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

特許第4289817号
(P4289817)

(45)発行日　平成21年7月1日(2009.7.1)　(24)登録日　平成21年4月10日(2009.4.10)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330B
G06F 21/24	(2006.01)	G06F	12/14	530D
G06F 12/00	(2006.01)	G06F	12/00	537A
H04L 9/32	(2006.01)	H04L	9/00	673B
H04L 9/10	(2006.01)	H04L	9/00	621Z

請求項の数 8　(全 20 頁)

(21)出願番号　特願2002-50290(P2002-50290)
(22)出願日　平成14年2月26日(2002.2.26)
(65)公開番号　特開2003-256279(P2003-256279A)
(43)公開日　平成15年9月10日(2003.9.10)
審査請求日　平成16年12月14日(2004.12.14)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(72)発明者　重枝　伸之
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

最終頁に続く

(54)【発明の名称】情報管理装置及び方法

(57)【特許請求の範囲】
【請求項１】
データを格納する仮想的な格納領域であって、１つの格納領域に対してユーザ毎に異なる認証情報が対応付けられた格納領域を複数有する格納部を備えた情報管理装置であって、
ユーザによって入力された初期認証情報を受信する受信手段と、
前記初期認証情報に基づいて、前記ユーザが前記情報処理装置へログインすることを許可又は禁止する制御手段と、
前記制御手段によってログインが許可されたユーザによる、前記複数の格納領域のうちのいずれかの格納領域の指定を受け付ける受付手段と、
暗号化された認証情報であって、前記ユーザに指定された格納領域に対応し、且つ当該ユーザに対応する認証情報を、認証情報記憶部から取得する認証情報取得手段と、
前記認証情報取得手段によって取得された認証情報を、前記受信手段によって受信された初期認証情報を用いて復号する復号化手段と、
前記復号化手段によって復号された認証情報を用いて、前記ユーザに指定された格納領域へのアクセスを制御するアクセス制御手段と、
を有することを特徴とする情報管理装置。
【請求項２】
前記初期認証情報に基づいて前記複数の格納領域それぞれに対応した認証情報を暗号化する暗号化手段を更に有し、前記暗号化手段によって暗号化された認証情報は、前記認証

情報記憶部に記憶されることを特徴とする請求項１に記載の情報管理装置。
【請求項３】
前記認証情報記憶部は、前記情報管理装置と接続されたデータベースであって、前記認証情報取得手段は、ＬＤＡＰを用いて認証情報を取得することを特徴とする請求項１又は２に記載の情報管理装置。
【請求項４】
前記受信手段によって受信された初期認証情報を、前記ユーザがログアウトするまでの間保持する保持手段を更に有することを特徴とする請求項１乃至３の何れか１項に記載の情報管理装置。
【請求項５】
前記復号化手段及び前記暗号化手段は、前記初期認証情報を秘密鍵として、前記認証情報の暗号並びに復号処理を行うことを特徴とする請求項２に記載の情報管理装置。
【請求項６】
前記格納部に格納されたデータに基づいて印刷処理を行う印刷手段を更に有することを特徴とする請求項１乃至５の何れか１項に記載の情報管理装置。
【請求項７】
受信手段と、制御手段と、受付手段と、認証情報取得手段と、復号化手段と、アクセス制御手段と、データを格納する仮想的な格納領域であって、１つの格納領域に対してユーザ毎に異なる認証情報が対応付けられた格納領域を複数有する格納部とを備えた情報管理装置における情報管理方法であって、
前記受信手段が、ユーザによって入力された初期認証情報を受信する受信工程と、
前記制御手段が、前記初期認証情報に基づいて、前記ユーザが前記情報処理装置へログインすることを許可又は禁止する制御工程と、
前記受付手段が、前記制御工程によってログインが許可されたユーザによる、前記複数の格納領域のうちのいずれかの格納領域の指定を受け付ける受付工程と、
前記認証情報取得手段が、暗号化された認証情報であって、前記ユーザに指定された格納領域に対応し、且つ当該ユーザに対応する認証情報を、認証情報記憶部から取得する認証情報取得工程と、
前記復号化手段が、前記認証情報取得工程によって取得された認証情報を、前記受信工程によって受信された前記初期認証情報を用いて復号する復号化工程と、
前記アクセス制御手段が、前記復号化工程によって復号された認証情報を用いて、前記ユーザに指定された格納領域へのアクセスを制御するアクセス制御工程と、
を有することを特徴とする情報管理方法。
【請求項８】
受信手段と、制御手段と、受付手段と、認証情報取得手段と、復号化手段と、アクセス制御手段と、データを格納する仮想的な格納領域であって、１つの格納領域に対してユーザ毎に異なる認証情報が対応付けられた格納領域を複数有する格納部とを備えた情報管理装置における情報管理方法をコンピュータに実行させる情報管理プログラムであって、当該情報管理方法は、
前記受信手段が、ユーザによって入力された初期認証情報を受信する受信工程と、
前記制御手段が、前記初期認証情報に基づいて、前記ユーザが前記情報処理装置へログインすることを許可又は禁止する制御工程と、
前記受付手段が、前記制御工程によってログインが許可されたユーザによる、前記複数の格納領域のうちのいずれかの格納領域の指定を受け付ける受付工程と、
前記認証情報取得手段が、暗号化された認証情報であって、前記ユーザに指定された格納領域に対応し、且つ当該ユーザに対応する認証情報を、認証情報記憶部から取得する認証情報取得工程と、
前記復号化手段が、前記認証情報取得工程によって取得された認証情報を、前記受信工程によって受信された前記初期認証情報を用いて復号する復号化工程と、
前記アクセス制御手段が、前記復号化工程によって復号された認証情報を用いて、前記

