(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2007-272583
(P2007-272583A)
(43)公開日　平成19年10月18日(2007.10.18)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330A	5B285
H04L 9/32	(2006.01)	H04L	9/00	673A	5J104

審査請求 未請求　請求項の数 13　ＯＬ　（全 42 頁）

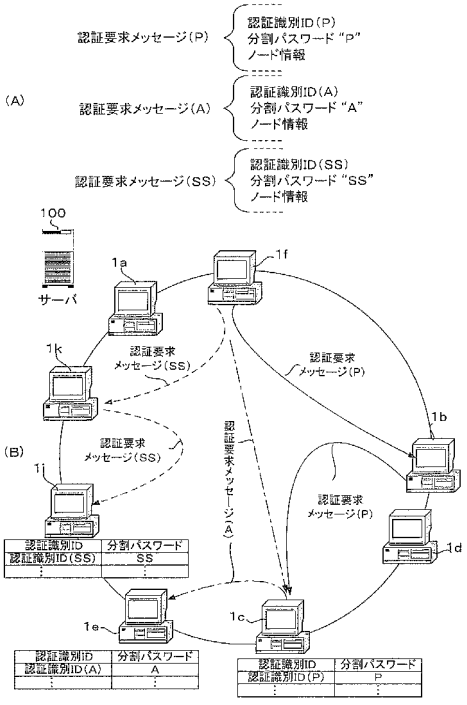
(21)出願番号　特願2006-97703(P2006-97703)
(22)出願日　平成18年3月31日(2006.3.31)

(71)出願人　899000068
学校法人早稲田大学
東京都新宿区戸塚町１丁目１０４番地
(71)出願人　000005267
ブラザー工業株式会社
愛知県名古屋市瑞穂区苗代町１５番１号
(71)出願人　396004833
株式会社エクシング
愛知県名古屋市瑞穂区塩入町１８番１号
(74)代理人　100083839
弁理士　石川　泰男
(74)代理人　100109139
弁理士　今井　孝弘
(74)代理人　100120189
弁理士　奥　和幸

最終頁に続く

(54)【発明の名称】情報共有システム、情報共有システムにおける認証方法、管理装置及び情報処理装置等

(57)【要約】
【課題】認証用サーバ等を用いずに、複数のノード装置間で認証処理を行なうことができる情報共有システム等を提供することを課題とする。
【解決手段】本発明は、ネットワークを介して互いに通信可能な複数の情報処理装置を備えた情報共有システムに含まれるユーザによる操作の制限がなされた前記情報処理装置において、ユーザによる操作を許可するためのパスワードを、分割して複数の分割パスワードを生成する手段と、各分割パスワードに対応する固有の識別情報に基づいて各分割パスワードの認証処理を行なう情報処理装置を夫々特定し、特定された各情報処理装置から正当である旨の認証結果を取得した場合には、前記情報処理装置の操作制限を解除して、ユーザの情報処理装置の操作を許可する手段と、を有することを特徴とする。
【選択図】図８



【特許請求の範囲】
【請求項１】
ネットワークを介して互いに通信可能な複数の情報処理装置を備え、当該複数の情報処理装置によって共用される複数の共用情報が複数の情報処理装置に分散されて保存されている情報共有システムであって、該システムを利用する複数のユーザの管理を行なう管理装置を含む前記情報共有システムにおいて、
前記管理装置は、
前記ユーザによる前記情報処理装置の操作を許可するためのパスワードを、文字数や分割数等が決められた所定の分割手法で分割して複数の分割パスワードを生成する第１分割パスワード生成手段と、
前記ユーザを識別するための固有のユーザ情報と、各前記分割パスワードと、に対応する固有の識別情報を生成する第１識別情報生成手段と、
前記複数の情報処理装置のうち、前記識別情報に基づいて前記各分割パスワードの認証処理を行なうべき情報処理装置を夫々特定し、特定された前記各情報処理装置に認証処理担当となることを要求する認証処理担当要求手段と、を有し、
各前記情報処理装置は、
前記管理装置によって、前記識別情報に基づいて前記分割パスワードの前記認証処理を行なうべき情報処理装置として特定され、認証処理担当となることを要求された場合には、当該識別情報及び前記分割パスワードを取得して、夫々対応付けて記憶する記憶手段を有し、
前記ユーザによる操作の制限がなされた前記情報処理装置は、
前記ユーザが前記パスワードと、前記ユーザ情報を入力する入力手段と、
前記入力されたパスワードを、文字数や分割数等が決められた所定の分割手法で分割して前記複数の分割パスワードを生成する第２分割パスワード生成手段と、
前記ユーザ情報と、前記各分割パスワードと、に対応する前記識別情報を夫々生成する第２識別情報生成手段と、
前記複数の情報処理装置のうち、前記識別情報に基づいて前記各分割パスワードの認証処理を行なう情報処理装置を夫々特定し、特定された前記各情報処理装置に、夫々の前記識別情報と、当該識別情報に対応する前記分割パスワードを夫々送信して、該各情報処理装置から前記分割パスワードの認証結果を夫々取得する認証結果取得手段と、
前記第２分割パスワード生成手段にて生成した全ての前記分割パスワードについて、正当である旨の認証結果を取得した場合には、前記情報処理装置の操作制限を解除して、前記ユーザの前記情報処理装置の操作を許可する操作許可手段と、を有し、
何れかの前記情報処理装置から前記分割パスワード及び前記識別情報を受信して、認証要求がされた前記情報処理装置は、
受信した前記識別情報が前記記憶手段に記憶されている場合には、当該識別情報に対応付けて前記記憶手段に記憶された前記分割パスワードが、受信した前記分割パスワードと一致するか否かに基づいて、受信した前記分割パスワードの認証を行なう認証手段と、
前記認証手段による認証結果を前記分割パスワード及び前記識別情報の送信元の情報処理装置へ送信する認証結果送信手段と、
を有することを特徴とする情報共用システム。
【請求項２】
ネットワークを介して互いに通信可能な複数の情報処理装置を備え、当該複数の情報処理装置によって共用される複数の共用情報が複数の情報処理装置に分散されて保存されている情報共有システムであって、該システムを利用する複数のユーザの管理を行なう管理装置を含む前記情報共有システムにおける認証方法において、
前記管理装置が、前記ユーザによる前記情報処理装置の操作を許可するためのパスワードを、文字数や分割数等が決められた所定の分割手法で分割して複数の分割パスワードを生成する工程と、
前記管理装置が、前記ユーザを識別するための固有のユーザ情報と、各前記分割パスワ

ードと、に対応する固有の識別情報を生成する工程と、
前記管理装置が、前記複数の情報処理装置のうち、前記識別情報に基づいて前記各分割パスワードの認証処理を行なうべき情報処理装置を夫々特定し、特定された前記各情報処理装置に認証処理担当となることを要求する工程と、
前記管理装置によって、前記識別情報に基づいて前記分割パスワードの前記認証処理を行なうべき情報処理装置として特定され、認証処理担当となることを要求された各前記情報処理装置が、当該識別情報及び前記分割パスワードを取得して、夫々対応付けて記憶手段に記憶する工程と、
ユーザによる操作の制限がなされた前記情報処理装置が、
前記ユーザが前記パスワードと、前記ユーザ情報を入力する工程と、
前記入力されたパスワードを、文字数や分割数等が決められた所定の分割手法で分割して前記複数の分割パスワードを生成する分割パスワード生成工程と、
前記ユーザ情報と、前記各分割パスワードと、に対応する前記識別情報を夫々生成する工程と、
前記複数の情報処理装置のうち、前記識別情報に基づいて前記各分割パスワードの認証処理を行なう情報処理装置を夫々特定し、特定された前記各情報処理装置に、夫々の前記識別情報と、当該識別情報に対応する前記分割パスワードを夫々送信する工程と、
何れかの前記情報処理装置から前記分割パスワード及び前記識別情報を受信して、認証要求がされた前記情報処理装置が、受信した前記識別情報が前記記憶手段に記憶されている場合には、前記記憶手段に当該識別情報に対応付けて記憶された前記分割パスワードが、受信した前記分割パスワードと一致するか否かに基づいて、受信した前記分割パスワードの認証を行ない、当該認証結果を前記分割パスワード及び前記識別情報の送信元の情報処理装置へ送信する工程と、
前記ユーザによって操作される前記情報処理装置が、前記分割パスワードの認証結果を夫々取得し、かつ、前記分割パスワード生成工程にて生成した全ての前記分割パスワードについて、正当である旨の認証結果を取得した場合には、前記情報処理装置の操作制限を解除して、前記ユーザの前記情報処理装置の操作を許可する工程と、
を有することを特徴とする情報共有システムにおける認証方法。
【請求項３】
ネットワークを介して互いに通信可能な複数の情報処理装置を備え、当該複数の情報処理装置によって共用される複数の共用情報が複数の情報処理装置に分散されて保存されている情報共有システムであって、該システムを利用する複数のユーザの管理を行なう管理装置において、
前記ユーザによる前記情報処理装置の操作を許可するためのパスワードを、文字数や分割数等が決められた所定の分割手法で分割して複数の分割パスワードを生成する第１分割パスワード生成手段と、
前記ユーザを識別するための固有のユーザ情報と、各前記分割パスワードに基づいて、前記各分割パスワードに対応する固有の識別情報を生成する第１識別情報生成手段と、
前記複数の情報処理装置のうち、前記識別情報に基づいて前記各分割パスワードの認証処理を行なうべき情報処理装置を夫々特定し、特定された前記各情報処理装置に認証処理担当となることを要求する認証処理担当要求手段と、
を有することを特徴とする管理装置。
【請求項４】
請求項３に記載の管理装置において、
前記第１識別情報生成手段は、前記分割パスワード当たり所定数の前記識別情報を生成することを特徴とする管理装置。
【請求項５】
請求項３又は４に記載の管理装置において、
前記ユーザ情報と、前記パスワードと、を夫々対応付けて記憶する記憶手段を有し、
何れかの前記情報処理装置から前記パスワード及び前記ユーザ情報を受信して、前記各

情報処理装置間で行なわれる認証ができないことに基づく認証処理要求を受け付ける認証処理受付手段と、
受信した前記ユーザ情報に対応付けて前記記憶手段に記憶された前記パスワードが、受信した前記パスワードと一致するか否かに基づいて、受信した前記パスワードの認証を行なう認証手段と、
前記認証手段による認証結果を前記パスワード及び前記ユーザ情報の送信元の情報処理装置へ送信する認証結果送信手段と、
を有することを特徴とする管理装置。
【請求項６】
請求項３乃至５のいずれか一項に記載の管理装置において、
前記認証手段は、何れかの前記情報処理装置から前記ユーザ情報、前記パスワード及び新しいパスワードを受信し、パスワードの変更処理要求がされると、前記受信した前記パスワードの認証を行ない、
前記パスワードにかかる認証結果が正当である場合には、
前記記憶手段は、前記ユーザ情報と、前記新しいパスワードと、を対応付けて記憶し、
前記第１分割パスワード生成手段は、前記パスワードにかかる認証結果が正当である場合には、前記受信した新しいパスワードを、前記所定の分割手法で分割して前記複数の分割パスワードを生成し、
前記第１識別情報生成手段は、前記ユーザ情報と、前記生成された分割パスワードに対応する前記識別情報を生成し、
前記認証処理担当要求手段は、前記複数の情報処理装置のうち、前記識別情報に基づいて前記各分割パスワードの認証処理を行なうべき情報処理装置を夫々特定し、特定された前記各情報処理装置に認証処理担当となることを要求することを特徴とする管理装置。
【請求項７】
コンピュータを、請求項３乃至６のいずれか一項に記載の管理装置として機能させることを特徴とする管理処理プログラム。
【請求項８】
ネットワークを介して互いに通信可能な複数の情報処理装置を備え、当該複数の情報処理装置によって共用される複数の共用情報が複数の情報処理装置に分散されて保存されている情報共有システムに含まれる前記情報処理装置であって、ユーザによる操作の制限がなされた前記情報処理装置において、
前記ユーザによる前記情報処理装置の操作を許可するためのパスワードと、前記ユーザを識別するための固有のユーザ情報と、を入力する入力手段と、
前記入力されたパスワードを、文字数や分割数等が決められた所定の分割手法で分割して複数の分割パスワードを生成する第２分割パスワード生成手段と、
前記ユーザ情報と、前記各分割パスワードに基づいて、前記各分割パスワードに対応する固有の識別情報を夫々生成する第２識別情報生成手段と、
前記複数の情報処理装置のうち、前記識別情報に基づいて前記各分割パスワードの認証処理を行なう情報処理装置を夫々特定し、特定された前記各情報処理装置に、夫々の前記識別情報と、当該識別情報に対応する前記分割パスワードを夫々送信して、該各情報処理装置から前記分割パスワードの認証結果を夫々取得する認証結果取得手段と、
前記第２分割パスワード生成手段にて生成した全ての前記分割パスワードについて、正当である旨の認証結果を取得した場合には、前記情報処理装置の操作制限を解除して、前記ユーザの前記情報処理装置の操作を許可する操作許可手段と、
を有することを特徴とする情報処理装置。
【請求項９】
請求項８に記載の情報処理装置において、
前記第２識別情報生成手段は、前記分割パスワード当たり所定数の前記識別情報を生成し、
前記認証結果取得手段は、前記分割パスワード毎に、前記所定数の識別情報に基づいて

特定された所定数台の前記各情報処理装置に、夫々の前記識別情報と、当該識別情報に対応する前記分割パスワードを夫々送信して、該各情報処理装置から前記分割パスワードの認証結果を夫々取得し、

前記第２分割パスワード生成手段にて生成した前記分割パスワードのうち、少なくとも一の前記分割パスワードについて、前記所定数のうち前記認証結果取得手段が認証結果を取得できなかった数が、有効閾値以下であるか否かを判定する判断有効判定手段を有し、

前記判定の結果、認証結果を取得できなかった数が、有効閾値以下であると判定された場合には、前記操作許可手段は、前記全ての分割パスワードについて、前記認証結果取得手段が取得した認証結果のうち、正当である旨の認証結果が、所定閾値以上である場合に、前記情報処理装置の操作制限を解除して、前記ユーザの前記情報処理装置の操作を許可することを特徴とする情報処理装置。

【請求項１０】

請求項９に記載の情報処理装置において、

前記所定閾値は、前記第２識別情報生成手段が生成する前記識別情報の前記所定数、前記第２識別情報生成手段が生成する前記識別情報の前記所定数の半数、又は、一の前記分割パスワードについて前記認証結果取得手段が取得した認証結果の数、又は、一の前記分割パスワードについて前記認証結果取得手段が取得した認証結果の半数、又は、１であることを特徴とする情報処理装置。

【請求項１１】

請求項９又は１０に記載の情報処理装置において、

前記情報共有システムは、該システムを利用する複数の前記ユーザについて、前記ユーザ情報と、当該ユーザ情報に対応する前記パスワードと、を夫々記憶する管理装置を含み、

前記判断有効判定手段の判定の結果、前記第２分割パスワード生成手段にて生成した前記分割パスワードのうち、少なくとも１の前記分割パスワードについて、前記所定数のうち前記認証結果取得手段が認証結果を取得できなかった数が、有効閾値以下でないと判定された場合には、前記認証結果取得手段は、前記管理装置に対して、前記パスワードと前記ユーザ情報を送信し、前記管理装置から前記パスワードの認証結果を取得し、

前記操作許可手段は、前記管理装置から、前記パスワードが正当である旨の認証結果を取得した場合には、前記情報処理装置の操作制限を解除して、前記ユーザの前記情報処理装置の操作を許可することを特徴とする情報処理装置。

【請求項１２】

請求項１１に記載の情報処理装置において、

前記管理装置に対して、前記ユーザ情報、前記パスワード及び新しいパスワードを送信し、前記パスワードの変更処理要求を行なうパスワード変更処理要求手段を有することを特徴とする情報処理装置。

【請求項１３】

コンピュータを、請求項８乃至１２のいずれか一項に記載の情報処理装置として機能させることを特徴とする情報処理プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

ネットワークを介して互いに通信可能な複数の情報処理装置を備えたピアツーピア（Peer to Peer（P2P））型の情報共有システムであって、少なくとも１以上の共用情報を複数の情報処理装置によって共用可能に保持させるための管理装置等に関する。

【背景技術】

【０００２】

近年、インターネット等のネットワークを介して上記コンテンツを蓄積しているサーバ等にノード装置からアクセスし、そのノード装置において視聴が所望されているコンテンツを当該ノード装置に配信して視聴する、いわゆるコンテンツ配信を行なう情報配信シス

テムについての研究開発が盛んである。
【０００３】
そして、当該情報配信システムの一つとして、ネットワークに属するノード装置間で、当該コンテンツが相互に直接授受される情報共有システム、例えば、各コンテンツを複数のノード装置間で分散して複数のノード装置で共用させるＰ２Ｐ型の情報共有システムがある。このＰ２Ｐ型の情報共有システムは、従来のクライアント・サーバ型のモデルの欠点である、サーバへのアクセス集中や、高い管理コストを解決する手法として注目されている。
【０００４】
また、この分野の研究では、Ｐ２Ｐ型の配信システムの一つとして、ピアツーピア型の情報共有システムにおいて、例えば、分散ハッシュテーブル（以下、ＤＨＴ（Distributed Hash Table）という）を利用して論理的に構築されたオーバーレイネットワークでは、各ノードが、当該オーバーレイネットワークに参加している全てのノード装置へのリンク情報（例えば、ＩＰアドレス）を認識しているわけではなく、参加の際などに得られる一部のノード装置へのリンク情報だけを所持しており、かかるリンク情報に基づき、データの問い合わせ等を行なうようになっている。
【０００５】
このようなオーバーレイネットワークにおいては、ノード装置の参加及び脱退（離脱）が頻繁に行われても、負荷分散が適切に行われる必要があり、非特許文献１には、オーバーレイネットワークにおいて、参加及び脱退（離脱）が頻繁に行われる場合であっても、適切に負荷分散を行なうための技術が開示されている。また、特許文献１、２にもＤＨＴに係る技術が開示されている。
【０００６】
また、従来よりノード装置を操作して各種サービスを提供するシステムを利用するため、ノード装置に予めパスワードを登録しておき、該パスワードを入力させ、該ノード装置で入力したパスワードの認証を行なうことで、システムを利用できる正規のユーザであるか否かを確認し、パスワードが正当であると認証された場合にだけ、ノード装置の操作制限を解除して、システムにログインできるという認証手法がある。
【非特許文献１】「分散ハッシュテーブルの軽量な負荷分散手法の検討」　社団法人　電子情報通信学会　信学技報
【特許文献１】特開２００３－９９３３７号公報
【特許文献２】特開２００３‐２１６５２１号公報
【発明の開示】
【発明が解決しようとする課題】
【０００７】
上記認証手法では、ユーザはパスワードを登録済みのノード装置からしか、システムを利用することができない。これに対処するために、認証用サーバにパスワードを登録しておき、ノード装置で入力されたパスワードをサーバに送信して認証を行なうという方法も考えられる。しかしこの方法では、複数のユーザがシステムにログインしようとする都度、各ノード装置から認証用サーバに過大な処理負担を課すこととなり、システムに参加するノード装置が増えるほどこの処理負担が増大し続けるという問題が生じる。
【０００８】
本発明は、以上の問題等に鑑みてなされたものであり、認証用サーバ等を用いずに、複数のノード装置間で認証処理を行なうことができる情報共有システム、情報共有システムにおける認証方法、管理装置及び情報処理装置等を提供することを課題とする。
【課題を解決するための手段】
【０００９】
上記課題を解決するため、請求項１に記載の発明は、ネットワークを介して互いに通信可能な複数の情報処理装置を備え、当該複数の情報処理装置によって共用される複数の共用情報が複数の情報処理装置に分散されて保存されている情報共有システムであって、該

