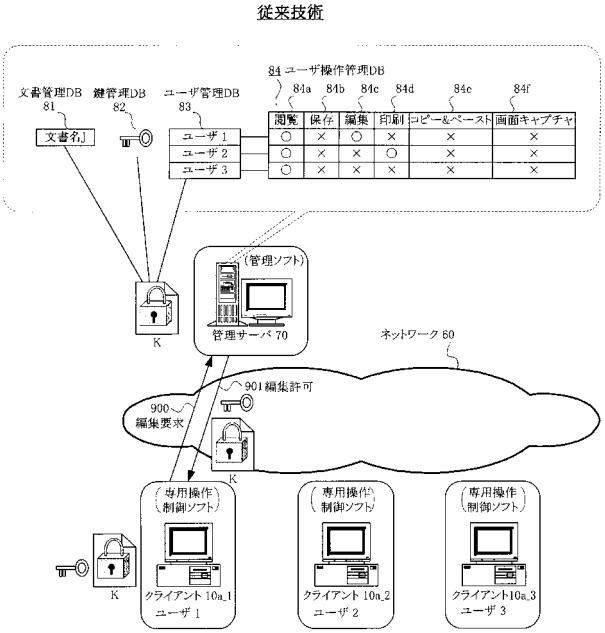
(3b)

データ名	データ内容	鍵
文書ファイル 0	新暗号化分割文書ファイル 0-2	新分割鍵 0-2
文書ファイル 1	暗号化分割文書ファイル 1-2	分割鍵 1-2

【図２３】


本発明の実施例(4):動作手順(アクセス合意部の分散)
100z
10_1
10_3
10_2
クライアント
クライアント
クライアント
アドホックネットワーク構築部14_1～14_3によるアドホックネットワーク62の構築
S10,S20,S30
25_1
25_3
25_2
データ格納部
データベース構築部
ユーザアカウントDB
文書ファイルDB
19_1
21z_1
26z_1
19_3
21z_3
26z_3
19_2
21z_2
26z_2
821 文書検索(ブロードキャスト)
S11
S21
認証処理
820 文書検索(ブロードキャスト)
822a 参照
822b 参照
823a 参照
823b 参照
824 文書検索応答(文書名、アクセス権保有ユーザID)
S31
825 文書検索応答(文書名、アクセス権保有ユーザID)
826 参照
S32
アクセス権許可要求文書ファイル決定
アクセス権許可要求 827_1
アクセス権許可要求 827_2
S12
可否判断
829a 暗号化分割文書ファイル
829b 分割鍵
アクセス権許可要求結果 832
(可否、暗号化分割文書ファイル、分割鍵)
831a 暗号化分割文書ファイル
831b 分割鍵
830 アクセス権許可要求結果(可否、暗号化分割文書ファイル、分割鍵)
S33
文書ファイル再分割
新分割情報(ユーザID=0,1) 833
新分割情報(新暗号化分割文書ファイル、新分割鍵) 834
新分割情報 835
(ユーザ2、新暗号化分割文書ファイル、新分割鍵)
新分割情報 836
(ユーザ2、新暗号化分割文書ファイル、新分割鍵)
更新 837
更新 838
更新 839
更新 840

【図２４】


従来技術
84 ユーザ操作管理DB
文書管理DB 81
鍵管理DB 82
ユーザ管理DB 83
84a
84b
84c
84d
84e
84f
閲覧
保存
編集
印刷
コピー&ペースト
画面キャプチャ
文書名
ユーザ 1
ユーザ 2
ユーザ 3
(管理ソフト)
管理サーバ 70
ネットワーク 60
901 編集許可
900 編集要求
K
専用操作制御ソフト
クライアント 10a_1
ユーザ 1
クライアント 10a_2
ユーザ 2
クライアント 10a_3
ユーザ 3