ユーザに指定された格納領域へのアクセスを制御するアクセス制御工程と、
を有することを特徴とする情報管理プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、キャビネット毎にユーザパスワードを設定できるセキュリティ機能を有するアプリケーション、オペレーティングシステム並びに装置のユーザ認証機能に係り、特に、キャビネットの機密性を保持しながら、ユーザ認証情報の入力作業を簡素化することにより、ユーザの利便性を図るのに好適な情報管理装置及び情報管理方法に関する。

【０００２】

【従来の技術】

従来、文書データをスキャニングして装置内の記憶領域にデータを保持する機能を有するデジタル複合機や、コンピュータ上で処理することができる文書データやファイル情報を保持・管理するためのファイル管理モジュールにおいては、データを効率的に保持・管理するためのデータ記憶領域（以下、このデータ記憶領域を「キャビネット」という。）を有している。

【０００３】

キャビネットは、ボックス、フォルダなどと呼ばれることもあり、任意の階層構造を有する論理的なデータ記憶領域とみなすことができる。このキャビネットには、キャビネット内に保持・管理されるデータの機密性を保証するための利用者個人を特定するための利用者認証情報（以下、「認証情報」という。）をキャビネット毎に設定できるようになっている。従って、利用者はキャビネットに格納されている情報にアクセスするためには、その都度、そのキャビネットに設定されている認証情報を入力して、システムの認証を得てから管理されているデータにアクセスすることができた。

【０００４】

しかしながら、このような装置、あるいはシステムにおいて、利用者はキャビネットに格納されているデータにアクセスするためには、そのアクセスの度に認証情報を入力しなければならず、また異なる複数の認証情報がキャビネット毎に記憶されている場合には、キャビネット毎に認証処理が必要とされ手間と労力を必要としていた。

【０００５】

こうした問題を解決するため、キャビネットに設定する認証情報を、全てのキャビネットにおいて統一して利用するといった運用上の解決策を講じる解決方法や、いわゆる「シングルサインオン」と呼ばれる技術を利用する方法が考案された。このシングルサインオンと呼ばれる技術を利用すると、認証情報を１度入力して利用者の認証が行われた後は、同一の認証情報が設定されているキャビネットについては、認証情報を入力することなく該当するキャビネットにアクセスすることが可能となる。これにより、認証情報をキャビネット毎に入力する手間が省け、かつ、複数の認証情報を記憶する必要が無くなり、利用者の利便性を向上させることができる。

【０００６】

【発明が解決しようとする課題】

しかしながら、上記の従来技術で述べたキャビネットに設定する認証情報を統一する運用上の解決策では、キャビネットの認証情報を設定できる全ての利用者に対して運用ルールの周知徹底を図る必要があり、別の観点で利便性を害する恐れがある。加えて、全てのキャビネットに統一的な認証情報が設定されるため、統一した認証情報の機密性を保証することも困難であり、キャビネットの機密性が実質、劣化するといった深刻な問題が新たに生じることになる。

【０００７】

一方、シングルサインオン技術を利用するためには、既に利用者に導入されているキャビネット機能を有する既存のデジタル複合機やファイル管理システムをそのまま利用することができず、所定のシングルサインオンシステムに適合すべく新たに開発された機種、あ

るいは新しいバージョンに置き換えなければならない。このような新たな機種やバージョンの導入は、利用者にコスト面、並びに管理面に及ぶ新たな負担を強いることとなる。

【０００８】

例えば、既存の装置やファイル管理システムにおける認証情報の設定を移行することが一般的に困難であり、利用者に認証情報の再設定をさせ、キャビネットに保持・管理されているデータの移行といった手間のかかる作業を強いることとなる。