システムを利用する複数のユーザの管理を行なう管理装置を含む前記情報共有システムにおいて、前記管理装置は、前記ユーザによる前記情報処理装置の操作を許可するためのパスワードを、文字数や分割数等が決められた所定の分割手法で分割して複数の分割パスワードを生成する第１分割パスワード生成手段と、前記ユーザを識別するための固有のユーザ情報と、各前記分割パスワードと、に対応する固有の識別情報を生成する第１識別情報生成手段と、前記複数の情報処理装置のうち、前記識別情報に基づいて前記各分割パスワードの認証処理を行なうべき情報処理装置を夫々特定し、特定された前記各情報処理装置に認証処理担当となることを要求する認証処理担当要求手段と、を有し、各前記情報処理装置は、前記管理装置によって、前記識別情報に基づいて前記分割パスワードの前記認証処理を行なうべき情報処理装置として特定され、認証処理担当となることを要求された場合には、当該識別情報及び前記分割パスワードを取得して、夫々対応付けて記憶する記憶手段を有し、前記ユーザによる操作の制限がなされた前記情報処理装置は、前記ユーザが前記パスワードと、前記ユーザ情報を入力する入力手段と、前記入力されたパスワードを、文字数や分割数等が決められた所定の分割手法で分割して前記複数の分割パスワードを生成する第２分割パスワード生成手段と、前記ユーザ情報と、前記各分割パスワードと、に対応する前記識別情報を夫々生成する第２識別情報生成手段と、前記複数の情報処理装置のうち、前記識別情報に基づいて前記各分割パスワードの認証処理を行なう情報処理装置を夫々特定し、特定された前記各情報処理装置に、夫々の前記識別情報と、当該識別情報に対応する前記分割パスワードを夫々送信して、該各情報処理装置から前記分割パスワードの認証結果を夫々取得する認証結果取得手段と、前記第２分割パスワード生成手段にて生成した全ての前記分割パスワードについて、正当である旨の認証結果を取得した場合には、前記情報処理装置の操作制限を解除して、前記ユーザの前記情報処理装置の操作を許可する操作許可手段と、を有し、何れかの前記情報処理装置から前記分割パスワード及び前記識別情報を受信して、認証要求がされた前記情報処理装置は、受信した前記識別情報が前記記憶手段に記憶されている場合には、当該識別情報に対応付けて前記記憶手段に記憶された前記分割パスワードが、受信した前記分割パスワードと一致するか否かに基づいて、受信した前記分割パスワードの認証を行なう認証手段と、前記認証手段による認証結果を前記分割パスワード及び前記識別情報の送信元の情報処理装置へ送信する認証結果送信手段と、を有することを特徴とする情報共用システムである。

【００１０】

この発明によれば、ユーザによる情報処理装置の操作制限を解除するための認証処理を、従来の認証処理を行なう認証サーバを用いずとも、複数の情報処理装置で行なうことができる。更にパスワードを複数の分割パスワードに分割して、それぞれ異なる情報処理装置にて認証を行なうので、セキュリティ性の高い認証を行なうことができる。また、ユーザ情報及びパスワードに基づいて認証を行なうので、ユーザは何れの情報処理装置であっても、ユーザ情報及びパスワードを入力して正当である旨の認証結果を得れば、操作制限を解除して、コンテンツ検索やコンテンツ視聴等、情報共有システムを利用することができる。

【００１１】

上記課題を解決するため、請求項２に記載の発明は、ネットワークを介して互いに通信可能な複数の情報処理装置を備え、当該複数の情報処理装置によって共用される複数の共用情報が複数の情報処理装置に分散されて保存されている情報共有システムであって、該システムを利用する複数のユーザの管理を行なう管理装置を含む前記情報共有システムにおける認証方法において、前記管理装置が、前記ユーザによる前記情報処理装置の操作を許可するためのパスワードを、文字数や分割数等が決められた所定の分割手法で分割して複数の分割パスワードを生成する工程と、前記管理装置が、前記ユーザを識別するための固有のユーザ情報と、各前記分割パスワードと、に対応する固有の識別情報を生成する工程と、前記管理装置が、前記複数の情報処理装置のうち、前記識別情報に基づいて前記各分割パスワードの認証処理を行なうべき情報処理装置を夫々特定し、特定された前記各情報処理装置に認証処理担当となることを要求する工程と、前記管理装置によって、前記識

別情報に基づいて前記分割パスワードの前記認証処理を行なうべき情報処理装置として特定され、認証処理担当となることを要求された各前記情報処理装置が、当該識別情報及び前記分割パスワードを取得して、夫々対応付けて記憶手段に記憶する工程と、ユーザによる操作の制限がなされた前記情報処理装置が、前記ユーザが前記パスワードと、前記ユーザ情報を入力する工程と、前記入力されたパスワードを、文字数や分割数等が決められた所定の分割手法で分割して前記複数の分割パスワードを生成する分割パスワード生成工程と前記ユーザ情報と、前記各分割パスワードと、に対応する前記識別情報を夫々生成する工程と、前記複数の情報処理装置のうち、前記識別情報に基づいて前記各分割パスワードの認証処理を行なう情報処理装置を夫々特定し、特定された前記各情報処理装置に、夫々の前記識別情報と、当該識別情報に対応する前記分割パスワードを夫々送信する工程と、何れかの前記情報処理装置から前記分割パスワード及び前記識別情報を受信して、認証要求がされた前記情報処理装置が、受信した前記識別情報が前記記憶手段に記憶されている場合には、前記記憶手段に当該識別情報に対応付けて記憶された前記分割パスワードが、受信した前記分割パスワードと一致するか否かに基づいて、受信した前記分割パスワードの認証を行ない、当該認証結果を前記分割パスワード及び前記識別情報の送信元の情報処理装置へ送信する工程と、前記ユーザによって操作される前記情報処理装置が、前記分割パスワードの認証結果を夫々取得し、かつ、前記分割パスワード生成工程にて生成した全ての前記分割パスワードについて、正当である旨の認証結果を取得した場合には、前記情報処理装置の操作制限を解除して、前記ユーザの前記情報処理装置の操作を許可する工程と、を有することを特徴とする情報共有システムにおける認証方法である。

【００１２】

この発明によれば、ユーザによる情報処理装置の操作制限を解除するための認証処理を、従来の認証処理を行なう認証サーバを用いずとも、複数の情報処理装置で行なうことができる。更にパスワードを複数の分割パスワードに分割して、それぞれ異なる情報処理装置にて認証を行なうので、セキュリティ性の高い認証を行なうことができる。また、ユーザ情報及びパスワードに基づいて認証を行なうので、ユーザは何れの情報処理装置であっても、ユーザ情報及びパスワードを入力して正当である旨の認証結果を得れば、操作制限を解除して、コンテンツ検索やコンテンツ視聴等、情報共有システムを利用することができる。

【００１３】

上記課題を解決するため、請求項３に記載の発明は、ネットワークを介して互いに通信可能な複数の情報処理装置を備え、当該複数の情報処理装置によって共用される複数の共用情報が複数の情報処理装置に分散されて保存されている情報共有システムであって、該システムを利用する複数のユーザの管理を行なう管理装置において、前記ユーザによる前記情報処理装置の操作を許可するためのパスワードを、文字数や分割数等が決められた所定の分割手法で分割して複数の分割パスワードを生成する第１分割パスワード生成手段と、前記ユーザを識別するための固有のユーザ情報と、各前記分割パスワードに基づいて、前記各分割パスワードに対応する固有の識別情報を生成する第１識別情報生成手段と、前記複数の情報処理装置のうち、前記識別情報に基づいて前記各分割パスワードの認証処理を行なうべき情報処理装置を夫々特定し、特定された前記各情報処理装置に認証処理担当となることを要求する認証処理担当要求手段と、を有することを特徴とする管理装置である。

【００１４】

この発明によれば、ユーザによる情報処理装置の操作制限を解除するための認証処理を、従来の認証処理を行なう認証サーバを用いずとも、複数の情報処理装置で行なわせるよう要求することができる。更にパスワードを複数の分割パスワードに分割して、それぞれ異なる情報処理装置を認証処理担当として要求するので、セキュリティ性の高い認証を行なうことができる。

【００１５】

上記課題を解決するため、請求項４に記載の発明は、請求項３に記載の管理装置におい

て、前記第１識別情報生成手段は、前記分割パスワード当たり所定数の前記識別情報を生成することを特徴とする管理装置である。

【００１６】

この発明によれば、一部の認証担当の情報処理装置に障害が発生した場合であっても、ユーザの認証を行なうことができる。

【００１７】

上記課題を解決するため、請求項５に記載の発明は、請求項３又は４に記載の管理装置において、前記ユーザ情報と、前記パスワードと、を夫々対応付けて記憶する記憶手段を有し、何れかの前記情報処理装置から前記パスワード及び前記ユーザ情報を受信して、前記各情報処理装置間で行なわれる認証ができないことに基づく認証処理要求を受け付ける認証処理受付手段と、受信した前記ユーザ情報に対応付けて前記記憶手段に記憶された前記パスワードが、受信した前記パスワードと一致するか否かに基づいて、受信した前記パスワードの認証を行なう認証手段と、前記認証手段による認証結果を前記パスワード及び前記ユーザ情報の送信元の情報処理装置へ送信する認証結果送信手段と、を有することを特徴とする管理装置である。

【００１８】

この発明によれば、管理装置にユーザ情報とパスワードを記憶させるよう構成し、情報処理装置間で各分割パスワードの認証が適式に行なわれない場合には、管理装置がユーザ情報とパスワードを受信して、管理装置にて認証処理を行なうこともできる。

【００１９】

上記課題を解決するため、請求項６に記載の発明は、請求項３乃至５のいずれか一項に記載の管理装置において、前記認証手段は、何れかの前記情報処理装置から前記ユーザ情報、前記パスワード及び新しいパスワードを受信し、パスワードの変更処理要求がされると、前記受信した前記パスワードの認証を行ない、前記パスワードにかかる認証結果が正当である場合には、前記記憶手段は、前記ユーザ情報と、前記新しいパスワードと、を対応付けて記憶し、前記第１分割パスワード生成手段は、前記パスワードにかかる認証結果が正当である場合には、前記受信した新しいパスワードを、前記所定の分割手法で分割して前記複数の分割パスワードを生成し、前記第１識別情報生成手段は、前記ユーザ情報と、前記生成された分割パスワードに対応する前記識別情報を生成し、前記認証処理担当要求手段は、前記複数の情報処理装置のうち、前記識別情報に基づいて前記各分割パスワードの認証処理を行なうべき情報処理装置を夫々特定し、特定された前記各情報処理装置に認証処理担当となることを要求することを特徴とする管理装置である。

【００２０】

この発明によれば、管理装置にてパスワードを変更可能に構成したので、大規模なシステム障害が発生したときなど、認証担当の情報処理装置が全てダウンした場合であっても、パスワードの変更等を行なって、再度、複数の情報処理装置に分割パスワードを記憶させて認証担当となるよう要求し、新たなパスワードの認証担当の情報処理装置を迅速に設定することができる。

【００２１】

上記課題を解決するため、請求項７に記載の発明は、コンピュータを、請求項３乃至６のいずれか一項に記載の管理装置として機能させることを特徴とする管理処理プログラムである。

【００２２】

この発明によれば、上記管理処理プログラムをコンピュータにて実行することで、請求項３乃至６のいずれか一項に記載の発明の効果を奏することができる。

【００２３】

上記課題を解決するため、請求項８に記載の発明は、ネットワークを介して互いに通信可能な複数の情報処理装置を備え、当該複数の情報処理装置によって共用される複数の共用情報が複数の情報処理装置に分散されて保存されている情報共有システムに含まれる前記情報処理装置であって、ユーザによる操作の制限がなされた前記情報処理装置において

、前記ユーザによる前記情報処理装置の操作を許可するためのパスワードと、前記ユーザを識別するための固有のユーザ情報と、を入力する入力手段と、前記入力されたパスワードを、文字数や分割数等が決められた所定の分割手法で分割して複数の分割パスワードを生成する第２分割パスワード生成手段と、前記ユーザ情報と、前記各分割パスワードに基づいて、前記各分割パスワードに対応する固有の識別情報を夫々生成する第２識別情報生成手段と、前記複数の情報処理装置のうち、前記識別情報に基づいて前記各分割パスワードの認証処理を行なう情報処理装置を夫々特定し、特定された前記各情報処理装置に、夫々の前記識別情報と、当該識別情報に対応する前記分割パスワードを夫々送信して、該各情報処理装置から前記分割パスワードの認証結果を夫々取得する認証結果取得手段と、前記第２分割パスワード生成手段にて生成した全ての前記分割パスワードについて、正当である旨の認証結果を取得した場合には、前記情報処理装置の操作制限を解除して、前記ユーザの前記情報処理装置の操作を許可する操作許可手段と、を有することを特徴とする情報処理装置である。

【００２４】

この発明によれば、ユーザによる情報処理装置の操作制限を解除するための認証処理を、従来の認証処理を行なう認証サーバを用いずとも、複数の情報処理装置で行なうことができる。更にパスワードを複数の分割パスワードに分割して、それぞれ異なる情報処理装置にて認証を行なうので、セキュリティ性の高い認証を行なうことができる。また、ユーザ情報及びパスワードに基づいて認証を行なうので、ユーザは何れの情報処理装置であっても、ユーザ情報及びパスワードを入力して正当である旨の認証結果を得れば、操作制限を解除して、コンテンツ検索やコンテンツ視聴等、情報共有システムを利用することができる。

【００２５】

上記課題を解決するため、請求項９に記載の発明は、請求項８に記載の情報処理装置において、前記第２識別情報生成手段は、前記分割パスワード当たり所定数の前記識別情報を生成し、前記認証結果取得手段は、前記分割パスワード毎に、前記所定数の識別情報に基づいて特定された所定数台の前記各情報処理装置に、夫々の前記識別情報と、当該識別情報に対応する前記分割パスワードを夫々送信して、該各情報処理装置から前記分割パスワードの認証結果を夫々取得し、前記第２分割パスワード生成手段にて生成した前記分割パスワードのうち、少なくとも一の前記分割パスワードについて、前記所定数のうち前記認証結果取得手段が認証結果を取得できなかった数が、有効閾値以下であるか否かを判定する判断有効判定手段を有し、前記判定の結果、認証結果を取得できなかった数が、有効閾値以下であると判定された場合には、前記操作許可手段は、前記全ての分割パスワードについて、前記認証結果取得手段が取得した認証結果のうち、正当である旨の認証結果が、所定閾値以上である場合に、前記情報処理装置の操作制限を解除して、前記ユーザの前記情報処理装置の操作を許可することを特徴とする情報処理装置である。

【００２６】

この発明によれば、一部の認証担当の情報処理装置に障害が発生した場合であっても、ユーザの認証を行なうことができる。また、取得した認証結果のうち、正当である旨の認証結果が、所定閾値以上である場合に、情報処理装置の操作制限を解除するよう構成したので、所望の認証の厳密性に応じて適宜設定できる。

【００２７】

上記課題を解決するため、請求項１０に記載の発明は、請求項９に記載の情報処理装置において、前記所定閾値は、前記第２識別情報生成手段が生成する前記識別情報の前記所定数、前記第２識別情報生成手段が生成する前記識別情報の前記所定数の半数、又は、一の前記分割パスワードについて前記認証結果取得手段が取得した認証結果の数、又は、一の前記分割パスワードについて前記認証結果取得手段が取得した認証結果の半数、又は、１であることを特徴とする情報処理装置である。

【００２８】

上記課題を解決するため、請求項１１に記載の発明は、請求項９又は１０に記載の情報

処理装置において、前記情報共有システムは、該システムを利用する複数の前記ユーザについて、前記ユーザ情報と、当該ユーザ情報に対応する前記パスワードと、を夫々記憶する管理装置を含み、前記判断有効判定手段の判定の結果、前記第２分割パスワード生成手段にて生成した前記分割パスワードのうち、少なくとも一の前記分割パスワードについて、前記所定数のうち前記認証結果取得手段が認証結果を取得できなかった数が、有効閾値以下でないと判定された場合には、前記認証結果取得手段は、前記管理装置に対して、前記パスワードと前記ユーザ情報を送信し、前記管理装置から前記パスワードの認証結果を取得し、前記操作許可手段は、前記管理装置から、前記パスワードが正当である旨の認証結果を取得した場合には、前記情報処理装置の操作制限を解除して、前記ユーザの前記情報処理装置の操作を許可することを特徴とする情報処理装置である。

【００２９】

この発明によれば、情報処理装置間で各分割パスワードの認証が適式に行なわれない場合には、管理装置にユーザ情報とパスワードを送信して、管理装置から認証結果を取得することもできる。

【００３０】

上記課題を解決するため、請求項１２に記載の発明は、請求項１１に記載の情報処理装置において、前記管理装置に対して、前記ユーザ情報、前記パスワード及び新しいパスワードを送信し、前記パスワードの変更処理要求を行なうパスワード変更処理要求手段を有することを特徴とする情報処理装置である。

【００３１】

この発明によれば、大規模なシステム障害が発生したときなど、認証担当の情報処理装置が全てダウンした場合であっても、管理装置にてパスワードの変更処理要求を行なうことができるので、新たなパスワードの認証担当の情報処理装置を迅速に設定することができる。

【００３２】

上記課題を解決するため、請求項１３に記載の発明は、コンピュータを、請求項８乃至１２のいずれか一項に記載の情報処理装置として機能させることを特徴とする情報処理プログラム。

【００３３】

この発明によれば、上記情報処理プログラムをコンピュータにて実行することで、請求項８乃至１２のいずれか一項に記載の発明の効果を奏することができる。

【発明の効果】

【００３４】

本発明によれば、ユーザによる情報処理装置の操作制限を解除するための認証処理を、従来の認証処理を行なう認証サーバを用いずとも、複数の情報処理装置で行なうことができる。更にパスワードを複数の分割パスワードに分割して、それぞれ異なる情報処理装置にて認証を行なうので、セキュリティ性の高い認証を行なうことができる。また、ユーザ情報及びパスワードに基づいて認証を行なうので、ユーザは何れの情報処理装置であっても、ユーザ情報及びパスワードを入力して正当である旨の認証結果を得れば、操作制限を解除して、コンテンツ検索やコンテンツ視聴等、情報共有システムを利用することができる。

【発明を実施するための最良の形態】

【００３５】

［１．コンテンツ配信システムの構成等］

始めに、図１を参照して、複数のノード装置で情報を共用する情報共用システムとしてのコンテンツ配信システムの概要構成等について説明する。

【００３６】

図１は、本実施形態に係るコンテンツ配信システムＳにおける各ノード装置の接続態様の一例を示す図である。

【００３７】

図１の下部枠５０１内に示すように、中継装置としてのＩＸ（Internet eXchange）３、ＩＳＰ（Internet Service Provider）４、ＤＳＬ（Digital Subscriber Line）回線事業者の装置５、ＦＴＴＨ（Fiber To The Home）回線事業者の装置６、及び通信回線（例えば、電話回線や光ケーブル等）７等によって、インターネット等のネットワーク（現実世界のネットワーク）８が構築されている。