【０００９】

また、装置やファイル管理システムの設計が、特定のシングルサインオンシステムの仕様に依存してしまうため、柔軟な製品仕様を利用者に提供することが困難でもある。

【００１０】

【課題を解決するための手段】

本発明は、このような従来の技術の有する未解決の課題に着目してなされたものであって、データの機密性を保証しながら、なお且つ、利用者における認証情報の入力作業を簡素化し、操作の利便性を向上させるのに好適な情報管理装置及び情報管理方法等を提供することを目的としている。

【００１１】

上記課題を解決する本発明にかかる情報管理装置及び情報管理方法等は主として以下の構成よりなることを特徴とする。

【００１２】

すなわち、本発明にかかる情報管理装置は、データを格納する仮想的な格納領域であって、１つの格納領域に対してユーザ毎に異なる認証情報が対応付けられた格納領域を複数有する格納部を備えた情報管理装置であって、

ユーザによって入力された初期認証情報を受信する受信手段と、

前記初期認証情報に基づいて、前記ユーザが前記情報処理装置へログインすることを許可又は禁止する制御手段と、

前記制御手段によってログインが許可されたユーザによる、前記複数の格納領域のうちのいずれかの格納領域の指定を受け付ける受付手段と、

暗号化された認証情報であって、前記ユーザに指定された格納領域に対応し、且つ当該ユーザに対応する認証情報を、認証情報記憶部から取得する認証情報取得手段と、

前記認証情報取得手段によって取得された認証情報を、前記受信手段によって受信された初期認証情報を用いて復号する復号化手段と、

前記復号化手段によって復号された認証情報を用いて、前記ユーザに指定された格納領域へのアクセスを制御するアクセス制御手段と、を有することを特徴とする。

【００２１】

また、本発明にかかる情報管理方法は、受信手段と、制御手段と、受付手段と、認証情報取得手段と、復号化手段と、アクセス制御手段と、データを格納する仮想的な格納領域であって、１つの格納領域に対してユーザ毎に異なる認証情報が対応付けられた格納領域を複数有する格納部とを備えた情報管理装置における情報管理方法であって、

前記受信手段が、ユーザによって入力された初期認証情報を受信する受信工程と、

前記制御手段が、前記初期認証情報に基づいて、前記ユーザが前記情報処理装置へログインすることを許可又は禁止する制御工程と、

前記受付手段が、前記制御工程によってログインが許可されたユーザによる、前記複数の格納領域のうちのいずれかの格納領域の指定を受け付ける受付工程と、

前記認証情報取得手段が、暗号化された認証情報であって、前記ユーザに指定された格納領域に対応し、且つ当該ユーザに対応する認証情報を、認証情報記憶部から取得する認証情報取得工程と、

前記復号化手段が、前記認証情報取得工程によって取得された認証情報を、前記受信工程によって受信された前記初期認証情報を用いて復号する復号化工程と、

前記アクセス制御手段が、前記復号化工程によって復号された認証情報を用いて、前記ユーザに指定された格納領域へのアクセスを制御するアクセス制御工程と、を有すること

を特徴とする。
【００２７】
また、本発明にかかる情報管理プログラムは、受信手段と、制御手段と、受付手段と、認証情報取得手段と、復号化手段と、アクセス制御手段と、データを格納する仮想的な格納領域であって、１つの格納領域に対してユーザ毎に異なる認証情報が対応付けられた格納領域を複数有する格納部とを備えた情報管理装置における情報管理方法をコンピュータに実行させる情報管理プログラムであって、当該情報管理方法は、
前記受信手段が、ユーザによって入力された初期認証情報を受信する受信工程と、
前記制御手段が、前記初期認証情報に基づいて、前記ユーザが前記情報処理装置へログインすることを許可又は禁止する制御工程と、
前記受付手段が、前記制御工程によってログインが許可されたユーザによる、前記複数の格納領域のうちのいずれかの格納領域の指定を受け付ける受付工程と、
前記認証情報取得手段が、暗号化された認証情報であって、前記ユーザに指定された格納領域に対応し、且つ当該ユーザに対応する認証情報を、認証情報記憶部から取得する認証情報取得工程と、
前記復号化手段が、前記認証情報取得工程によって取得された認証情報を、前記受信工程によって受信された前記初期認証情報を用いて復号する復号化工程と、
前記アクセス制御手段が、前記復号化工程によって復号された認証情報を用いて、前記ユーザに指定された格納領域へのアクセスを制御するアクセス制御工程と、を有することを特徴とする。
【００２８】
【発明の実施形態】
以下、本発明の実施形態について図面を参照しながら説明する。
【００２９】
＜システムの概要＞
図１は、キャビネット毎に利用者認証情報を登録し、利用者のアクセスを統一的に管理するシステムの概略構成を示す図である。図１においてファイル管理モジュール１００は、文書データ等を保存するための複数のキャビネットを論理的に作成し、保存、管理することができる。
【００３０】
キャビネットはそのファイル管理モジュール１００に接続された記憶装置１０１の所定の記憶領域に作成され、作成された種々のデータは記憶装置１０１に作成された所定のキャビネットにおいて保存、管理される。ファイル管理モジュール１００及び記憶装置１０１は、データの授受を可能にする所定の信号線によって物理的に接続している。
【００３１】
ファイル管理モジュール１００の機能は、上位のユーザコンピュータ（以下、「ＰＣ」という。）上のソフトウエアとして実現される。
【００３２】
ユーザコンピュータ（ＰＣ）１０２は、ファイル管理モジュール１００の利用者に必要なユーザインターフェースを提供するものであり、そのインタフェース機能は、ユーザコンピュータ１０２の所定の記憶領域で動作するソフトウエアにより実現される。
【００３３】
なお、ユーザコンピュータ（ＰＣ）１０２は、不図示の要素であるＣＰＵ、ＲＯＭ、ＲＡＭ（１次記憶装置）、Ｉ／Ｏデバイス、ハードディスク（２次記憶装置）、入出力デバイス（ＣＲＴ、キーボード、マウスなど）、及びこれらを結合するシステムバスから構成され、ＲＯＭ並びにハードディスクに記憶されたソフトウエアを所定のメモリ空間にロードし、このソフトウエアに基づいてＣＰＵやＩ／Ｏデバイス等を作動せしめることで、所定の処理を実行することができる構成となっている。
【００３４】
図１のデジタル複合機１０３は、破線で囲まれた部分により示され、ファイル管理モジュ

ール１００、記憶装置１０１、並びにユーザコンピュータ１０２による機能構成を少なくとも含むものである。

【００３５】

このデジタル複合機１０３としては、ＭＦＰ(MULTI FUNCTION PERIPHERAL)と呼ばれる多目的なネットワーク機器が含まれ、ＭＦＰにおけるスキャナ機能、プリント機能、ファクシミリ機能等、各機能相互間におけるデータのアクセス制御や、ネットワークに接続するホストコンピュータからのデータ制御、データの編集において、所定のデータにアクセスする際の情報管理装置として本発明にかかる装置は機能することができる。

【００３６】

制御プロトコルとしてＬＤＡＰ（Lightweight Directory Access Protocol）を適用してデータの管理を実行する。ＬＤＡＰは、ＯＳＩのＸ．５００ディレクトリアクセスプロトコルに対する軽いフロントエンドとして機能するようＩＥＴＦのＷＧにて開発された標準的なディレクトリアクセスプロトコルで、ＲＦＣ１７７７並びにＲＦＣ２２５１などに仕様が規定されている。

【００３７】

また、ディレクトリサーバ１０４に接続するデータベース１０５は、上述のディレクトリサーバ１０４のバックエンドとして機能し、各種ディレクトリオブジェクトをデータベースとしてハンドリングする。

【００３８】

このディレクトリオブジェクトの実体は、データベース１０５に結合された記憶装置１０６に保持される。不図示のネットワークインターフェースカードによりディレクトリサーバ１０４とユーザコンピュータ１０２は、それぞれネットワークに接続し、標準的なネットワーク通信プロトコル（例えば、ＴＣＰ／ＩＰなど）を利用して情報通信することが可能である。上述のＬＤＡＰはアプリケーションレイヤのプロトコルとして、標準的なネットワーク通信プロトコルの上で動作する。

【００３９】

なお、本実施形態で説明するディレクトリサーバ１０４及びデータベース１０５、記憶装置１０６は、ディレクトリサーバ機能を提供する商用製品として販売されているActive Directory Server、Novell Directory Serviceあるいはオープンソースとして頒布されているOpen LDAPなどを利用することでも構成することができる。

【００４０】

＜キャビネットの説明＞

ここで、図１のファイル管理モジュール１００が提供するキャビネットについて、図３を用いて簡単にその内容を説明する。従来例でも述べた通り、キャビネットは、ボックス、フォルダなどと呼ばれることもあり、任意のディレクトリ構造を有する論理的なデータ記憶領域とみなすことができる。キャビネットは文書や各種ユーザデータを効率的に保持し管理するための論理的な階層構造を有している。更に、キャビネット内に保持・管理されるデータの機密性を保証するために、キャビネット毎に認証情報を設定できるようになっている。システム内において、一つのキャビネットを特定するには、一般的にはそのキャビネットに付けられた名称を指定するが、システムによってはキャビネットを特定するＩＤ値をソフトウエア的に保持しておき、そのＩＤによってキャビネットを特定する場合もある。これは、キャビネットの名称を後で柔軟に変更できるようにするために有効な手法である。