【００３８】

そして、このようなネットワーク８を介して相互に接続された各ノード装置１ａ，１ｂ，１ｃ・・・１ｘ，１ｙ，１ｚ・・には、ＩＰ（Internet Protocol）アドレス等の宛先情報を含むノード装置を示す情報（ノード情報）が割り当てられており、更に各ノード装置を特定するための固有の値としてのノードＩＤ（ＩＤentifier）が割り当てられている。これらノードＩＤは複数のノード装置間で重複しないものである。なお、以下の説明において、ノード装置１ａ，１ｂ，１ｃ・・・１ｘ，１ｙ，１ｚ・・・のうち何れかのノード装置を示す場合には、便宜上、ノード装置１という場合がある。

【００３９】

また、コンテンツ配信システムＳにおいて、当該ノード装置１が、他のノード装置１の持つ情報にアクセスする際には、その情報を持つノード装置１の宛先情報（ＩＰアドレス及びポート番号）を知っていなければならない。

【００４０】

このようなシステムの一例として、ＤＨＴを利用したアルゴリズムによって、図１の上部枠５００内に示すような、オーバーレイネットワーク９が構築されることになる。つまり、このオーバーレイネットワーク９は、既存のネットワーク８を用いて形成された仮想的なリンクを構成するネットワークを意味する。

【００４１】

ノードＩＤは、各ノード装置を一意に識別することができるものであればよく、例えば、工場出荷時に予め割り振られる製造番号やマシン名等を共通のハッシュ関数（ハッシュアルゴリズム）によりハッシュ化して得たハッシュ値をＧＵＩＤ（Global Unique IDentifier）として用い、これをノードＩＤとして各ノード装置１に用いることが可能である。

【００４２】

またノードＩＤは、ノード装置の最大運用台数を収容できるだけのｂｉｔ数を持たせる必要がある。例えば、１２８ｂｉｔの番号とすれば、2^128　340×10^36台のノード装置を運用できる。実際には既知のハッシュ関数であるＳＨＡ－１（Secure Hash Algorithm 1）（生成桁数１６０bit）やMD5（Message Digest 5）（生成桁数１２０Bit）を用いることが想定される。

【００４３】

また、コンテンツ配信システムＳは、本発明の管理装置の一例としてのシステム管理サーバ（以下、「サーバ」と言う。）１００を備える。このサーバ１００は、オーバーレイネットワーク９内の各ノード装置１を利用できるユーザを、後述するユーザＩＤ及びパスワードにて管理している。また、サーバ１００は、各ノード装置１で共用されるコンテンツをコンテンツ配信システムＳに投入してノード装置１に登録させると共に、ネットワーク内にあるコンテンツのタイトル、コンテンツＩＤ、コンテンツの価格等を含むコンテンツ登録情報をカタログリストとして全ノード装置１に配布するなどのコンテンツ登録作業等を行なう。

【００４４】

さらに、コンテンツ配信システムＳは、ユーザが最初に、ユーザＩＤ及びパスワードをサーバ１００に登録するためのユーザ登録用装置２００を備える。このユーザ登録用装置２００は、ユーザが、コンテンツ配信システムＳを利用するためにノード装置１を購入したときに、サーバ１００にアクセスしてユーザＩＤ及びパスワードを登録するための装置で、ユーザ管理の観点から、購入店舗に設置されているものである。

【００４５】

［１－１．ＤＨＴの概要］

以下に、本実施形態に係る分散ハッシュテーブル（以下、ＤＨＴ（Distributed Hash Table）という）を利用したアルゴリズムについて説明する。

【００４６】

本実施形態は、ＤＨＴを利用したアルゴリズムによって構築されたオーバーレイネットワーク９を前提としており、このオーバーレイネットワーク９（図１の上部枠５００内）に配置されたノード装置１を、オーバーレイネットワーク９に参加しているノード装置１という。言い換えれば、オーバーレイネットワーク９は、ノード装置１の参加により形成されている。このようなオーバーレイネットワーク９への参加は、参加していないノード装置１が、参加している任意のノード装置１に対して参加要求をすることによって行われる。

【００４７】

また、コンテンツ配信システムＳに参加している複数のノード装置１には、１のノード装置１から他のノード装置１に配信される共用情報としてのコンテンツ（例えば、映画や音楽等）データが分散して保存（格納）されているが、当該コンテンツにも、それぞれのコンテンツ毎にユニーク（固有）なコンテンツＩＤが付与される。

【００４８】

このコンテンツＩＤは、ノードＩＤと同様の長さ（例えば、１２８ｂｉｔ等）であって、コンテンツをコンテンツ配信システムＳに投入してノード装置１に登録を行なうサーバ１００によって決定され各コンテンツに付与される。

【００４９】

図２は３２ｂｉｔでノードＩＤ及びコンテンツＩＤを付与し、ＩＤ空間上に図示したものである。図中黒点はノードＩＤを、黒ひし形はコンテンツＩＤを示し、反時計回りでＩＤが増加するものとする。

【００５０】

図２に示すようなＩＤ空間において、どのノード装置１に、どのコンテンツが管理されるかは、コンテンツＩＤとノードＩＤとが「所定の関係」にあるか否かによって決定される。ここで、「所定の関係」とは、一定の規則の下に決定されるが、本実施形態においては、「あるコンテンツＩＤを有するコンテンツデータを管理するノード装置は、そのコンテンツＩＤに最も近接するノードＩＤを有するノード装置１である」という規則とする。つまり、コンテンツＩＤと最も近接する（例えば、上位桁がより多く一致する）ノードＩＤであって、コンテンツＩＤの値と同じかそれ以下の値となるノードＩＤを有するノード装置１が、当該コンテンツデータを保存するノード装置の所在情報を管理することとする。

【００５１】

本実施形態における「所定の関係」の定義は、当該コンテンツＩＤを超えず、コンテンツＩＤとノードＩＤとの差が一番少ないものとするが、各コンテンツデータの管理を各ノード装置１に割り振る際に、一貫していればどのような定義であってもよい。同図に示す例では、この定義に基づいて、コンテンツＩＤａは、ノードＩＤａを有するノード装置に管理され、コンテンツＩＤｂは、ノードＩＤｂを有するノード装置に管理される。また、コンテンツＩＤｃ、ＩＤｄは、ノードＩＤｃを有するノード装置１に管理されるように、あるノード装置は複数の異なるコンテンツデータを管理することもある。なお、ここで「管理」というのは、コンテンツを保存／保持していることを意味するのではなく、「コンテンツのデータ（コンテンツデータ）が何れのノード装置１に保存されているかを知っている」ことを言う。

【００５２】

このようなコンテンツ配信システムＳを利用するユーザは、最初にサーバ１００に対してシステム利用登録を行なうこととする。そして、システム利用登録を行なった正規のユーザが、オーバーレイネットワーク９に含まれる何れかのノード装置１を操作して、氏名、ニックネーム、会員番号又はハンドルネーム等の「ユーザＩＤ」（ユーザ情報の一例）、及び当該ユーザＩＤに対応する「パスワード」を入力し、ユーザ認証がされた場合にだ

け、操作制限を解除することができる。図３にノード装置１のユーザＩＤ及びパスワード入力画面例を示す。

【００５３】

操作制限とは、ユーザ認証がされなければ、システムを利用することができない、つまり、ノード装置１を操作してコンテンツの検索やコンテンツの視聴などができないことをいう。

【００５４】

ユーザＩＤ及びパスワードによるユーザ認証は、各ノード装置１にて分散して行なわれるが、あるノード装置１が、任意のユーザのユーザＩＤ及びパスワードの組を記憶して、認証処理を遂行できるよう構成すると、自分以外の他のノード装置１がユーザＩＤ及びパスワードの組を知ることとなるので、セキュリティ上好ましくない。

【００５５】

従って、ここではパスワードを所定の分割手法で分割し、分割パスワードを夫々異なるノード装置１が記憶して認証するよう構成した。

【００５６】

例えば、パスワードが“ＰＡＳＳ”である場合、所定の文字数毎に分割する。ここで、所定の文字数毎とは、例えばパスワードの先頭から１文字毎としてもよく、或いは、２文字毎としてもよい。また、所定文字数毎に分割するとともに、分割数を規定したり、分割数に閾値を設けてもよい。本実施形態の分割手法は、パスワードを構成する文字数を、３で割った商の一の位の数の文字毎に、パスワードを区切り分割パスワードとする。このとき、分割数は最大３つまでとし、余った文字は最後の分割パスワードに組み込むこととした。

【００５７】

パスワード“ＰＡＳＳ”の場合、

（ｉ）パスワード“ＰＡＳＳ”を構成する文字数は、「４」

（ｉｉ）４を３で割った商は、４÷３＝１．３３…　　従って商の整数部は「１」

（ｉｉｉ）パスワード“ＰＡＳＳ”を「１」文字毎に、分割数最大３つまで区切り（Ｐ、Ｓ、Ｓ）あまった文字Ｓを、最後の分割パスワードＳに組み込み、“Ｐ”、“Ａ”、“ＳＳ”の３つの分割パスワードに分割する。

【００５８】

そして、誰の、どの分割パスワードが、どのノード装置１に（記憶されて）認証されるかは、サーバ１００が、ユーザＩＤと分割パスワードに対応する固有の認証識別ＩＤ（識別情報の一例）を生成し、生成した認証識別ＩＤとノードＩＤとが「所定の関係」にあるノード装置１に対して、当該認証識別ＩＤに対応する（生成元となった）分割パスワードと当該認証識別ＩＤを記憶するよう、すなわち、この認証識別ＩＤに対応する（生成元となった）ユーザＩＤの、分割パスワードの認証を担当するよう要求する。本実施形態では「所定の関係」を、上述したコンテンツのルートノードと同様に、当該認証識別ＩＤを超えず、認証識別ＩＤとの差が一番少ないノードＩＤのノード装置１とするが、決め方はこれに限定されるものではなく、一定の規則の下に決定すればよい。

【００５９】

具体的には、認証識別ＩＤは、ユーザＩＤと、当該ユーザＩＤにかかるパスワードをｎつ（ｎは、ここでは「３」）に分割したときの分割番号ｎ（１≦ｎ≦３、ｎは自然数）と、からなる文字列を、上記ノードＩＤを得るときと共通のハッシュ関数によりハッシュ化して生成する。例えば、あるユーザのユーザＩＤが“ｕｓｅｒ１”であって、パスワード“ＰＡＳＳ”に基づいて分割した分割パスワードが夫々“Ｐ”、“Ａ”、“ＳＳ”である場合には、分割パスワード毎に異なる認証識別ＩＤが生成される。

【００６０】

図４は３２ｂｉｔでノードＩＤ及び認証識別ＩＤを付与し、ＩＤ空間上に図示したものである。図中黒点はノードＩＤを、黒ひし形は認証識別ＩＤを示し、反時計回りでＩＤが増加するものとする。図４に示す例では、この定義に基づいて、認証識別ＩＤ（Ｐ）の分

割パスワード“Ｐ”は、ノードＩＤａを有するノード装置が認証担当となり、認証識別ＩＤ（Ａ）の分割パスワード“Ａ”は、ノードＩＤｂを有するノード装置が認証担当となり、認証識別ＩＤ（ＳＳ）の分割パスワード“ＳＳ”は、ノードＩＤｃを有するノード装置が認証担当となる。あるノード装置が、異なるユーザの、異なる分割パスワードを複数記憶して、夫々の認証担当となることもある。さらに、当該分割パスワードを記憶する際のＤＨＴルーティングによる経路上に在るノード装置も分割パスワードを記憶して、補助の認証担当となる。この、分割パスワードを記憶する際のＤＨＴルーティングによる経路上に在るノード装置については、後に詳述する。

【００６１】

［１－２．ルーティングテーブルの作成］

ここで、図５及び図６を参照して、ＤＨＴで用いるルーティングテーブルの作成手法の一例について説明する。

【００６２】

図５は、ＤＨＴにおけるルーティングテーブルの構成の一例を示す図である。

【００６３】

まず、図５（Ａ）に示す如く、ＩＤ空間を幾つかのエリアに分割する。なお、このエリアはルーティングテーブルを作成するためにＩＤ空間を分割したものであって、実際には、１６分割程度が良く用いられるが、説明を簡単にするためここでは４分割とし、ＩＤをビット長１６Ｂｉｔの４進数で表すこととした。そして、ノード装置１Ｎのノードを「10230210」とし、このノード装置１Ｎのルーティングテーブルを作る例について説明する。

【００６４】

（レベル１のルーティング）

まず、ＩＤ空間を４分割とすると、それぞれのエリアは４進数で表すと最大桁が異なる４つのエリア「0XXXXXXX」「1XXXXXXX」、「2XXXXXXX」、「3XXXXXXX」（Xは０から３の自然数、以下同様。）で分けられる。あるノード装置（以下、ノード装置１Ｎと言う。）は、当該ノード装置１Ｎ自身のノードＩＤが「10230210」であるため、図中左下「1XXXXXXX」のエリアに存在することになる。そして、ノード装置１Ｎは、自分の存在するエリア（すなわち、「1XXXXXXX」のエリア）以外のエリアに存在するノード装置１を適当に選択し、当該ノードＩＤの宛先情報（ＩＰアドレス及びポート番号）をレベル１のテーブルに記憶する。図６（Ａ）がレベル１のテーブルの一例である。２列目はノード装置１Ｎ自身を示しているため、宛先情報（ＩＰアドレス及びポート番号）を記憶する必要は無い。

【００６５】

（レベル２のルーティング）

次に、図５（Ｂ）に示す如く、上記ルーティングによって４分割したエリアのうち、自分の存在するエリアを更に４分割し、更に４つのエリア「10XXXXXX」「11XXXXXX」、「12XXXXXX」、「13XXXXXX」と分ける。そして、上記と同様に自分の存在するエリア以外のエリアに存在するノード装置１を適当に選択し、当該ノードＩＤの宛先情報（ＩＰアドレス及びポート番号）をレベル２のテーブルに記憶する。図６（Ｂ）がレベル２のテーブルの一例である。１列目はノード装置１Ｎ自身を示しているため、宛先情報（ＩＰアドレス及びポート番号）を記憶する必要は無い。

【００６６】

（レベル３のルーティング）

さらに、図５（Ｃ）に示す如く、上記ルーティングによって４分割したエリアのうち、自分の存在するエリアを更に４分割し、更に４つのエリア「100XXXXX」「101XXXXX」、「102XXXXX」、「103XXXXX」と分ける。そして、上記と同様に自分の存在するエリア以外のエリアに存在するノード装置１を適当に選択し、当該ノードＩＤの宛先情報（ＩＰアドレス及びポート番号）をレベル１のテーブルに記憶する。図６（Ｃ）がレベル３のテーブルの一例である。３列目はノード装置１Ｎ自身を示しているため、宛先情報（ＩＰアドレス及びポート番号）を記憶する必要は無く、２列目、４列目はそのエリアにノード装置が存

在しないため空白となる。

【００６７】

このようにして、レベル４以下レベル８まで同様にルーティングテーブル図６（Ｄ）に示す如く作成することにより、１６ｂｉｔのＩＤ全てを網羅することができる。レベルが上がる毎にテーブルの中に空白が目立つようになる。

【００６８】

実際に、オーバーレイネットワーク９に未参加のノード装置１が、オーバーレイネットワーク９に参加して、上述したような構成になるようにテーブルを作るには、まず、オーバーレイネットワーク９に参加する際に、最初にアクセスしたノード装置１に対して参加依頼メッセージを送信すると共に、当該ノード装置１からルーティングテーブルをコピーさせてもらう。また、メッセージの転送などの際に、他のノード装置１の存在を知ったタイミングで、その装置のノードＩＤがテーブルのどのマス目に適合するかを判断して、各テーブルの内容を追記（更新）していく。また、他のノード装置が脱退したことを知ったタイミングで、当該装置のノードＩＤをテーブルから削除する。

【００６９】

以上説明した手法に従って、ノード装置１が使用するルーティングテーブルが作成され、動的に追記（更新）されていく。

【００７０】

［１－３．分割パスワードの認証担当ノード装置の特定］

以下、図７を用いて、分割パスワードの認証担当のノード装置を特定する手法について説明する。図７（Ａ）はサーバ１００からノード装置１へ送信される「分割パスワード記憶要求メッセージ」の説明図、図７（Ｂ）は、ノード装置１が分割パスワードの認証担当となる際の様子をＤＨＴのＩＤ空間にて示した概念図である。

【００７１】

サーバ１００は、各分割パスワードの認証担当となることを要求すべく、分割パスワードの記憶を要求する「分割パスワード記憶要求メッセージ」を、ＤＨＴルーティングによって特定されるノード装置１へと送出する。この「分割パスワード記憶要求メッセージ」には、図７（Ａ）に示すように、分割パスワード、及び当該分割パスワードに対応する認証識別ＩＤが含まれる。そして、図７（Ｂ）に示すように、「分割パスワード記憶要求メッセージ」は、該メッセージに含まれる認証識別ＩＤをキーとするルーティングに従って、各ノード装置１間を転送し、当該認証識別ＩＤを超えず、認証識別ＩＤとの差が一番少ないノードＩＤのノード装置１まで辿り着く。そして、当該ノード装置１が他に「分割パスワード記憶要求メッセージ」を転送する先が無いことを認識し、自己の記憶部に、分割パスワードと、認証識別ＩＤを対応付けて記憶する。このようなノード装置１を、分割パスワードの認証ルートノードと呼ぶ。

【００７２】

図７（Ｂ）に示す例によれば、分割パスワード“Ｐ”、“Ａ”、“ＳＳ”にかかる「分割パスワード記憶要求メッセージ」は、サーバ１００から、先ず、ノード装置１ａに送信される。そして、分割パスワード“Ｐ”にかかる「分割パスワード記憶要求メッセージ（Ｐ）」は、実線で示すようにノード装置１ａからノード装置１ｄ、そしてノード装置１ｃへと転送され、分割パスワード“Ａ”にかかる「分割パスワード記憶要求メッセージ（Ａ）」は、一点鎖線で示すようにノード装置１ａからノード装置１ｃ、そしてノード装置１ｅへと転送され、分割パスワード“ＳＳ”にかかる「分割パスワード記憶要求メッセージ（ＳＳ）」は、破線で示すようにノード装置１ａからノード装置１ｉへと転送される。そして、最終的に辿り着いたノード装置１ｃ、１ｅ、１ｉにて、分割パスワード“Ｐ”、“Ａ”、“ＳＳ”が、夫々認証識別ＩＤ（Ｐ）認証識別ＩＤ（Ａ）、認証識別ＩＤ（ＳＳ）、と対応付けて記憶され、夫々の分割パスワードの認証要求に応えることとなる。

【００７３】

特定のノード装置１のみ高負荷となることを防ぐため、サーバ１００から最初に「分割パスワード記憶要求メッセージ」を受けるノード装置を、サーバ１００に登録されている

ノード装置の中からランダムに選択するよう構成すればよい。

【００７４】

また、サーバ１００が、各「分割パスワード記憶要求メッセージ」を夫々異なるノード装置に送信すれば、更にセキュリティ性を向上させることができる。

【００７５】

［１－４．ユーザ認証］

次に、ユーザ認証について図８及び図９を用いて説明する。図８（Ａ）は、ユーザが操作するノード装置１から各ノード装置１へ送信される「認証要求メッセージ」の説明図、図８（Ｂ）は、ユーザ認証を受けるべく、他のノード装置に認証要求をする際の様子をＤＨＴのＩＤ空間にて示した概念図である。

【００７６】

上述したように、ユーザが任意のノード装置１を操作して、コンテンツ配信等を利用しようとする際には、ユーザＩＤとパスワードを入力しなければならない（図３参照。）。

【００７７】

ユーザが操作するノード装置１では、ユーザＩＤ“ｕｓｅｒ１”“及びパスワード“ＰＡＳＳ”が入力され、図３中、カーソルが指し示すように、ログイン実行の要求がされると、パスワードの分割処理が行なわれる。パスワードの分割は、サーバ１００にて当該パスワードを分割したとき、つまり、当該パスワードを分割して各ノード装置１に記憶させたときと同じ分割手法で分割する。本実施形態では、パスワードが“ＰＡＳＳ”である場合、上述したサーバ１００での分割手法と同じく“Ｐ”、“Ａ”、“ＳＳ”の３つの分割パスワードに分割する。

【００７８】

そして、ユーザＩＤと分割パスワード“Ｐ”に対応する認証識別ＩＤ（Ｐ）、ユーザＩＤと分割パスワード“Ａ”に対応する認証識別ＩＤ（Ａ）、ユーザＩＤと分割パスワード“ＳＳ”に対応する認証識別ＩＤ（ＳＳ）を夫々生成し、各分割パスワードの認証を要求すべく、当該認証識別ＩＤ、分割パスワード及びノード情報（認証結果を受けるため自己の宛先情報を含む）を含む「認証要求メッセージ（図８（Ａ））が、認証担当のノード装置１へ向けて夫々送出される。

【００７９】

この「認証要求メッセージ」は、上記「分割パスワード記憶要求メッセージ」と同様に、メッセージに含まれる認証識別ＩＤをキーとするルーティングに従って、各ノード装置１間を転送し、当該認証識別ＩＤを超えず、認証識別ＩＤとの差が一番少ないノードＩＤのノード装置１まで辿り着く。つまり、「分割パスワード記憶要求メッセージ」と同じ認証識別ＩＤをキーとするルーティングに基づいてノード装置１が特定されるので、ユーザによって、ユーザＩＤ及びパスワードが正しく入力されれば、分割パスワードを記憶し、認証担当となったノード装置（認証ルートノード）に「認証要求メッセージ」が確実に辿り着くようになっている。

【００８０】

図８（Ｂ）に示す例の場合、分割パスワード“Ｐ”、“Ａ”、“ＳＳ”の認証を要求する「認証要求メッセージ（Ｐ）」、「認証要求メッセージ（Ａ）」、「認証要求メッセージ（ＳＳ）」は、夫々、認証識別ＩＤ（Ｐ）、認証識別ＩＤ（Ａ）、認証識別ＩＤ（ＳＳ）キーとするルーティングに従って、各ノード装置１間を転送し、認証担当のノード装置１（同図では、ノード装置１ｃ、１ｅ、１ｉ）まで辿り着く。そして、当該ノード装置１が他に該メッセージを転送する先が無く、自己が認証担当であることを認識すると、該メッセージに含まれる、認証識別ＩＤ及び分割パスワードの正否を認証する。そして、図９に示すように、各分割パスワードについて認証を行なったノード装置１ｃ、１ｅ、１ｉは、各「認証要求メッセージ」に含まれる宛先情報に従って認証結果Ｒ（Ｐ）、Ｒ（Ａ）、Ｒ（ＳＳ）を夫々ノード装置１ｆに返信する。

【００８１】

そして、ノード装置１ｆが、全ての分割パスワード“Ｐ”、“Ａ”、“ＳＳ”について

、正当である（認証ＯＫ）旨の認証結果Ｒを取得した場合にのみ、ノード装置１ｆの操作制限を解除することができる。

【００８２】

［１－５．パスワード変更］

登録済みのパスワードを変更したい場合には、ユーザＩＤ、現在使用中のパスワード及び新しいパスワードをサーバ１００へ送信し、サーバ１００に記憶されているパスワードを変更（更新）する。

【００８３】

具体的には、ユーザがノード装置１を操作して、「パスワード変更」を選択すると（図３参照。）、図１０（Ａ）に示す表示画面例のように、ユーザＩＤ“ｕｓｅｒ１”、現在使用中のパスワード“ＰＡＳＳ”を確認のため再入力するとともに、新しいパスワード“ＰＡＳＳＮＥＷ”を入力する。そして、同図においてカーソルが指し示すように、パスワード変更の要求が選択されると、サーバ１００へユーザＩＤ、現在使用中のパスワード及び新しいパスワードをサーバ１００が送信され（図１０（Ｂ）参照。）、サーバ１００にて、ユーザＩＤ、現在使用中のパスワードの確認された後に、新しいパスワードに変更される。なお、ノード装置１及びサーバ１００の具体的な処理は後にフローチャートを用いて詳述する。

【００８４】

［１－６．ユーザ認証　応用実施例］

上述したように、１つの分割パスワードの認証を、１台のノード装置１のみが担当するよう構成しているが、認証要求が行なわれたときに、当該認証担当のノード装置１がシステムから脱退していたり、或いは、大規模なシステム障害の発生した場合には、脱退したノード装置１が認証担当となっている分割パスワードについての認証が行なわれなくなってしまう。

【００８５】

そこで、異なる複数のノード装置１を、１の分割パスワードの認証担当のノード装置として特定するよう構成する。

【００８６】

図１１（Ａ）に示すように、ユーザＩＤ、分割番号及び接尾辞（例えば、コンテンツ配信システムＳ内で統一された特定文字列ｓａｌｔ）からなる文字列を、上記ノードＩＤを得るときと共通のハッシュ関数によりハッシュ化して認証識別ＩＤを生成する。ここでは、接尾辞として使用する文字列ｓａｌｔを、ｓａｌｔ１、ｓａｌｔ２、ｓａｌｔ３、、、、ｓａｌｔ１０とした、１０個（所定数＝１０）の異なる認証識別ＩＤを生成する。

【００８７】

そして、生成した認証識別ＩＤを夫々含む１０個の「分割パスワード記憶要求メッセージ」を送出し、認証識別ＩＤをキーとするルーティングに従って１０台の異なるノード装置１を特定して、認証識別ＩＤ及び分割パスワードの記憶を要求する。このように、１つの分割パスワードについて、１０台の認証ルートノードを設定する。

【００８８】

ユーザが認証を要求する際にも同様にして、ユーザが操作するノード装置１にて、１つの分割パスワードについて、１０個の認証識別ＩＤを生成する。そして、各認証識別ＩＤを含む１０個の「認証要求メッセージ」を生成（図１１（Ｂ）参照。）し、該メッセージが、認証識別ＩＤをキーとするルーティングに従って、各ノード装置１間を転送して、最終的に辿り着いた認証担当のノード装置１にて分割パスワードの認証が行なわれる。

【００８９】

図１２は、分割パスワード“Ｐ”の認証結果Ｒを１０台の認証担当のノード装置１から受ける際の様子をＤＨＴのＩＤ空間にて示した概念図である。

【００９０】

同図において実線で示すように、分割パスワード“Ｐ”の認証担当の１０台のノード装置１から夫々認証結果Ｒ（Ｐ）を受ける。分割パスワード“Ａ”及び“ＳＳ”についても

、同様にして、認証担当の１０台のノード装置から認証結果Ｒ（Ａ）（一点鎖線）、認証結果Ｒ（ＳＳ）（破線）を受けることとなる。なお、図１２においてノード装置１ｆが受ける認証結果Ｒの数は、図示を簡単にするため省略している。

【００９１】

本実施形態では、正当である（認証ＯＫ）旨の認証結果Ｒが、送出した「認証要求メッセージ」の半数（つまり、生成した認証識別ＩＤの半数）以上である場合、つまり、所定閾値（Ｔｈ）（ここでは５）以上である場合には、該分割パスワードについて正当であるとの認証を受けたものとする。そして、分割パスワード“Ｐ”、“Ａ”、“ＳＳ”の全てについて、夫々、認証ＯＫが５つ以上となり、正当である旨の認証を受けると、ノード装置１ｆの操作制限を解除する。

【００９２】

図１３に示す各分割パスワードの認証結果Ｒの一例を用いて具体的に説明する。同図に示す分割パスワード“Ｐ”の認証結果Ｒは、ｓａｌｔ８を用いて生成された認証識別ＩＤを含む「認証要求メッセージ」に対する認証結果Ｒ（以下、単に「ｓａｌｔに対する認証結果Ｒ」と言う。）のみが、認証ＮＧとするもので、ｓａｌｔ１～７、９及び１０に対する認証結果Ｒは、認証ＯＫとするものである。従って、分割パスワード“Ｐ”は正当である旨の認証結果を得る。

【００９３】

また、分割パスワード“Ａ”のｓａｌｔ７に対する認証結果Ｒのみが、当該認証担当のノード装置１が脱退しているなどの何らかの理由で、認証結果が得られない（応答なし）であって、その他のｓａｌｔ１～６、８～１０に対する認証結果Ｒは、認証ＯＫとするものである。従って、分割パスワード“Ａ”の認証結果は正当である旨の認証結果を得る。

【００９４】

さらに、分割パスワード“ＳＳ”のｓａｌｔ１～３、７に対する認証結果Ｒが、認証ＮＧとするもので、その他のｓａｌｔ４～６、８～１０に対する認証結果Ｒは、認証ＯＫとするものである。従って、認証ＯＫが５つ以上であるので、分割パスワード“ＳＳ”も正当である旨の認証結果を得る。

【００９５】

［２．各装置の構成等］

続いて、ノード装置１、サーバ１００及びユーザ登録用装置２００の構成及び機能について説明する。

【００９６】

［２－１．ノード装置の構成等］

先ず、ノード装置１の構成及び機能について説明する。

【００９７】

図１４は、ノード装置１の概要構成例を示すブロック図である。

【００９８】

図１４に示すように、実施形態に係るノード装置１は、演算機能を有するＣＰＵ，作業用ＲＡＭ，各種データ及びプログラム（本発明の情報処理プログラムを含む）を記憶するＲＯＭ等から構成されたコンピュータとしての制御部１１と、各種データ（例えば、コンテンツデータのレプリカ、ＤＨＴ）及びプログラム等を記憶保存（格納）するためのＨＤＤ等から構成された記憶部１２（上記、コンテンツデータのレプリカは、保存されていないノード装置１もある）と、受信されたコンテンツデータのレプリカを一時蓄積するバッファメモリ１３と、コンテンツデータのレプリカに含まれるエンコードされたビデオデータ（映像情報）及びオーディオデータ（音声情報）等をデコード（データ伸張や復号化等）するデコーダ部１４と、当該デコードされたビデオデータ等に対して所定の描画処理を施しビデオ信号として出力する映像処理部１５と、当該映像処理部１５から出力されたビデオ信号に基づき映像表示するＣＲＴ，液晶ディスプレイ等の表示部１６と、上記デコードされたオーディオデータをアナログオーディオ信号にＤ（Digital）／Ａ（Analog）変換した後これをアンプにより増幅して出力する音声処理部１７と、当該音声処理部１７か

ら出力されたオーディオ信号を音波として出力するスピーカ１８と、ネットワーク８を通じて他のノード装置１との間の情報の通信制御を行なうための通信部２０と、ユーザからの指示を受け付け当該指示に応じた指示信号を制御部１１に対して与える入力手段としての入力部（例えば、キーボード、マウス、或いは、操作パネル等）２１と、を備えて構成され、制御部１１、記憶部１２、バッファメモリ１３、デコーダ部１４、及び通信部２０はバス２２を介して相互に接続されている。

【００９９】

記憶部１２は、オーバーレイネットワーク９に参加する際に最初にアクセスするサーバ１００の宛先情報（ＩＰアドレス及びポート番号）を記憶する。また、自己のノードＩＤとして工場出荷時の製造番号をハッシュ化して得たＧＵＩＤ「XXXXXXXX」（Xは自然数であって、各ノード装置毎に固有の値である。）によるノードＩＤを記憶する。

【００１００】

また、記憶部１２は、記憶手段として機能し、表１に示すように、自身が認証担当である分割パスワードについて、「分割パスワード記憶要求メッセージ」を受信して、各分割パスワードの記憶要求を受けた際に、夫々の「分割パスワード記憶要求メッセージ」に含まれる認証識別ＩＤ、分割パスワードを夫々対応付けて記憶している。

【００１０１】

【表１】

認証識別ＩＤ	分割パスワード
認証識別ＩＤ（Ｐ）	Ｐ
認証識別ＩＤ（Ａ）	Ａ
認証識別ＩＤ（ＴＲ）	ＴＲ
…	…

そして、制御部１１におけるＣＰＵが記憶部１２等に記録された各種プログラムを実行することにより、制御部１１が、実施形態に係るノード装置１としての全体動作を統括制御し、上記各構成部材と協動して、入力手段、第２分割パスワード生成手段、第２識別情報生成手段、認証結果取得手段、操作許可手段、判断有効判定手段、認証手段、認証結果送信手段、及びパスワード変更処理要求手段として機能し、当該ノード装置１を本発明における情報処理装置として機能させる。

【００１０２】

［２－２．サーバの構成等］

図１５は、サーバ１００の概要構成例を示すブロック図である。

【００１０３】

図１５に示すように、本実施形態に係るサーバ１００は、演算機能を有するＣＰＵ、作業用ＲＡＭ（Random Access Memory）、各種データ及びプログラムを記録するＲＯＭ（Read Only Memory）等から構成された制御部１０１と、上記コンテンツ自体としてのコンテンツデータ、その配信に必要な各種ルーティング用データ及びその他の必要なプログラム（本発明の管理処理プログラムを含む）等を記録保存（格納）するためのＨＤＤ（Hard Disc Drive）等から構成された記憶部１０２と、ネットワークを通じてシステムに含まれる各ノード装置１等との間の情報の通信制御を行なうための通信部１０３と、当該サーバ１００を管理する管理者からの指示を受け付け当該指示に応じた指示信号を制御部１０１に出力する入力部（例えば、キーボード、マウス或いは、操作パネル等）１０４と、を備えて構成され、制御部１０１、記憶部１０２及び通信部１０３はバス１０５を介して相互にデータの授受が可能に接続されている。

【００１０４】

記憶部１０２は、記憶手段として機能し、表２に示すようにユーザＩＤとパスワードを夫々対応付けて記憶している。

【０１０５】

【表２】

ユーザＩＤ	パスワード
ｕｓｅｒ１	ＰＡＳＳ
ｕｓｅｒ２	ＳＳＵＳ
ｕｓｅｒ３	ＹＫ
…	…

そして、制御部１０１におけるＣＰＵが記憶部１０２等に記録された各種プログラムを実行することにより、制御部１０１が、実施形態に係るサーバ１００としての全体動作を統括制御し、上記各構成部材と協動して、第１識別情報生成手段、第１分割パスワード生成手段、認証処理担当要求手段、記憶手段、認証処理受付手段、認証手段及び認証結果送信手段として機能し、当該サーバ１００を本発明における管理装置として機能させる。

【０１０６】

［２－３．ユーザ登録用装置の構成等］

図１６は、ユーザ登録用装置２００の概要構成例を示すブロック図である。

【０１０７】

図１６に示すように、本実施形態に係るユーザ登録用装置２００は、演算機能を有するＣＰＵ，作業用ＲＡＭ，各種データ及びプログラムを記憶するＲＯＭ等から構成されたコンピュータとしての制御部２０１と、各種データ及びプログラム等を記憶保存（格納）するためのＨＤＤ等から構成された記憶部２０２と、ユーザ登録用装置２００を操作する店舗店員にたいして各種指示を表示するＣＲＴ，液晶ディスプレイ等の表示部２０３と、ネットワーク８を通じてサーバ１００等との間の情報の通信制御を行なうための通信部２０４と、店舗店員からの指示を受け付け当該指示に応じた指示信号を制御部２０１に対して与えるの入力部（例えば、キーボード、マウス、或いは、操作パネル等）２０５と、を備えて構成され、制御部２０１、記憶部２０２、表示部２０４、及び通信部２０４はバス２０６を介して相互に接続されている。

【０１０８】

そして、制御部２０１におけるＣＰＵが記憶部２０２等に記録された各種プログラムを実行することにより、制御部２０１が、実施形態に係るユーザ登録用装置２００としての全体動作を統括制御する。

【０１０９】

［３．各装置の処理動作］

続いて、各装置の具体的な処理動作について図を用いて説明する。なお、以下の説明は、「１－６．ユーザ認証　応用実施例」にて説明したように、１つの分割パスワードの認証を、ｓａｌｔ１～ｓａｌｔ１０を用いて生成された認証識別ＩＤで特定される１０台の認証ルートノードにて行なう場合について説明する。

【０１１０】

［３－１．ノード装置の処理］

［３－１－１．メイン処理］

初めに、各ノード装置にて実行される処理について説明する。図１７（Ａ）及び（Ｂ）は、ノード装置１におけるメイン処理の一例を示すフローチャートであり、この処理は、制御部１１の制御に基づいて実行され、また、ノード装置１の電源がオンとされることにより開始する。

【０１１１】
先ず、制御部１１は、機器認証処理を行なう（ステップＳ１）。機器認証処理とは、オーバーレイネットワーク９に参加するための認証処理動作であり、先ず、記憶部１２に予め記憶していたサーバ１００の宛先情報（ＩＰアドレス及びポート番号）に基づいて、サーバ１００にアクセスし、コンタクトノードの問合せメッセージを送信する。次に、サーバ１００から、コンタクトノード（オーバーレイネットワーク９に参加している何れかのノード装置１）の宛先情報（ＩＰアドレス及びポート番号）を受信して、コンタクトノードの紹介を受ける。そして、該コンタクトノードに対して、自身のノード装置１の電子証明書を送信する。コンタクトノードでは、その電子証明書に基づいてネットワークへの参加を認めるかどうかを判定して、その判定結果を返答する。ノード装置１は、コンタクトノードからの判定結果が認証ＯＫであれば、オーバーレイネットワーク９に参加できる。
【０１１２】
その後、受信スレッド生成処理を開始する（ステップＳ２）。受信スレッド生成処理は、図１７（Ｂ）のフローチャートに従って実行される。
【０１１３】
先ず、メッセージの受信を待機し（ステップＳ１１）、上述した「分割パスワード記憶要求メッセージ」、「認証要求メッセージ」、後述する「分割パスワード削除要求メッセージ」の何れかの認証関連の各種要求メッセージを受信したか否かを判定（ステップＳ１２）する。なお、当該認証関連の各種要求メッセージは、ＤＨＴルーティングに従ってノード装置間を転送するメッセージである。
【０１１４】
認証関連の各種要求メッセージを受信すると、認証関連の各種要求メッセージを受信時の処理に移行する（ステップＳ１２：Ｙｅｓ、ステップＳ１３）。なお、「認証関連の各種要求メッセージを受信時の処理」については後に詳述する。
【０１１５】
認証関連の各種要求メッセージの受信が無ければ、その他のメッセージの受信時の処理に移行する（ステップＳ１２：Ｎｏ、ステップＳ１４）。なお、その他のメッセージとは、コンテンツの所在（コンテンツを保持するノード装置）を問い合わせるメッセージ等である。
【０１１６】
そして、当該ノード装置１の電源がオフとされるまで、ステップＳ１１～１４の処理が繰り返し実行される。
【０１１７】
図１７（Ａ）のフローチャートでは、ステップＳ２の受信スレッド生成処理を開始した後に、「ログイン関連処理」が実行される（ステップＳ３）。なお、「ログイン関連処理」については後に詳述する。
【０１１８】
ログインが許可されたか否かを判定（ステップＳ４）し、ログインが許可されるとコンテンツ検索、コンテンツ視聴など、ノード装置としての主要な処理を行なう（ステップＳ４：Ｙｅｓ、ステップＳ５）。具体的には、サーバ１００から配布されたコンテンツのカタログを表示部１６に表示してユーザに提示し、ユーザがその中から見たいコンテンツを選択して、そのコンテンツを保持するノード装置をＤＨＴルーティングにより特定し、当該ノード装置よりコンテンツを配信してもらい視聴するなどの動作を行なう。なお、この動作は、表示部１６に表示された図示しない「ログアウトボタン」を選択する等の動作が行なわれるまで、ステップＳ５の処理が実行されつづける（ステップＳ６：Ｎｏ）。ログアウトボタンが選択されると（ステップＳ６：Ｙｅｓ）、コンテンツの視聴画面の表示等を終了するなど、ユーザによる当該ノード装置１の操作を再び制限するログアウト処理が実行される（ステップＳ７）。
【０１１９】
他方、ログインが許可されなかった場合（ステップＳ４：Ｎｏ）、及びステップＳ７で