【００４１】

図３におけるキャビネット０（３００）は、ルートのキャビネットである。このキャビネットの中に、更にキャビネット１（３０１）、キャビネット２（３０２）、キャビネット３（３０３）、キャビネット４（３０４）などと複数のキャビネットを設けて、階層化することができる。例えば、複数のキャビネットに対して利用者はそれぞれのキャビネットの利便性を考慮した意味付けを行い、文書ファイルや画像データなどを保管することができる。更に、キャビネットを複数の階層にすることも可能で、図３のキャビネット１－１

（３０５）、並びにキャビネット１－２（３０６）は、キャビネット１（３０１）の中に作成されたキャビネットの構成を示している。どのような論理構造にするかはファイル管理モジュール１００を使用する利用者が任意に決めることが可能である。

【００４２】

キャビネット毎に関連付けられる認証情報は、ファイル管理モジュール１００内部における論理情報として、それぞれのキャビネットが保持するものとする。すなわち、キャビネット０（３００）にアクセスするために必要な認証情報は、キャビネット０（３００）に付随した情報として、利用者毎に関連付けをされて保持される。

【００４３】

利用者毎に関連付けされる情報は、各キャビネットに対するアクセス許可を与える認証情報の他に、その利用者の操作権限などを付随させてもよい。この場合、ある利用者のキャビネットへのアクセスを、例えば「読み取り」、「書き込み」、「実行」などと、操作の種類に応じて細かく権限分配して、キャビネットに対するアクセスを制御することも可能である。キャビネットに付随する認証情報は、キャビネット毎に設定することが可能であり、更に操作権限を重畳させることにより、特に機密性の高いデータの保持、管理を有効なものとすることができる。

【００４４】

なお、キャビネットは、階層構造の制限や認証制御リストの構造などに設計上の相違はあるものの、デジタル複合機１０３においても同様の機能が備わっている。

【００４５】

＜ユーザコンピュータの構成＞

図２は、ユーザコンピュータ１０２の特徴的な構成を示すブロック図である。同図において破線で示したディレクトリサーバ１０４及びキャビネットのユーザインタフェース（ＵＩ）モジュール２０６と、ユーザコンピュータ１０２の結合関係は破線により示され、ユーザコンピュータ１０２の内部における各モジュールの結合関係は実線により示すものとする。

【００４６】

ユーザインタフェース（ＵＩ）モジュール２００は、利用者がシステムを利用するための初期認証情報を入力処理するための処理モジュールを提供する。これはシステムへのログイン（あるいはログオン）と呼ばれる行為に相当し、利用者が初めて本システムを利用するために必要なプロセスである。ログイン機能として、本実施形態では初期認証情報を入力するためのダイアログボックスを不図示のＰＣディスプレイ上に表示し、利用者に初期認証情報の入力を促すと共に、その利用者の入力した初期認証情報が真正なものか否かの照合がされる。

【００４７】

ユーザコンピュータ１０２がＵＩモジュール２００において入力処理した利用者の初期認証情報は、その利用者が権限を有する所定の期間中、ユーザコンピュータ１０２の内部記憶領域に安全に保持されるものとする。ここで、上述の「利用者が権限を有する所定の期間」とは、その利用者がシステムの利用を終え、ログアウトするまでの期間である。初期認証情報を安全に保持するのは、図２における初期認証情報保持モジュール２０１で行われ、ユーザコンピュータ１０２の一時記憶領域に、ユーザコンピュータ１０２からのみ操作できる形態で保持することで実現されるものである。

【００４８】

更に、ユーザコンピュータ１０２は、ファイル管理モジュール１００の利用者に対して、そのファイル管理モジュール１００を操作するための必要なユーザインターフェース部分を提供する。すなわち、利用者はファイル管理モジュール１００に作成されたキャビネットにアクセスするために、所定のキャビネットを指定する操作をそのユーザインタフェースを介して行う。キャビネット指定モジュール２０２は、上述のユーザインターフェース部分と協調動作し、システムの利用者が指定するキャビネットを認識し、そのキャビネットの名称を取得する。このキャビネットの「名称」は、そのキャビネットに関連付けられ