ログアウト処理が行なわれた場合には、ステップＳ３に移行する。

【０１２０】

なお、上述したノード装置の基本処理は、ノード装置１の電源がオフとならない限り実行され続ける。

【０１２１】

［３－１－２．ログイン関連処理］

次に、上述したステップＳ３で実行される「ログイン関連処理」について図１８のフローチャートを用いて説明する。

【０１２２】

先ず、制御部１１は、入力手段として機能し、表示部１６にログイン画面を表示し、ユーザＩＤ及びパスワードの入力を指示する（ステップＳ２１）（図３参照。）。そして、ログイン実行が要求されると（ステップＳ２２：Ｙｅｓ）、ユーザＩＤ及びパスワードが入力されているか否かを判定（ステップＳ２３）し、入力されている場合（ステップＳ２３：Ｙｅｓ）には「認証要求処理」を行ない（ステップＳ２４）、処理を終了する。

【０１２３】

他方、ログイン実行が要求されない場合（ステップＳ２２：Ｎｏ）には、パスワード変更の要求がされたか否かを判定（ステップＳ２５）し、パスワード変更の要求がされた場合（ステップＳ２５：Ｙｅｓ）には「パスワード変更処理」を行ない（ステップＳ２６）、処理を終了する。

【０１２４】

また、ステップＳ２３においてユーザＩＤ及びパスワードが入力されていない場合（ステップＳ２３：Ｎｏ）、及びパスワード変更の要求がされていない場合（ステップＳ２５：Ｎｏ）にも、当該処理を終了する。

【０１２５】

なお、ステップＳ２４の「認証要求処理」及びステップＳ２６の「パスワード変更処理」については、この次に詳細に説明する。

【０１２６】

［３－１－３．パスワード変更処理］

次に、上述したステップＳ２６で実行される「パスワード変更処理」について、図１９のフローチャートを用いて説明する。

【０１２７】

先ず、表示部１６に図１０（Ａ）に図示するような表示画面を表示して、ユーザＩＤ、パスワード、及び新しいパスワードの入力をユーザに指示する（ステップＳ３１）。そして、ユーザがカーソル等によってパスワード変更を選択し、パスワード変更が要求されると（ステップＳ３２：Ｙｅｓ）、制御部１１は、パスワード変更処理要求手段として機能し、ユーザＩＤ及びパスワードが入力されているか否かを判定（ステップＳ３３）し、入力されている場合（ステップＳ３３：Ｙｅｓ）にはサーバ１００に、ユーザＩＤ、パスワード、及び新しいパスワードを通知して、パスワード変更を要求する（ステップＳ３４）。そして、サーバ１００からパスワード変更の結果（パスワード変更完了又はパスワード変更拒否）を受信する。

【０１２８】

ステップＳ３３においてユーザＩＤ及びパスワードが入力されていない場合（ステップＳ３３：Ｎｏ）、及びサーバ１００からパスワード変更拒否を受信した場合（ステップＳ３５）には、エラー処理を行なって（ステップＳ３６）処理を終了する。エラー処理とは、例えば、パスワードの変更ができないことを表示部１６に表示してユーザに提示し、最初の画面表示（例えば、図３参照。）に戻る等の処理である。

【０１２９】

［３－１－４．認証要求処理］

次に、上述したステップＳ２４で実行される「認証要求処理」について、図２０のフローチャートを用いて説明する。

【０１３０】
先ず、制御部１１は、第２分割パスワード生成手段として機能し、ステップＳ２３で入力確認がされたパスワードを所定の分割方法で分割し、ｎ個の分割パスワードを生成する（ステップＳ４０）。続いて、分割番号ｉを１として初期化する（ステップＳ４１）。そして、認証要求したものの、タイムアウトや認証担当のノード装置ではない旨の通知がされ、認証結果を取得できなかった数ｃｏｕｎｔを０として初期化する（ステップＳ４２）。
【０１３１】
次に、制御部１１は第２識別情報生成手段として機能し、分割番号ｉの分割パスワードの認証識別ＩＤを生成する（ステップＳ４３）。具体的には、ユーザＩＤ、分割番号ｉ（ｉは分割数１～３）及び接尾辞（特定文字列ｓａｌｔ：ｓａｌｔ１、ｓａｌｔ２、ｓａｌｔ３、、、、ｓａｌｔ１０）からなる文字列を、ノードＩＤを得るときと共通のハッシュ関数によりハッシュ化して認証識別ＩＤを生成する（図１１（Ａ）参照）。これにより、各分割パスワードについて、ｓａｌｔ１、ｓａｌｔ２、ｓａｌｔ３、、、、ｓａｌｔ１０個の認証ルートノードを順次特定することができる。
【０１３２】
そして、生成した認証識別ＩＤに基づくＤＨＴルーティングにより、分割番号ｉの分割パスワードを認証するノード装置１に対して「認証要求メッセージ」を送信する（ステップＳ４４）。
【０１３３】
続いて、特定されたノード装置からの応答を待ち、所定時間が経過した場合（タイムアウト）或いは、特定されたノード装置１から、認証担当のノード装置でない旨の通知を受信したか否かを判定する（ステップＳ４５）。認証担当のノード装置でない旨の通知とは、「認証要求メッセージ」を受けたノード装置自身が「認証要求メッセージ」にかかる認証識別ＩＤの分割パスワードを記憶していないし、当該メッセージを次に転送すべきノード装置がない場合に、当該ノード装置から通知されるものである。ＤＨＴルーティングによって特定されたノード装置が、認証担当のノード装置である場合には、認証結果が通知されてくる。
【０１３４】
そして、ｓａｌｔのバリエーションが未だあるか否かを判定し（ステップＳ４６）、未だある場合（ステップＳ４６：Ｙｅｓ）には、他のｓａｌｔの分割番号ｉの分割パスワードの認証識別ＩＤを生成し（ステップＳ４７）、ｓａｌｔが異なる１０個の認証識別ＩＤを夫々含む、１０個の「認証要求メッセージ」を送信し終えるまでステップＳ４４～ステップＳ４７の処理を繰り返し行なう。
【０１３５】
全てのｓａｌｔについて、処理が終わっている場合には（ステップＳ４６：Ｎｏ）、分割番号ｉに１加算し（ステップＳ４８）、ｉが分割した数ｎ以下である場合（ステップＳ４９：Ｙｅｓ）には、ステップＳ４２に戻り、次の分割番号の分割パスワードについて同様の処理を行なう。
【０１３６】
そして、制御部１１は認証結果取得手段として機能し、全ての分割番号について１０個の「認証要求メッセージ」を送信し、認証結果を取得し、各分割パスワードについて、取得した認証結果のうち認証ＯＫとする認証結果が所定閾値（Ｔｈ）以上であるか否かを判定する（ステップＳ５０）。認証ＯＫとする認証結果が所定閾値（Ｔｈ）以上である場合（ステップＳ５０：Ｙｅｓ）には、制御部１１は、操作許可手段として機能し、操作制限を解除して（ステップＳ５１）、ユーザによるノード装置１の操作を可能にする。
【０１３７】
他方、取得した認証結果のうち認証ＯＫとする認証結果が所定閾値（Ｔｈ）以上で無い場合（ステップＳ５０：Ｎｏ）、操作制限の解除をせず、ログインできない旨を表示部１６に表示するなどのログイン拒否処理を行ない（ステップＳ５２）、処理を終了する。

【０１３８】
ステップＳ４５で、特定されたノード装置からの応答を待ち、所定時間が経過した場合（タイムアウト）或いは、特定されたノード装置１から、認証担当のノード装置でない旨の通知を受信した場合には、ｃｏｕｎｔを１加算した（ステップＳ６１）後に、制御部１１は判断有効判定手段として機能し、ｃｏｕｎｔが有効閾値（ｃｔｈ）以下であるか否かを判定する（ステップＳ６２）。そして、ｃｏｕｎｔが有効閾値（ｃｔｈ）以下である場合（ステップＳ６２:Ｙｅｓ）には、ステップＳ４６に移行する。
【０１３９】
ｃｏｕｎｔが有効閾値（ｃｔｈ）以下で無い場合（ステップＳ６２:Ｎｏ）には、ノード装置間で認証ができないと判断して、サーバ１００に、ユーザＩＤ及びパスワードを通知して、認証を要求する（ステップＳ６３）。そして、サーバ１００から認証結果を受信し（ステップＳ６４）、認証ＯＫの場合、操作制限を解除してユーザによるノード装置１の操作を可能にし、認証ＮＧの場合、操作制限の解除をせず、ログイン拒否処理を行ない（ステップＳ６５）、処理を終了する。
【０１４０】
［３－１－５．認証関連の各種メッセージ受信時の処理］
次に、上述したステップＳ１３で実行される「認証関連の各種メッセージ受信時の処理」について、図２１のフローチャートを用いて説明する。当該処理は、オーバーレイネットワーク９に含まれる他のノード装置から送信されてきた「認証要求メッセージ」や、サーバ１００から送信された（或いは他のノード装置１から転送された）「分割パスワード記憶要求メッセージ」等を受信したときの処理である。
【０１４１】
先ず、ステップＳ１２で受信したメッセージが「認証要求メッセージ」であるか否かを判定（ステップＳ７０）し、「認証要求メッセージ」であれば（ステップＳ７０：Ｙｅｓ）、自身が認証担当のノード装置（認証ルートノード）であるか否かを判定する（ステップＳ７１）。
【０１４２】
自身が認証担当のノード装置である場合（ステップＳ７１：Ｙｅｓ）（例えば、図７（Ｂ）のノード装置１ｃ、１ｅ、１ｉ）には、「認証処理」を行ない（ステップＳ７２）、処理を終了する。 他方、自身が認証担当のノード装置で無い場合（ステップＳ７１：Ｎｏ）には、「認証要求メッセージ」の転送先が無い場合には、認証担当のノード装置ではない旨を「認証要求メッセージ」の送信元のノード装置１に通知し、「認証要求メッセージ」の転送先があれば、引き続き当該メッセージに含まれる認証識別ＩＤに基づいてメッセージを転送し（ステップＳ７３）、処理を終了する。
【０１４３】
一方、ステップＳ７２で受信したメッセージが「認証要求メッセージ」で無い場合で（ステップＳ７０：Ｎｏ）、受信したメッセージが他のノード装置１から転送された「分割パスワード記憶要求メッセージ」である場合（ステップＳ７３：Ｙｅｓ）には、メッセージの転送先が無ければ、「分割パスワード記憶要求メッセージ」に含まれる認証識別ＩＤと分割パスワードを記憶部１２に対応付けて記憶し、メッセージの転送先があれば、メッセージを転送する（ステップＳ７５）。
【０１４４】
そして、「分割パスワード記憶要求メッセージ」の転送先があるならば、転送した後に処理を終了する。
【０１４５】
受信したメッセージが「分割パスワード記憶要求メッセージ」ではなく（ステップＳ７４：Ｎｏ）、他のノード装置１から転送された「分割パスワード削除要求メッセージ」である場合（ステップＳ７６：Ｙｅｓ）には、「分割パスワード削除要求メッセージ」に含まれる認証識別ＩＤにかかる分割パスワードを記憶している場合には、「分割パスワード削除要求メッセージ」に含まれる認証識別ＩＤと分割パスワードと同一の認証識別ＩＤと

、当該認証識別ＩＤに対応付けて記憶されている分割パスワードを記憶部１２から削除し、「分割パスワード削除要求メッセージ」に含まれる認証識別ＩＤにかかる分割パスワードを記憶していない場合であって、メッセージの転送先があれば、メッセージを転送する（ステップＳ７７）。

【０１４６】

受信したメッセージが「分割パスワード削除要求メッセージ」でも無い場合（ステップＳ７４：Ｎｏ）には、そのまま処理を終了する。「分割パスワード削除要求メッセージ」は、パスワード変更処理が行なわれたときに、古いパスワードを削除するためにサーバ１００から送出されるメッセージである。サーバ１００のパスワード変更処理にて詳述する。

【０１４７】

［３－１－６．認証処理］

次に、上述したステップＳ７２で実行される「認証処理」について、図２２のフローチャートを用いて説明する。

【０１４８】

制御部１１は、認証手段として機能し、「認証要求メッセージ」に含まれる分割パスワードと、記憶部１２に記憶している分割パスワードが一致しているか否かを判定する（ステップＳ８０）。具体的には、記憶部１２に記憶している認証識別ＩＤ（表１参照。）のうち、「認証要求メッセージ」に含まれる認証識別ＩＤと同一の認証識別ＩＤと、対応付けて記憶されている分割パスワードが、「認証要求メッセージ」に含まれる分割パスワードと同じか否かに基づいて判定する。

【０１４９】

そして、制御部１１は、認証結果送信手段として機能し、判定の結果、分割パスワードが一致する場合（ステップＳ８０：Ｙｅｓ）には、認証ＯＫとする認証結果を「認証要求メッセージ」の送信元のノード装置１に通知（ステップＳ８１）し、一致していない場合（ステップＳ８０：Ｎｏ）には、認証ＮＧとする認証結果を「認証要求メッセージ」の送信元のノード装置１に通知（ステップＳ８２）する。「認証要求メッセージ」の送信元のノード装置１への認証結果の通知は、「認証要求メッセージ」に含まれるノード情報を参照すればよい。

【０１５０】

［３－１－７．新規登録要求処理］

続いて、ユーザが最初にユーザＩＤとパスワードをサーバ１００に登録する処理について説明する。

【０１５１】

この処理は、ユーザ管理の観点から、ユーザが、コンテンツ配信システムＳを利用するためにノード装置１を購入したときに、購入店舗にあるユーザ登録用装置２００が、サーバ１００にアクセスして登録したり、ユーザがコンテンツ配信システムの利用料金の支払いを適式に行なった後に、ユーザが所有するノード装置１から、サーバ１００にアクセスして登録する際の、ユーザ登録用装置２００又はノード装置１にて行なわれる処理である。

【０１５２】

本実施形態では、ユーザ登録用装置２００で実行される「新規登録要求処理」について、図２３のフローチャートを用いて説明する。

【０１５３】

先ず、表示部２０３に、ユーザＩＤ及びパスワードの入力を促す表示画面を表示して、ユーザに入力を指示する（ステップＳ３１）。次に、制御部２０１は、ユーザＩＤ及びパスワードが入力されているか否かを判定（ステップＳ９１）し、入力されている場合にはサーバ１００に、ユーザＩＤ及びパスワードを通知して、新規登録を要求する（ステップＳ９１：Ｙｅｓ、ステップＳ９２）。

【０１５４】

そして、サーバ１００からの登録結果報告を受信し（ステップＳ９３）、登録結果を表示部２０３に表示して処理を終了する。

【０１５５】

サーバ１００からの登録結果報告とは、登録完了報告又は登録拒否報告である。サーバ１００では、ユーザＩＤやパスワードが既に登録済みのものと同じである場合には、同一ユーザＩＤの二重登録となり好ましくないので、登録拒否を行なう。詳細は次に説明するサーバ１００の「新規登録処理」にて説明する。

【０１５６】

［３－２．サーバの処理］

［３－２－１．メイン処理］

続いて、図２４を用いてサーバ１００にて実行されるメイン処理について説明する。この処理は、管理処理プログラムが制御部１０１の制御に基づいて実行され、サーバ１００の電源がオンとされることにより開始する。

【０１５７】

先ず、制御部１０１は、新規登録要求がされたか否かを判定（ステップ１１０）し、新規登録要求がされた場合（ステップＳ１１０：Ｙｅｓ）には「新規登録処理」を行ない（ステップＳ１１１）、新規登録要求がされない場合（ステップＳ１１０：Ｎｏ）には、認証要求がされたか否かを判定（ステップ１１２）する。

【０１５８】

そして、認証要求がされた場合（ステップＳ１１２：Ｙｅｓ）には「認証処理」を行ない（ステップＳ１１３）、認証要求がされない場合（ステップＳ１１２：Ｎｏ）には、パスワードの変更要求がされたか否かを判定（ステップ１１４）する。

【０１５９】

そして、パスワードの変更要求がされた場合（ステップＳ１１４：Ｙｅｓ）には「再登録処理」を行ない（ステップＳ１１５）、パスワードの変更要求がされない場合（ステップＳ１１４：Ｎｏ）には、ユーザ削除要求がされたか否かを判定（ステップ１１６）する。このユーザ削除要求とは、ユーザがシステムの利用料金の支払いを滞納したときなど、図示しない課金管理をする課金サーバ等から要求されるものである。そして、ユーザ削除要求がされた場合（ステップＳ１１６：Ｙｅｓ）には、「削除処理」を行ない（ステップＳ１１７）、ユーザ削除要求がされない場合（ステップＳ１１６：Ｎｏ）には、サーバ１００自身の電源がオフとされたか否かを判定（ステップ１１８）する。

【０１６０】

電源がオフとされた場合（ステップＳ１１８：Ｙｅｓ）には処理を終了し、電源がオフとされていない場合（ステップＳ１１８：Ｎｏ）には、その他の処理があれば実行する（ステップＳ１１９）。

【０１６１】

そして、上記ステップＳ１１１、Ｓ１１３、Ｓ１１５、Ｓ１１７及びＳ１１９の処理を終えると、ステップＳ１１０の処理に戻り、ステップＳ１１８にて電源がオフと判定されるまで、ステップＳ１１０～Ｓ１１９の処理を繰り返し行なう。

【０１６２】

［３－２－２．新規登録処理］

次に、上述したステップＳ１１１で実行される「新規登録処理」について図２５のフローチャートを用いて説明する。

【０１６３】

先ず、ユーザ登録用装置２００から送信されてきたユーザＩＤ及びパスワードが利用可能か否かを判定する（ステップＳ１３０）。上述したように、ユーザＩＤやパスワードが既に登録済みのものと同じである場合には、同一ユーザＩＤの二重登録となり好ましくないので、利用できない。また、パスワードが規定範囲の文字（キャラクタ）数で無い場合にも、利用できないものとして判定する。

【０１６４】

ユーザＩＤ及びパスワードが利用可能であると判定された場合（ステップＳ１３０：Ｙｅｓ）には、記憶部１０２にユーザＩＤ及びパスワードを対応付けて記憶する（表２参照。）（ステップＳ１３１）。次に、制御部１０１は第１分割パスワード生成手段として機能し、パスワードを分割してｎ個の分割パスワードを生成する（ステップＳ１３２）。続いて、分割番号ｉを１として初期化する（ステップＳ１３３）。

【０１６５】

そして、制御部１０１は第１識別情報生成手段、認証処理担当要求手段として機能し、分割番号ｉの分割パスワードの認証識別ＩＤを生成（ステップＳ１３４）する。具体的には、各ノード装置にて認証識別ＩＤを生成する際と同様に、ユーザＩＤ、分割番号ｉ（ｉは分割数１～３）及び接尾辞（特定文字列ｓａｌｔ：ｓａｌｔ１、ｓａｌｔ２、ｓａｌｔ３、、、、ｓａｌｔ１０）からなる文字列を、ノードＩＤを得るときと共通のハッシュ関数によりハッシュ化して認証識別ＩＤを生成する（図１１（Ａ）参照）。これにより、各分割パスワードについて、ｓａｌｔ１、ｓａｌｔ２、ｓａｌｔ３、、、、ｓａｌｔ１０個の認証ルートノードを順次特定することができる。

【０１６６】

そして、生成した認証識別ＩＤに基づくＤＨＴルーティングにより、分割番号ｉの分割パスワードを認証すべきノード装置（認証ルートノード）に対して「分割パスワード記憶要求メッセージ」を送信する（ステップＳ１３５）。

【０１６７】

そして、ｓａｌｔのバリエーションが未だあるか否かを判定し（ステップＳ１３７）、未だある場合（ステップＳ１３７：Ｙｅｓ）には、他のｓａｌｔの分割番号ｉの分割パスワードの認証識別ＩＤを生成し（ステップＳ１３６）、ｓａｌｔが異なる１０個の認証識別ＩＤを夫々含む、１０個の「分割パスワード記憶要求メッセージ」を送信し終えるまでステップＳ１３４～ステップＳ１３７の処理を繰り返し行なう。

【０１６８】

全てのｓａｌｔについて、処理が終わっている場合には（ステップＳ１３７：Ｎｏ）、分割番号ｉに１を加算し（ステップＳ１３８）、ｉが分割した数ｎ以下である場合には、ステップＳ１３４に戻り、次の分割番号の分割パスワードについて同様の処理を行なう（ステップＳ１３９：Ｙｅｓ）。

【０１６９】

ｉが分割した数ｎ以下で無い場合（ステップＳ１３９：Ｎｏ）は、全ての分割パスワードの分散記憶が完了しているので、ユーザ登録用装置２００に登録完了報告を通知（ステップＳ１４０）して処理を終了する。

【０１７０】

一方、ステップＳ１３０において、ユーザ登録用装置２００から送信されてきたユーザＩＤ及びパスワードが利用可能で無い場合（ステップＳ１３０：Ｎｏ）には、ユーザ登録用装置２００に登録拒否報告を通知（ステップＳ１４１）して処理を終了する。

【０１７１】

［３－２－３．認証処理］

次に、上述したステップＳ１１３で実行される「認証処理」について図２６のフローチャートを用いて説明する。

【０１７２】

先ず、認証要求をしてきたノード装置１から送信されたユーザＩＤが、記憶部１０２に登録されているユーザであるか否かを判定する（ステップＳ１５０）。

【０１７３】

登録されているユーザである場合（ステップＳ１５０：Ｙｅｓ）には、制御部１０１は認証手段として機能し、送信されてきたパスワードと、記憶部１０２に記憶しているパスワードが一致しているか否かを判定する（ステップＳ１５１）。具体的には、記憶部１０２に記憶しているユーザＩＤのうち、送信されてきたユーザＩＤと、同一のユーザＩＤに、対応付けて記憶されているパスワードが、送信されてきたパスワードと同じか否かに基

づいて判定する。

【０１７４】

判定の結果、パスワードが一致する場合（ステップＳ１５１：Ｙｅｓ）には、ユーザＩＤとパスワードに問題はないので、再度、分割パスワードを複数のノード装置に分散して記憶させ直す（ステップＳ１５２～ステップＳ１５９）。再度記憶させ直す処理（ステップＳ１５２～ステップＳ１５９）は、上述した「新規登録処理」のステップＳ１３２～ステップＳ１３９と同様の処理なので説明を省略する。

【０１７５】

ステップＳ１５９にて、全ての分割番号について１０個の「分割パスワード記憶要求メッセージ」を送信したことを確認した後（ステップＳ１５９：Ｎｏ）に、制御部１０１は認証結果送信手段として機能し、認証ＯＫとする認証結果を認証要求元のノード装置１に通知（ステップＳ１６０）して処理を終了する。

【０１７６】

一方、登録されているユーザで無い場合（ステップＳ１５０：Ｎｏ）、又はパスワードが一致しない場合（ステップＳ１５１：Ｎｏ）には、制御部１０１は認証結果送信手段として機能し、認証ＮＧとする認証結果を認証要求元のノード装置１に通知（ステップＳ１６１）して処理を終了する。

【０１７７】

［３－２－４．再登録処理］

次に、上述したステップＳ１１５で実行される「再登録処理」について図２７のフローチャートを用いて説明する。

【０１７８】

先ず、パスワードの変更要求をしてきたノード装置１から送信されたユーザＩＤが、記憶部１０２に登録されているユーザであるか否かを判定する（ステップＳ１７０）。

【０１７９】

登録されているユーザである場合（ステップＳ１７０：Ｙｅｓ）には、送信されてきたパスワードと、記憶部１０２に記憶しているパスワードが一致しているか否かを判定する（ステップＳ１７１）。具体的には、記憶部１０２に記憶しているユーザＩＤのうち、送信されてきたユーザＩＤと、同一のユーザＩＤに、対応付けて記憶されているパスワードが、送信されてきたパスワードと同じか否かに基づいて判定する。

【０１８０】

判定の結果、パスワードが一致する場合（ステップＳ１７１：Ｙｅｓ）には、記憶部１０２のパスワードを、新たなパスワードに書き換えて更新する（ステップＳ１７２）。

【０１８１】

以降、新しいパスワードの分割パスワードを複数のノード装置に記憶させる処理（ステップＳ１７３～Ｓ１８０）は、上述した「新規登録処理」のステップＳ１３２～ステップＳ１３９と同様の処理なので説明を省略する。

【０１８２】

ステップＳ１８０にて、全ての分割番号について１０個の「分割パスワード記憶要求メッセージ」を送信したことを確認した後（ステップＳ１８０：Ｎｏ）に、パスワード変更完了をパスワード変更要求元のノード装置１に通知（ステップＳ１８１）して処理を終了する。

【０１８３】

一方、登録されているユーザで無い場合（ステップＳ１７０：Ｎｏ）、又はパスワードが一致しない場合（ステップＳ１７１：Ｎｏ）には、パスワード変更拒否をパスワード変更要求元のノード装置１に通知（ステップＳ１８２）して処理を終了する。

【０１８４】

ステップＳ１７２にて記憶部１０２のパスワードを新たなパスワードに書き換えて更新する際に、変更前の（古い）パスワードにかかる分割パスワードの各認証ルートノードに対して分割パスワードの削除を指示するために、分割パスワード記憶要求メッセージを送

信したときと同様にして、ｎ個の分割パスワードと、認証識別ＩＤを生成し、これらを含む「分割パスワード削除要求メッセージ」を各認証ルートノードに対して送信する。具体的なメッセージ送信処理は「３－２－５.削除処理」と同様であるので、ここでの説明は省略する。この「分割パスワード削除要求メッセージ」は、変更前の分割パスワードが認証ルートノードに記憶された際と同様に、認証識別ＩＤをキーとするルーティングによって各ノード装置間を転送されるので、必ず認証ルートノードに辿りつくこととなる。そして、このメッセージを受信した各ノード装置は、自身の記憶部１２に該メッセージに含まれる認証識別ＩＤと同じ認証識別ＩＤが記憶されているか否かを判断し、記憶されていれば（つまり、自身が認証担当のノード装置）、当該認証識別ＩＤと分割パスワードの組を記憶部１２から削除し、記憶されていない場合には、（メッセージの転送先があれば）当該メッセージを転送するよう構成される。

【０１８５】

［３－２－５．削除処理］

次に、上述したステップＳ１１７で実行される「削除処理」について図２８のフローチャートを用いて説明する。

【０１８６】

先ず、ステップＳ１１６にて図示しない課金サーバ等から送信された削除対象のユーザＩＤが、記憶部１０２に登録されているユーザであるか否かを判定する（ステップＳ１９０）。登録されているユーザである場合（ステップＳ１９０：Ｙｅｓ）には、送信された削除対象のユーザＩＤと、同一のユーザＩＤに対応付けて記憶されているパスワードを分割し、ｎ個の分割パスワードを生成する（ステップＳ１９１）。

【０１８７】

当該分割パスワードを記憶しているノード装置に、当該分割パスワードを削除するよう要求する「分割パスワード削除要求メッセージ」の送信処理（ステップＳ１９２～１９９）は、上述した「新規登録処理」のステップＳ１３３～ステップＳ１３９にて説明した、「分割パスワード記憶要求メッセージ」の送信処理と同様の処理であるので説明を省略する。

【０１８８】

「分割パスワード削除要求メッセージ」は、「分割パスワード記憶要求メッセージ」と同じ認証識別ＩＤをキーとするルーティングにより、ノード装置を特定するので、分割パスワードを記憶するノード装置（認証ルートノード）に対して、削除要求を行なうことができるので、削除すべき分割パスワードを確実に削除することができる。

【０１８９】

そして、ステップＳ１９９にて、全ての分割番号について１０個の「分割パスワード削除要求メッセージ」を送信したことを確認した後（ステップＳ１９９：Ｎｏ）に、自身の記憶部１０２からも、削除要求対象のユーザＩＤとパスワードを削除（ステップＳ２００）して、課金サーバ等に削除完了を通知（ステップＳ２０１）して処理を終了する。

【０１９０】

一方、ステップＳ１９０の判定で登録済みのユーザで無いと判定された場合（ステップＳ１９０：Ｎｏ）には、課金サーバ等に削除不能を通知（ステップＳ２０２）して処理を終了する。

【０１９１】

以上説明した実施形態によれば、ユーザによるノード装置１の操作制限を解除するための認証処理を、従来の認証処理を行なう認証サーバを用いずとも、複数のノード装置１で行なうことができる。更にパスワードを複数の分割パスワードに分割して、それぞれ異なるノード装置１にて認証を行なうので、セキュリティ性の高い認証を行なうことができる。

【０１９２】

また、認証識別ＩＤ及びパスワードに基づいてユーザ認証を行なうので、ユーザは、自己が所有するノード装置１でなく、例えば友人宅のノード装置であっても（換言すれば、

オーバーレイネットワーク９に含まれる何れのノード装置１でも、）ユーザＩＤ及びパスワードを入力してユーザ認証が正当に行なわれれば、操作制限を解除して、コンテンツ検索やコンテンツ視聴等システムを利用することができる。

【０１９３】

なお、サーバ１００からノード装置１へ送信される「分割パスワード記憶要求メッセージ」に、ユーザＩＤ及び分割パスワードを含み、認証ルートノードとなった各ノード装置では、表３に示すようにユーザＩＤ及び分割パスワードを対応付けて記憶するよう構成することもできる。

【０１９４】

【表３】

ユーザＩＤ	分割パスワード
ｕｓｅｒ１	Ｐ
ｕｓｅｒ２	Ａ
ｕｓｅｒ３	ＴＲ
…	…

ユーザ認証を行なう際には、ユーザが操作するユーザ認証の要求元のノード装置から、「認証要求メッセージ」にユーザＩＤを含んで送信することにより、これを受けた認証ルートノードでは、「認証要求メッセージ」に含まれるユーザＩＤに基づいて、対応する分割パスワードと、メッセージに含まれる分割パスワードが一致するか否かにより、分割パスワードの認証を行なえばよい。このように、ユーザＩＤと分割パスワードを認証ルートノードに記憶させて、ユーザＩＤに基づいて分割パスワードの認証処理を行なうこともできるが、本実施形態のように、認証識別ＩＤと分割パスワードを認証ルートノードに記憶させて（表１参照）、認証識別ＩＤに基づいてユーザ認証を行なうよう構成すれば、ユーザＩＤ、パスワード及び分割パスワードを他のノード装置に知られることがないので、よりセキュリティ性の高い認証を行なうことができる。

【０１９５】

また、本実施形態では、１の分割パスワードについての認証を、複数のノード装置で行なうよう構成したので、一部の認証担当のノード装置に障害が発生した場合であっても、ユーザの認証を行なうことができる。

【０１９６】

更に、サーバ１００にユーザＩＤとパスワードを記憶させるよう構成し、ノード装置１間で各分割パスワードの認証が適式に行なわれるかを有効閾値（ｃｔｈ）を設定して判断可能に構成したので、ノード装置１間で各分割パスワードの認証が適式に行なわれないと判断した場合には、サーバ１００にユーザＩＤとパスワードを送信することで、サーバ１００にて認証処理を行なうこともできる。

【０１９７】

更に、サーバ１００にてパスワードを変更可能に構成したので、大規模なシステム障害が発生したときなど、認証担当のノード装置１が全てダウンした場合であっても、パスワードの変更等を行なって、再度、複数のノード装置１に分割パスワードを記憶させて認証担当となるよう要求し、新たなパスワードの認証担当のノード装置１を迅速に設定することができる。

【０１９８】

更に、１の分割パスワードについて、複数のノード装置１で認証を行なうよう構成した場合には、該１の分割パスワードについて正当であるとの認証を受けたものと判断するための、認証ＯＫの数を適宜変更可能な所定閾値（Ｔｈ）で判断できるようにしたので、シ

ステムの脆弱性を考慮して、所望の認証の厳密性に応じて適宜設定できる。例えばノード装置１の工場出荷時や、店舗にて購入する際にシステムの管理者によって定められた所定閾値（Ｔｈ）が予め設定されているものとする。

【０１９９】

なお、上述した実施形態では、分割パスワードについて正当であるとの認証を受けたものと判断するための、認証ＯＫの所定閾値（Ｔｈ）を、送出した「認証要求メッセージ」の半数（生成した認証識別ＩＤの所定数の半数）である“５つ”としたが、適宜変更可能である。例えば、送出した「認証要求メッセージ」の数（生成した認証識別ＩＤの所定数）にしてもよい。また、所定閾値（Ｔｈ）を取得した認証結果の半数とすれば、取得した認証結果Ｒに認証ＮＧが１つも無い場合にのみ、正当であるとの認証を受けたものと判断することができる。更に、取得した認証結果Ｒの半数とすることもできるし、或いは、所定閾値（Ｔｈ）を１として、１つでも認証ＯＫがあれば、正当であるとの認証を受けたとするよう構成することもできる。

【０２００】

また、分割パスワードを記憶させる際や、分割パスワードの認証を要求する際に、認証識別ＩＤを分割パスワードと共に各メッセージに含み、認証担当のノード装置１を特定する処理と、特定されたノード装置１に上記認証のための情報を送信する処理とを、一緒に行なうよう構成したが、本発明はこのような構成に限定されるものではなく、例えば、認証識別ＩＤに基づくルーティングによって分割パスワードを認証するノード装置１を特定した後に、当該特定されたノード装置からの応答を受けて、認証識別ＩＤ及び分割パスワードを当該認証担当のノード装置１に送信するよう構成してもよい。

【０２０１】

また、上記実施形態においては、ＤＨＴを利用したアルゴリズムによって構築されたオーバーレイネットワーク９を前提として説明したが、本発明はこれに限定されるものではなく、その他のコンピュータネットワークシステムに対しても適用可能である。

【図面の簡単な説明】

【０２０２】

【図１】本実施形態に係るコンテンツ配信システムにおける各ノード装置の接続態様の一例を示す図である。

【図２】ＤＨＴのＩＤ空間の一例を示す概念図である。

【図３】ノード装置１のユーザＩＤ及びパスワード入力画面例である。

【図４】ＤＨＴのＩＤ空間におけるノードＩＤ及び認証識別ＩＤの一例を示す概念図である。

【図５】ＤＨＴによってルーティングテーブルが作成される様子の一例を示す図である。

【図６】（Ａ）レベル１のテーブルの一例である。（Ｂ）レベル２のテーブルの一例である。（Ｃ）レベル３のテーブルの一例である。（Ｄ）完成したルーティングテーブルの一例である。

【図７】（Ａ）「分割パスワード記憶要求メッセージ」の説明図、（Ｂ）ノード装置１が分割パスワードの認証担当となる際の様子をＤＨＴのＩＤ空間にて示した概念図である。

【図８】（Ａ）「認証要求メッセージ」の説明図、（Ｂ）ノード装置１ｆが認証要求をする際の様子をＤＨＴのＩＤ空間にて示した概念図である。

【図９】ノード装置１ｆが認証結果Ｒを取得する様子を示した概念図である。

【図１０】（Ａ）パスワード変更の際の入力画面例、（Ｂ）パスワード変更の様子を示す説明図である。

【図１１】（Ａ）応用実施例における認証識別ＩＤの説明図、（Ｂ）応用実施例における「認証要求メッセージ」の説明図である。

【図１２】分割パスワード“Ｐ”の認証結果Ｒを１０台の認証担当のノード装置１から受ける際の様子をＤＨＴのＩＤ空間にて示した概念図である。

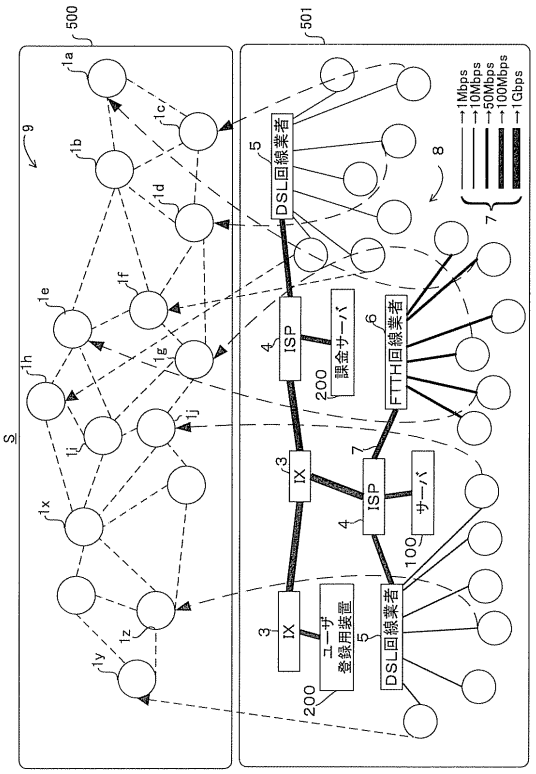
【図１３】各分割パスワードの認証結果Ｒの一例を示す説明図である。

【図１４】ノード装置１の概要構成例を示すブロック図である。

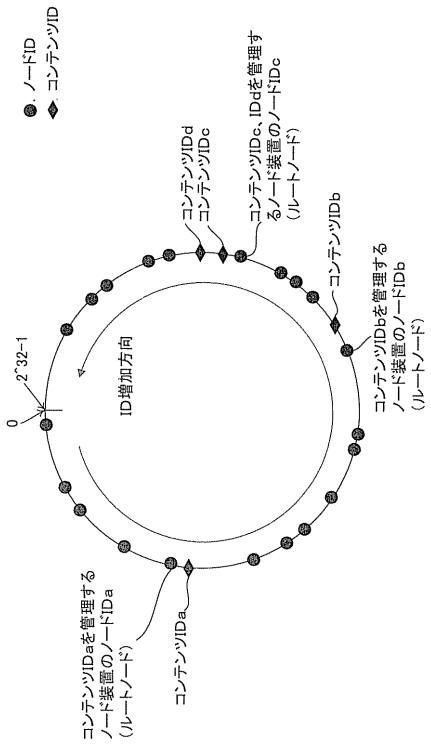
【図１５】サーバ１００の概要構成例を示すブロック図である。
【図１６】ユーザ登録用装置２００の概要構成例を示すブロック図である。
【図１７】ノード装置１におけるメイン処理の一例を示すフローチャートである。
【図１８】ノード装置１における「ログイン関連処理」の一例を示すフローチャートである。
【図１９】ノード装置１における「パスワード変更処理」の一例を示すフローチャートである。
【図２０】ノード装置１における「認証要求処理」の一例を示すフローチャートである。
【図２１】ノード装置１における「認証関連の各種メッセージ受信時の処理」の一例を示すフローチャートである。
【図２２】ノード装置１における「認証処理」の一例を示すフローチャートである。
【図２３】ユーザ登録用装置２００における「新規登録要求処理」にの一例を示すフローチャートである。
【図２４】サーバ１００におけるメイン処理の一例を示すフローチャートである。
【図２５】サーバ１００における「新規登録処理」の一例を示すフローチャートである。
【図２６】サーバ１００における「認証処理」の一例を示すフローチャートである。
【図２７】サーバ１００における「再登録処理」の一例を示すフローチャートである。
【図２８】サーバ１００における「削除処理」の一例を示すフローチャートである。
【符号の説明】
【０２０３】
１　ノード装置
３　ＩＸ
４　ＩＳＰ
５　ＤＳＬ回線事業者の装置
６　ＦＴＴＨ（Fiber To The Home）回線事業者の装置
７　通信回線
８　ネットワーク
９　オーバーレイネットワーク
１１　制御部
１２　記憶部
１３　バッファメモリ
１４　デコーダ部
１５　映像処理部
１６　表示部
１７　音声処理部
１８　スピーカ
２０　通信部
２１　入力部
２２　バス
１００　サーバ
１０１　制御部
１０２　記憶部
１０３　通信部
１０４　入力部
１０５　バス
２００　ユーザ登録用装置
２０１　制御部
２０２　記憶部
２０３　表示部
２０４　通信部