た認証情報を取得するために後の処理で必要な情報である。
【００４９】
なお、本実施形態では、キャビネットを特定するために、そのキャビネットの名称を取得するが、これ以外にキャビネットに関連付けられた識別情報として固有のＩＤを利用してもよい。いずれの方法をとるかは、ファイル管理モジュール１００におけるキャビネットの構成方法と複数キャビネットの管理方法などに依存し、設計効率の良い手段を選択することが可能である。
【００５０】
キャビネットの認証情報を取得するモジュール２０３は、システムにログインした利用者の初期認証情報と、キャビネット指定モジュール２０２で取得したキャビネットの名称あるいは当該キャビネット固有のＩＤ（識別子）とを指定して、ディレクトリサーバ１０４からそのキャビネットに対する利用者認証情報を取得する。前述した通り、ディレクトリサーバ１０４はＬＤＡＰをサポートするため、キャビネットの認証情報を取得する認証情報取得モジュール２０３はＬＤＡＰクライアントとしての機能を備え、ＬＤＡＰにより所定の利用者認証情報を取得する。
【００５１】
ディレクトリサーバ１０４から取得した利用者認証情報は、所定の暗号アルゴリズムを用いて利用者毎の初期認証情報を鍵として暗号化されている。暗号化された利用者認証情報は、利用者の初期認証情報を使ってキャビネットの認証情報を復号（解読）する復号・暗号モジュール２０４によって復号される。この復号・暗号モジュール２０４は、所定の暗号処理エンジンを内包したソフトウエアプログラムによって構成されており、利用者認証情報の暗号化処理及び復号化処理を行うことができるようになっている。もちろん、効果的な処理能力を確保するために、当該処理をハードウェアにて実現することも可能である。
【００５２】
キャビネット毎に設定される利用者認証情報は、あらかじめ復号・暗号モジュール２０４によって利用者の初期認証情報を鍵として暗号化され、ディレクトリサーバ１０４に保持される。
【００５３】
一方、利用者がキャビネットに格納されているデータにアクセスする場合は、上述のキャビネットの認証情報取得モジュール２０３がキャビネットの名称あるいは当該キャビネット固有のＩＤと、利用者の初期認証情報と、に基づきディレクトリサーバ１０４から暗号化された利用者認証情報が取得され、その取得された利用者認証情報は復号・暗号モジュール２０４によって復号処理される。
【００５４】
暗号並びに復号処理にあたって秘密鍵となる利用者の初期認証情報は、前述の初期認証情報保持モジュール２０１より保持されており、復号・暗号モジュール２０４は、この初期認証情報保持モジュール２０１から利用者の初期認証情報を取得する。
【００５５】
尚、上述の復号・暗号モジュールにおいて、処理エンジンがサポートするアルゴリズムは、既存の様々な種類の暗号・復号アルゴリズムがあり、システムにおいていずれをも利用してもよい。
【００５６】
さらに、利用者認証情報の暗号化、並びに復号化処理は、ユーザーコンピュータ１０２内部で閉じた処理として実行されるので、利用者の暗号化・復号化に利用される初期認証情報がネットワーク上を流れ、公開されることは無い。従ってネットワーク上の不正な盗聴行為によって、利用者の初期認証情報が盗まれるなどの問題を回避することができる。
【００５７】
復号（解読）して得られた利用者認証情報は入力モジュール２０５によって、ユーザインターフェース２０６に入力される。従来、ユーザインターフェースは認証情報を入力する

ダイアログなどで構成され、ダイアログへの利用者認証情報の入力作業は、キャビネット毎に利用者が認証情報を手入力していた。しかし、本実施形態にかかるシステムでは、キャビネットの利用者認証情報を入力するユニット２０５が、ダイアログを自動的にフックして利用者認証情報の入力を代行する。このため、キャビネットの利用者認証情報の入力は自動化されることになる。

【００５８】

既に述べた通り、キャビネットの利用者認証情報の検索と取得、並びに復号処理、利用者認証情報のダイアログへの入力といった一連のシーケンスは自動化され、利用者は自らキャビネットの利用者認証情報を入力する作業から開放される。

【００５９】

また、利用者認証情報の入力が本システムのバックエンドで自動的に行われるため、利用者はキャビネット毎に設定される固有の利用者認証情報を記憶しておく必要が無くなる。すなわち、利用者は、本システムを利用するにあたり、初期認証情報を入力し、認証を経た後は、利用したいキャビネットにアクセスするだけでよい。後は、指定されたキャビネットに対して、システムは自動的にキャビネットの利用者認証情報を入力して、キャビネットへのアクセスが利用者に許可されることになる。

【００６０】

＜ディレクトリサーバ１０４及びデータベース１０５間のデータの整合＞

次に、ディレクトリサーバ１０４を経てデータベース１０５に保持される利用者認証情報の情報管理に関する一定の規則（以下、スキーマ）について説明する。

【００６１】

利用者認証情報は上述のように、ファイル管理モジュール１００におけるキャビネットに対してアクセスするために、利用者が入力しなければならない情報である。この利用者認証情報はそのままの形式でディレクトリサーバ１０４に保持されるのではなく、復号・暗号モジュール２０４における所定の暗号アルゴリズムに従って暗号化されてからディレクトリサーバ１０４に送信され保持、管理される。