２０５　入力部
２０６　バス
Ｓ　コンテンツ配信システム
Ｒ　認証結果
ｃｔｈ　有効閾値
Ｔｈ　所定閾値

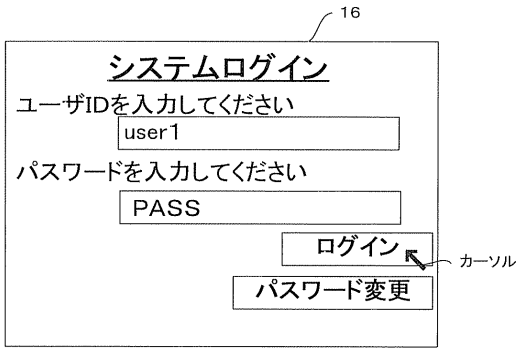
【図１】



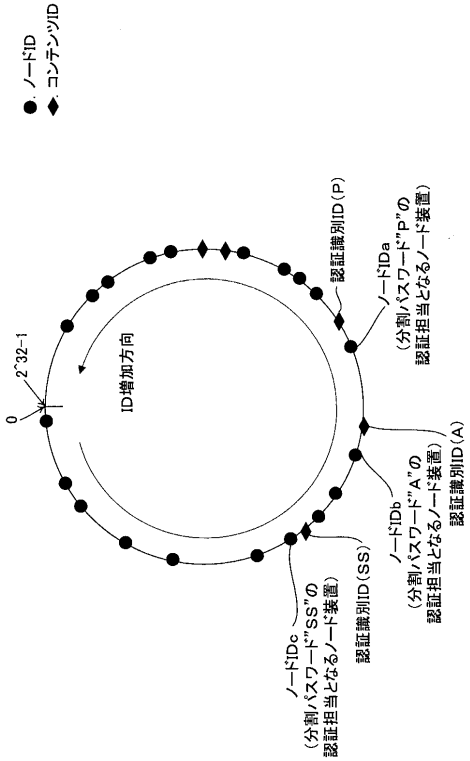
【図２】



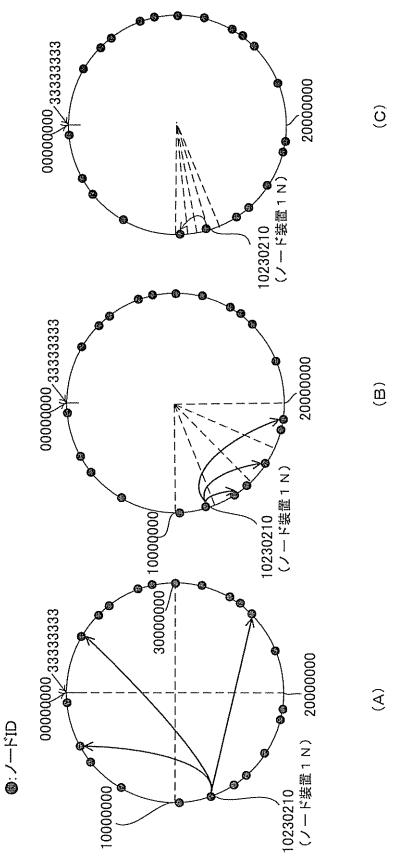
【図３】



【図４】



【図５】



【図６】

	各レベルの注目桁0	各レベルの注目桁1	各レベルの注目桁2	各レベルの注目桁3
レベル1	01300000	10230210	22031000	32201010
	IPアドレス0	-	IPアドレス2	IPアドレス3
レベル2	10230210	11320101	12020230	13210001
	-	IPアドレス4	IPアドレス5	IPアドレス6
レベル3	10000302	-	10230210	-
	IPアドレス7	-	-	10230210
レベル4	-	-	-	-
レベル5	10230210	-	-	-
	-	-	-	-
レベル6	-	-	10230210	-
レベル7	-	10230210	-	-
	-	-	-	-
レベル8	10230210	-	-	-
	-	-	-	-

(D)

01300000	10230210	22031000	32201010
IPアドレス0	-	IPアドレス2	IPアドレス3

(A)

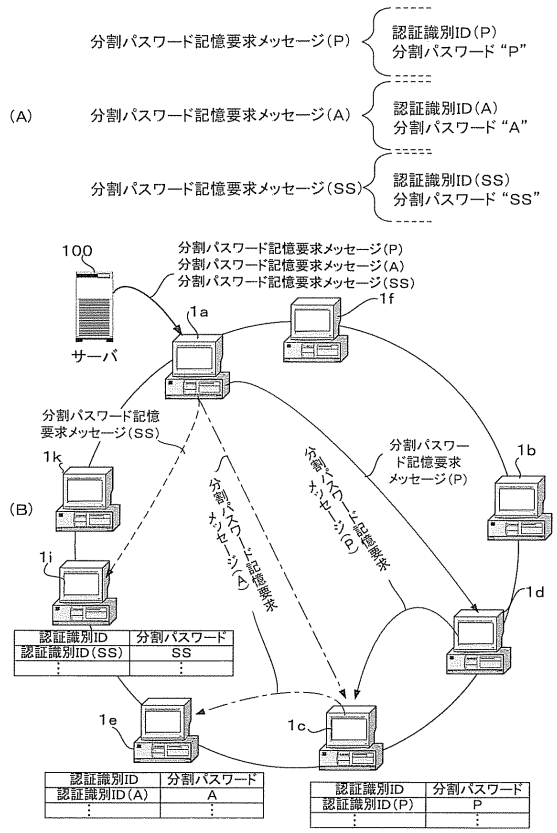
10230210	11320101	12020230	13210001
-	IPアドレス4	IPアドレス5	IPアドレス6

(B)

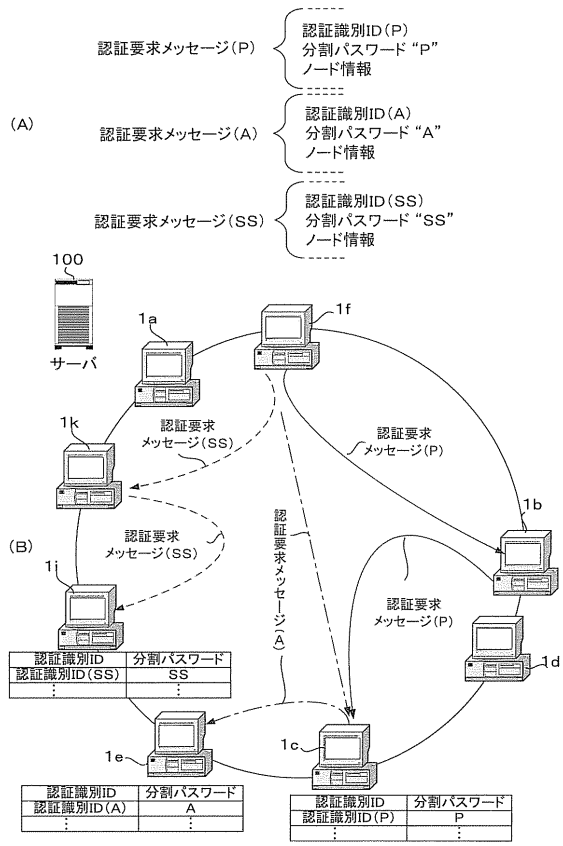
10000302	-	10230210	-
IPアドレス7	-	-	-

(C)

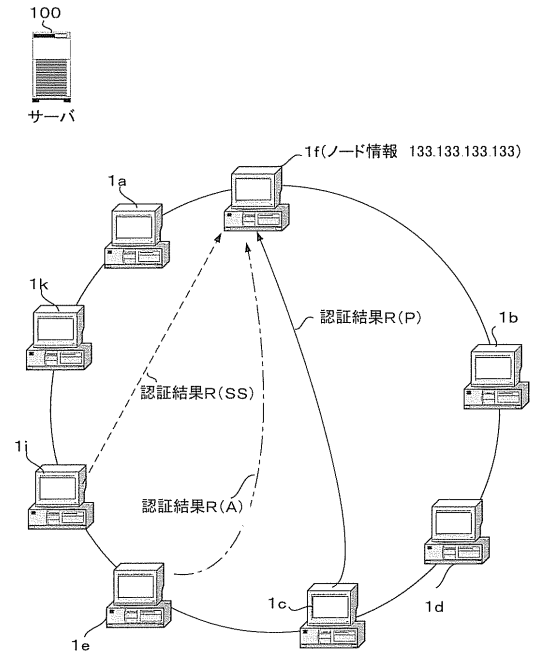
【図７】


分割パスワード記憶要求メッセージ(P)
認証識別ID(P)
分割パスワード “P”
(A)
分割パスワード記憶要求メッセージ(A)
認証識別ID(A)
分割パスワード “A”
分割パスワード記憶要求メッセージ(SS)
認証識別ID(SS)
分割パスワード “SS”
100
サーバ
1a
1f
1b
1d
1e
1c
(B)
1k
1j
分割パスワード記憶要求メッセージ(SS)
分割パスワード記憶要求メッセージ(P)
分割パスワード記憶要求メッセージ(A)
認証識別ID
分割パスワード
認証識別ID(SS)
SS
認証識別ID(A)
A
認証識別ID(P)
P

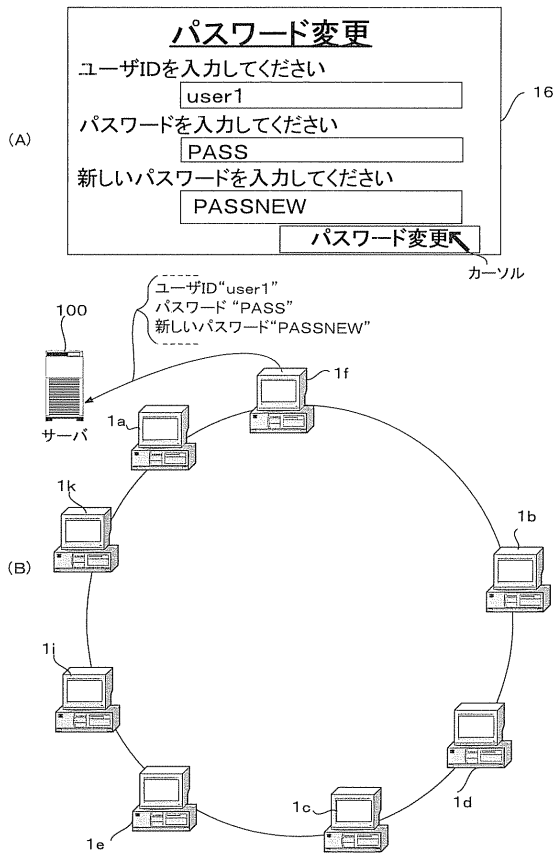
【図８】


認証要求メッセージ(P)
認証識別ID(P)
分割パスワード “P”
ノード情報
(A)
認証要求メッセージ(A)
認証識別ID(A)
分割パスワード “A”
ノード情報
認証要求メッセージ(SS)
認証識別ID(SS)
分割パスワード “SS”
ノード情報
100
サーバ
1a
1f
1b
1d
1e
1c
(B)
1k
1j
認証要求メッセージ(SS)
認証要求メッセージ(P)
認証要求メッセージ(A)
認証識別ID
分割パスワード
認証識別ID(SS)
SS
認証識別ID(A)
A
認証識別ID(P)
P

【図９】


100
サーバ
1f(ノード情報 133.133.133.133)
1a
1k
1b
認証結果R(P)
認証結果R(SS)
1j
認証結果R(A)
1c
1d
1e

【図１０】


パスワード変更
ユーザIDを入力してください
user1
パスワードを入力してください
PASS
新しいパスワードを入力してください
PASSNEW
パスワード変更
16
(A)
カーソル
ユーザID“user1”
パスワード “PASS”
新しいパスワード“PASSNEW”
100
サーバ
1f
1a
1k
1b
(B)
1j
1c
1d
1e

【図１１】

(A)

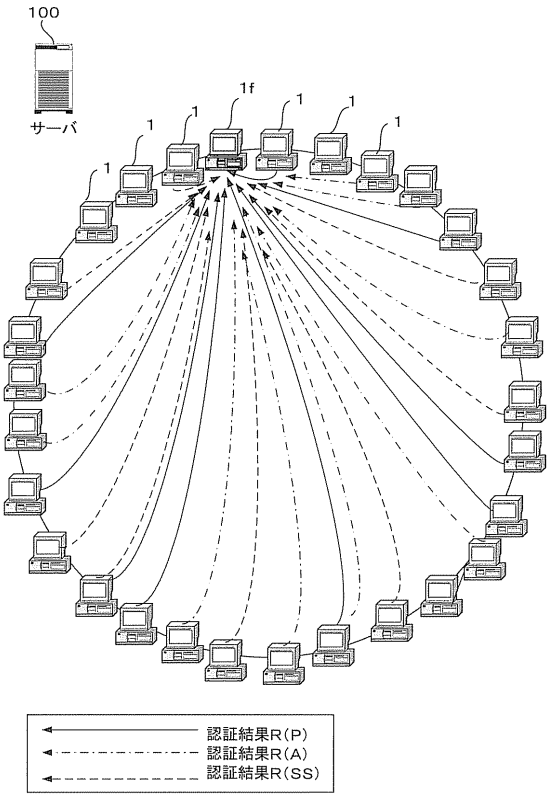
分割パスワード“SS”の認証識別IDの種類
分割パスワード“A”の認証識別IDの種類

分割パスワード“P”の認証識別IDの種類	
認証識別ID(P)(salt1)	ユーザID+分割番号+salt1
認証識別ID(P)(salt2)	ユーザID+分割番号+salt2
認証識別ID(P)(salt3)	ユーザID+分割番号+salt3
認証識別ID(P)(salt4)	ユーザID+分割番号+salt4
認証識別ID(P)(salt5)	ユーザID+分割番号+salt5
認証識別ID(P)(salt6)	ユーザID+分割番号+salt6
認証識別ID(P)(salt7)	ユーザID+分割番号+salt7
認証識別ID(P)(salt8)	ユーザID+分割番号+salt8
認証識別ID(P)(salt9)	ユーザID+分割番号+salt9
認証識別ID(P)(salt10)	ユーザID+分割番号+salt10

(B)

認証要求メッセージ(P)(sallt1)	認証識別ID(P)(sallt1) 分割パスワード“P” ノード情報
認証要求メッセージ(P)(sallt10)	認証識別ID(P)(sallt10) 分割パスワード“P” ノード情報
認証要求メッセージ(A)(sallt1)	認証識別ID(A)(sallt1) 分割パスワード“A” ノード情報
認証要求メッセージ(A)(sallt10)	認証識別ID(A)(sallt10) 分割パスワード“A” ノード情報
認証要求メッセージ(SS)(sallt1)	認証識別ID(SS)(sallt1) 分割パスワード“SS” ノード情報
認証要求メッセージ(SS)(sallt10)	認証識別ID(SS)(sallt10) 分割パスワード“SS” ノード情報

【図１２】



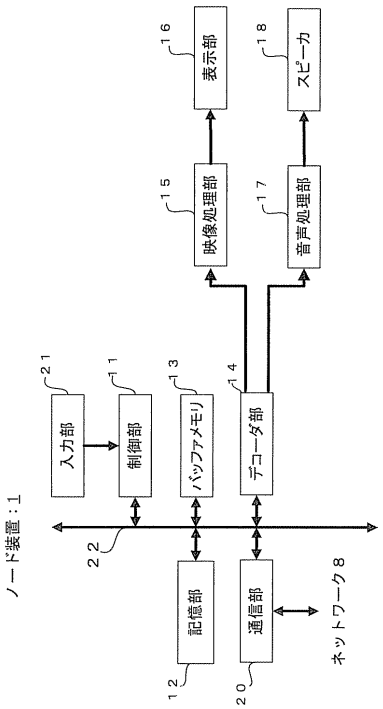
【図１３】

分割パスワード“P”の認証結果	
認証要求メッセージ(P)(salt1)	OK
認証要求メッセージ(P)(salt2)	OK
認証要求メッセージ(P)(salt3)	OK
認証要求メッセージ(P)(salt4)	OK
認証要求メッセージ(P)(salt5)	OK
認証要求メッセージ(P)(salt6)	OK
認証要求メッセージ(P)(salt7)	OK
認証要求メッセージ(P)(salt8)	NG
認証要求メッセージ(P)(salt9)	OK
認証要求メッセージ(P)(salt10)	OK

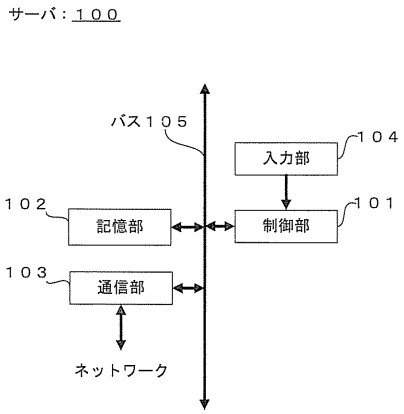
分割パスワード“A”の認証結果	
認証要求メッセージ(A)(salt1)	OK
認証要求メッセージ(A)(salt2)	OK
認証要求メッセージ(A)(salt3)	OK
認証要求メッセージ(A)(salt4)	OK
認証要求メッセージ(A)(salt5)	OK
認証要求メッセージ(A)(salt6)	OK
認証要求メッセージ(A)(salt7)	応答無し
認証要求メッセージ(A)(salt8)	OK
認証要求メッセージ(A)(salt9)	OK
認証要求メッセージ(A)(salt10)	OK

分割パスワード“SS”の認証結果	
認証要求メッセージ(SS)(salt1)	NG
認証要求メッセージ(SS)(salt2)	NG
認証要求メッセージ(SS)(salt3)	NG
認証要求メッセージ(SS)(salt4)	OK
認証要求メッセージ(SS)(salt5)	OK
認証要求メッセージ(SS)(salt6)	OK
認証要求メッセージ(SS)(salt7)	NG
認証要求メッセージ(SS)(salt8)	OK
認証要求メッセージ(SS)(salt9)	OK
認証要求メッセージ(SS)(salt10)	OK

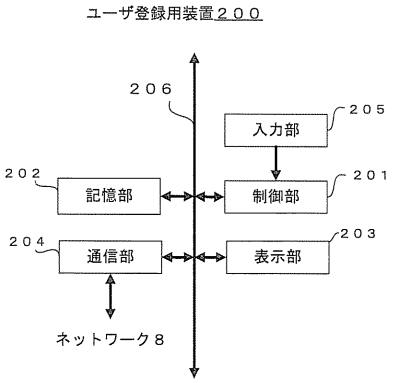
【図１４】



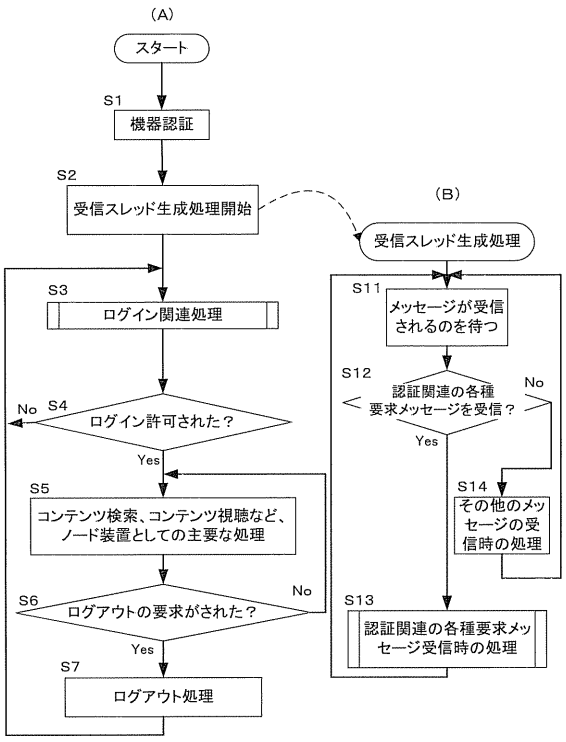
【図１５】



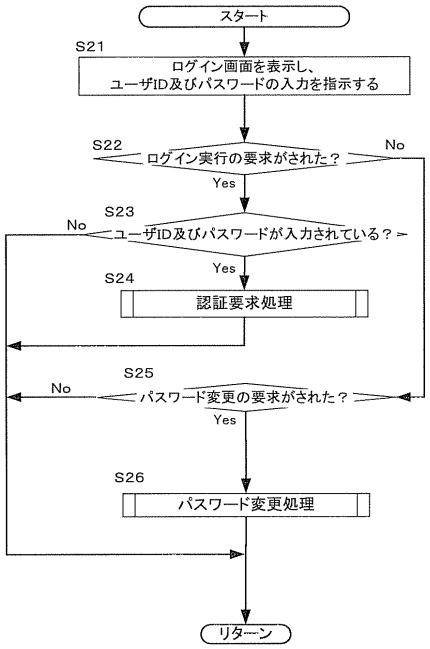
【図１６】



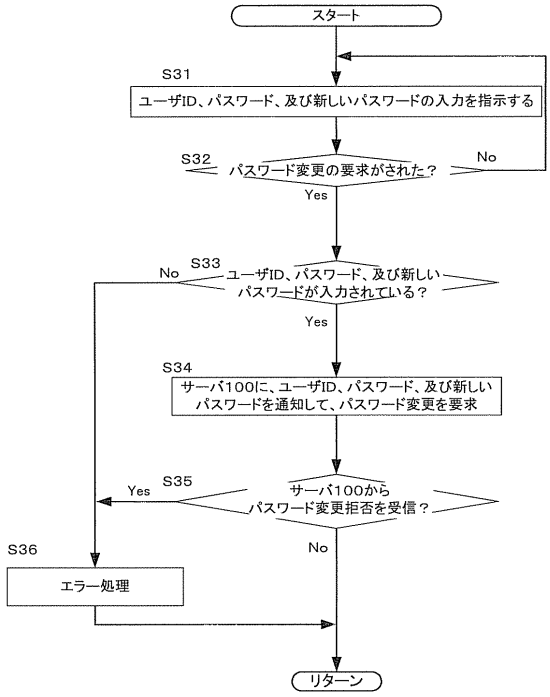
【図１７】



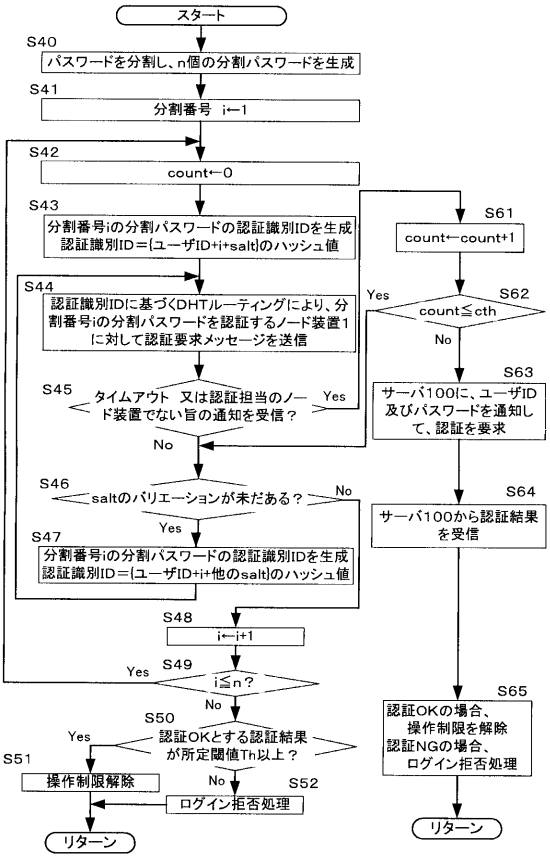
【図１８】



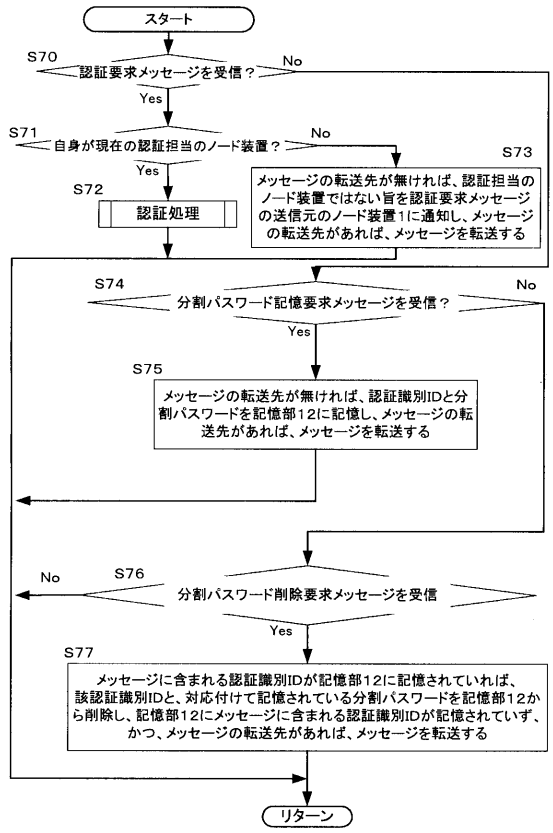
【図１９】



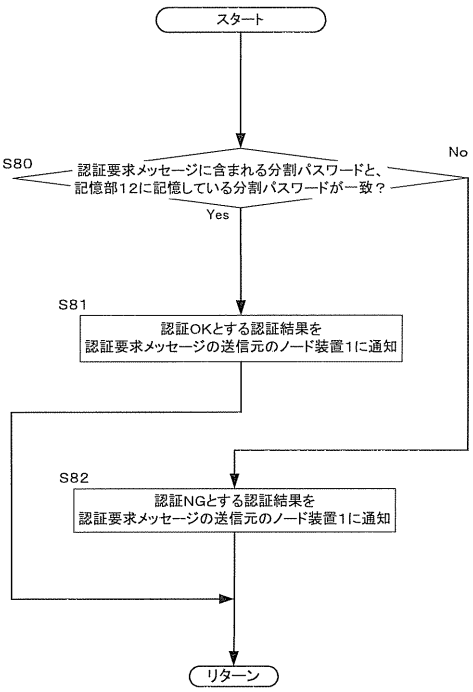
【図２０】



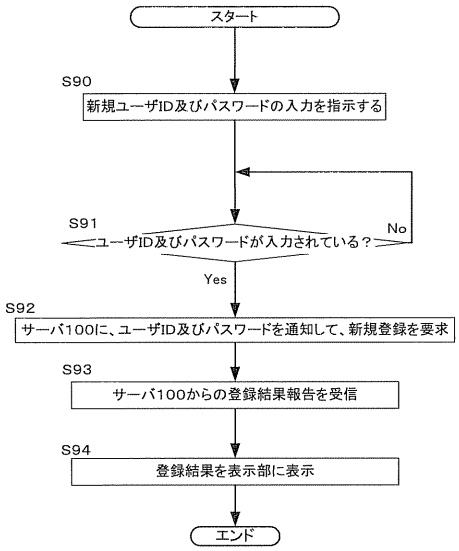
【図２１】



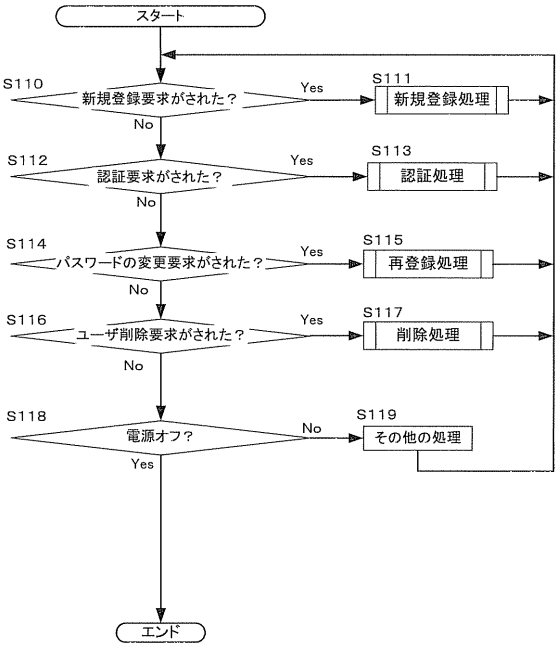
【図２２】



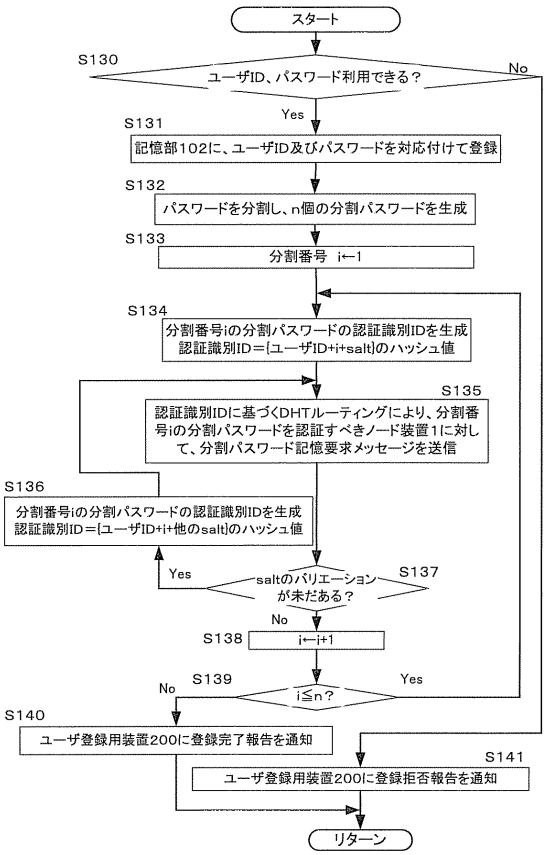
【図２３】



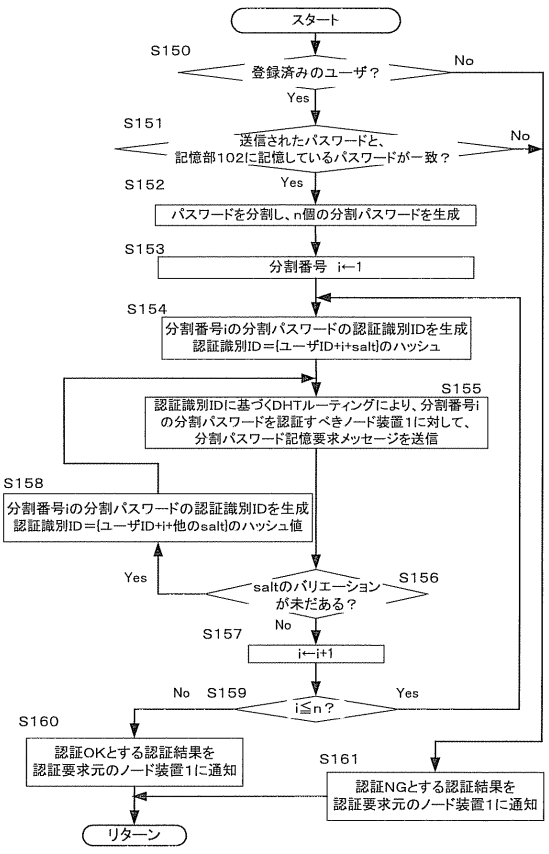
【図２４】



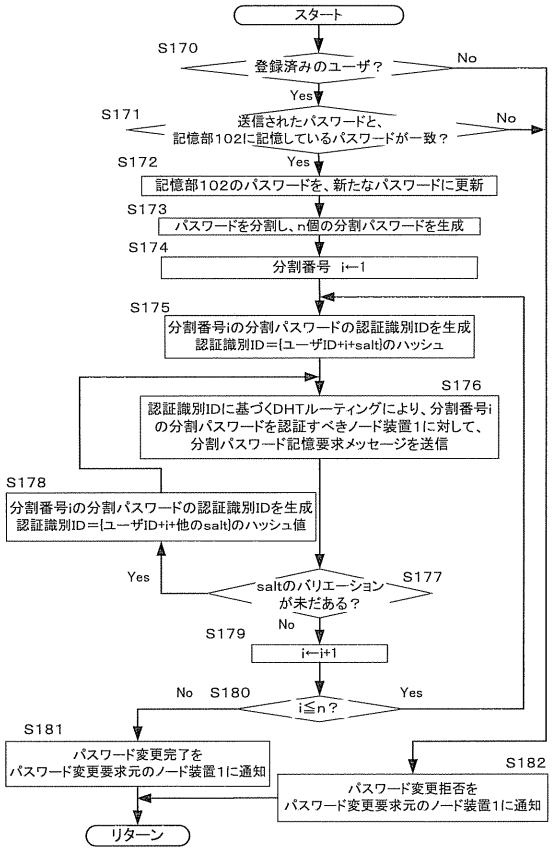
【図２５】



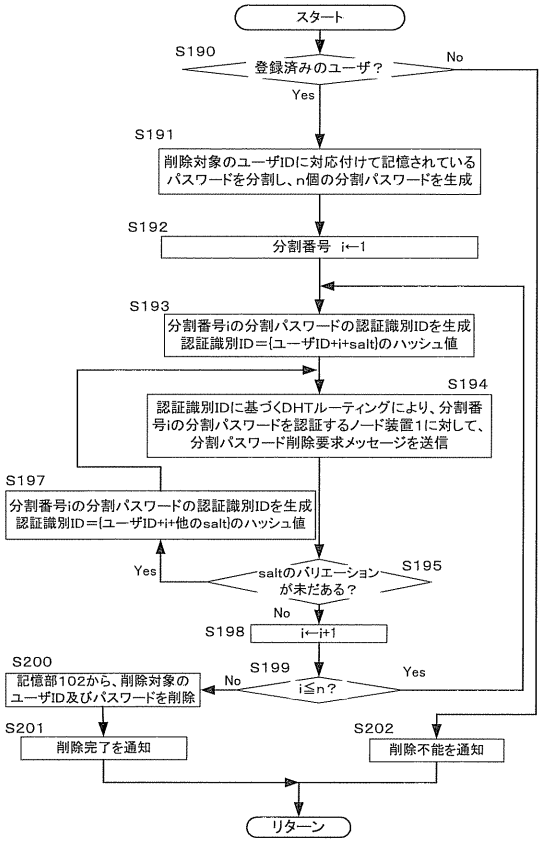
【図２６】



【図２７】


スタート
S170
登録済みのユーザ？
No
Yes
S171
送信されたパスワードと、
記憶部102に記憶しているパスワードが一致？
No
Yes
S172
記憶部102のパスワードを、新たなパスワードに更新
S173
パスワードを分割し、n個の分割パスワードを生成
S174
分割番号 i←1
S175
分割番号iの分割パスワードの認証識別IDを生成
認証識別ID＝{ユーザID+i+salt}のハッシュ
S176
認証識別IDに基づくDHTルーティングにより、分割番号i
の分割パスワードを認証すべきノード装置1に対して、
分割パスワード記憶要求メッセージを送信
S178
分割番号iの分割パスワードの認証識別IDを生成
認証識別ID＝{ユーザID+i+他のsalt}のハッシュ値
Yes
saltのバリエーション
が未だある？
S177
No
S179
i←i+1
No
S180
i≦n？
Yes
S181
パスワード変更完了を
パスワード変更要求元のノード装置1に通知
S182
パスワード変更拒否を
パスワード変更要求元のノード装置1に通知
リターン

【図２８】


スタート
S190
登録済みのユーザ？
No
Yes
S191
削除対象のユーザIDに対応付けて記憶されている
パスワードを分割し、n個の分割パスワードを生成
S192
分割番号 i←1
S193
分割番号iの分割パスワードの認証識別IDを生成
認証識別ID＝{ユーザID+i+salt}のハッシュ値
S194
認証識別IDに基づくDHTルーティングにより、分割番
号iの分割パスワードを認証するノード装置1に対して、
分割パスワード削除要求メッセージを送信
S197
分割番号iの分割パスワードの認証識別IDを生成
認証識別ID＝{ユーザID+i+他のsalt}のハッシュ値
Yes
saltのバリエーション
が未だある？
S195
No
S198
i←i+1
S200
記憶部102から、削除対象の
ユーザID及びパスワードを削除
No
S199
i≦n？
Yes
S201
削除完了を通知
S202
削除不能を通知
リターン

フロントページの続き

(74)代理人 100120237
弁理士 石橋 良規
(74)代理人 100123515
弁理士 石戸 孝則
(72)発明者 豊田 毅嗣
東京都新宿区大久保３－４－１ 早稲田大学理工学部内
(72)発明者 村岡 洋一
東京都新宿区大久保３－４－１ 早稲田大学理工学部内
(72)発明者 清原 裕二
愛知県名古屋市瑞穂区苗代町１５番１号 ブラザー工業株式会社内
(72)発明者 牛山 建太郎
愛知県名古屋市瑞穂区苗代町１５番１号 ブラザー工業株式会社内
(72)発明者 松尾 英輝
愛知県名古屋市瑞穂区苗代町１５番１号 ブラザー工業株式会社内
(72)発明者 飯島 康一
愛知県名古屋市瑞穂区塩入町１８番１号 株式会社エクシング内
Ｆターム(参考) 5B285 AA04 CB02 CB53 CB76
5J104 KA01 NA05 PA07