【００６２】

これはディレクトリサーバ１０４を総合的に管理する権限を有する別の利用者が、ディレクトリサーバ１０４に利用者毎に保持されている利用者認証情報を不正に参照するのを防ぐためである。すなわち、ディレクトリサーバ１０４の管理者が、ファイル管理モジュール１００の管理者（あるいは利用者）であるとは限らないので、ファイル管理モジュール１００のキャビネットにアクセスするための利用者認証情報を不正に盗まれてしまう恐れをなくすことを意図したものである。

【００６３】

ここで、説明のために、キャビネットＸを特定する名称を「CabinetX」とし、また、そのキャビネットＸに対応する利用者Ｙの利用者認証情報を「passYX」と表現する。

【００６４】

更に、ある情報「Ｍ」を想定し、この情報を、ある暗号鍵「ｋ」で暗号化することを「Ｅｋ（Ｍ）」と表現する。

【００６５】

以上の標記を規範とすると、例えば、キャビネット１（３０１）に設定された利用者１の利用者認証情報は、「pass１１」と表され、これを利用者１の暗号鍵ｋ１で暗号処理することは、

Ｅｋ１（pass１１）、と表現される。

【００６６】

加えて、キャビネット１（３０１）に関連付けされた利用者認証情報が、当該キャビネット１（３０１）を特定する名称Cabinet1に関連付けされていることを次のように表現する。

【００６７】

Ｅｋ１（pass１１）：Cabinet１

本実施形態では、ディレクトリサーバ１０４におけるスキーマとしてキャビネットを使用するユーザのクラスを意味する「cabinetPerson」が定義される。また、ユーザクラスは、暗号化された利用者認証情報をキャビネットに対応づけた値として「encryptedPass」が属性として定義さる。以下は、当該オブジェクトクラス、並びに属性をＲＦＣ２２５２の規定により例示したものである。

【００６８】

```
objectclass (1.1.2.2.1 NAME 'cabinetPerson'
DESC 'cabinet user'
SUP person STRUCTURAL
MUST ('encryptedPass'))
attributetype (1.1.2.1.1 NAME 'encryptedPass'
DESC 'encrypted password for cabinet'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 )
```

このように定義されたスキーマを用いて、システムは利用者認証情報をキャビネットに関連付けて、ユーザ毎にディレクトリサーバ１０４に保持する。図４は、この状態を示したものである。図４においてUser１のデータ群（４００）及びUser２のデータ群（４１０）は、cabinetPersonクラスによって定義されたオブジェクトである。また、それぞれのオブジェクトは、キャビネット毎に関連付けされた暗号化された利用者認証情報を、暗号化されたencryptedPass属性として所有している。

【００６９】

すなわち、User１（４００）は、キャビネット１（３０１）に対応する暗号化された利用者認証情報４０１と、キャビネット２（３０２）に対応する暗号化された利用者認証情報４０２、更にキャビネット３（３０３）、キャビネット４（３０４）に対応する利用者認証情報４０３、４０４を保持する。User２（４１０）についても同様である。

【００７０】

User１（４００）が所有するencryptedPass属性の一つである、Ek1(pass11):Cabinet1（４０１）は、上述の説明のとおり、ある利用者１がキャビネット１に対する利用者認証情報としてpass11を設定するもので、この利用者認証情報が利用者1の暗号鍵ｋ１によって暗号化され、キャビネット１に関連付けられてディレクトリサーバ１０４に維持されていることを意味している。

【００７１】

一方、User２（４１０）が所有するencryptedPass属性の場合、Ek2(pass21):Cabinet1（４１１）は、キャビネット１に設定された利用者認証情報pass1が利用者２の暗号鍵ｋ２で暗号処理される。従って、同一のキャビネットに対するものであっても、利用者認証情報に基づく暗号化情報が異なるため、利用者１は利用者２のキャビネットに対する利用者認証情報を取得して解読することができないことになり情報の機密性を高めることが可能になる。

【００７２】

cabinetPersonクラスによって定義されたオブジェクトは、利用者の登録状況に応じて動的に変更することが可能である。また、キャビネット毎に関連付けされた暗号化された利用者認証情報、すなわちencryptedPass属性は、この属性を所有する利用者の使用するキャビネットの登録状況に応じて変化するものである。

【００７３】

なお、利用者の登録やキャビネットへのアクセス設定は、はじめにファイル管理モジュール１００に対して行なわれ、その後、ファイル管理モジュール１００が利用者の登録、設定状況を吸い上げて、ディレクトリサーバ１０４に反映する。このファイル管理モジュール１００における、登録ユーザやキャビネットのアクセス設定を参照し、ディレクトリサーバ１０４に反映させる機能（以下、「シンクロナイズ機能」という。）は、図２におけるキャビネットの認証情報取得モジュール２０３に具備され、実行される。シンクロナイズ機能は、ユーザコンピュータ１０２のサービスとして登録されたデーモンプログラムに

よって、定期的かつ自動的に処理される。一方、この処理をシステムの管理者が手動で必要な時に実施することも可能である。このシンクロナイズ機能の動作モードの切り替えは、管理者によって選択的に設定することが可能である。

【００７４】

また、ディレクトリサーバ１０４におけるスキーマの定義は、本実施形態で先に例示した以外の形式においても可能である。例えば、キャビネットを使用するユーザによるクラス分けではなく、キャビネットそのものをクラスとして定義することも可能である。この場合、キャビネットクラスは、暗号化された利用者認証情報をキャビネットの利用者に関連付けた値を属性として所有することになる。以下にこの場合のオブジェクトクラス、並びに属性の定義を、ＲＦＣ２２５２に規定されたディレクティブに従って例示する。

【００７５】

```
objectclass (1.1.2.2.1 NAME 'cabinetName'
DESC 'cabinet name'
SUP top STRUCTURAL
MUST ('encryptedUserPass'))
attributetype (1.1.2.1.1 NAME 'encryptedUserPass'
DESC 'encrypted password for user'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 )
```

＜動作シーケンスの説明＞

次に、本実施形態にかかるシステムも若しくは装置において、キャビネット毎に登録できる利用者認証情報を統一的に管理するための処理動作シーケンスを図５～図８のフローチャートを参照しながら説明する。

【００７６】

図５は、本実施形態にかかるシステムの全体の動作シーケンスを説明するフローチャートである。

【００７７】

利用者がシステムを起動すると本フローが開始する（Ｓ５００）。

【００７８】

利用者がファイル管理モジュール１００において管理されている任意のキャビネットにアクセスしようとすると、ステップＳ５０１においてシステムは先ず利用者がアクセスしたキャビネットのプロファイルを取得し、そのキャビネットへのアクセスの認証を行うための認証データを管理する認証サーバ情報を取得する。

【００７９】

ここで、「プロファイル」とは、利用者のキャビネットへのアクセスを認証する認証サーバに関する情報、例えば、ネットワーク上における所在情報（IPアドレスなど）、データ通信プロトコル（ＬＤＡＰなど）などから構成される情報である。このプロファイル情報はファイル管理モジュール１００が保持している情報で、ユーザコンピュータ（ＰＣ）１０２が、プロファイルを参照して、どの認証サーバに、どの方式で認証するかを特定する。利用者がキャビネットにアクセスしてプロファイルを取得すると同時に、システムにおける認証ステータスも合わせて取得することができる。

【００８０】

ステップＳ５０２では、認証ステータスの状態を判断する。すなわち、利用者が初期認証情報を有力し、ログイン状態になっているか否かを判断する。ステップＳ５０２の判断において、初期認証が完了していない場合は（Ｓ５０２－ＮＯ)、処理をステップＳ５０３のキャビネット利用者の初期認証工程へ進める。既に初期認証が完了しユーザがログイン状態になっていた場合は（Ｓ５０２-ＹＥＳ）、利用者の初期認証プロセスは省略され、キャビネット利用工程（Ｓ５０５）に処理を進める。

【００８１】

ステップＳ５０３においては、ファイル管理モジュール１００の利用者の初期認証が行われる。この初期認証の詳細は後に説明する。そして、初期認証の結果は、認証ステータス

を評価するステップＳ５０４において判断される。ステップＳ５０４において、利用者があらかじめ登録された正規の利用者として認証されれば（Ｓ５０４-ＹＥＳ）、処理を次のキャビネットの利用工程へ進める。一方、間違った初期認証情報を入力するなど、利用者の認証ステータスが認証不可の場合は（Ｓ５０４－ＮＯ）、再び処理をステップＳ５０３に戻し、利用者からの正しい初期認証情報の入力を待つ。

【００８２】

利用者が正しく認証された場合（Ｓ５０４－ＹＥＳ）、その利用者の初期認証情報はユーザコンピュータ１０２における初期認証情報保持モジュール２０１において保持、管理される。

【００８３】

ステップＳ５０５におけるキャビネットの利用工程は、利用者が実際に指定したキャビネットへアクセスするために必要なデータ処理を実行する工程である。この詳細は後に説明する。

【００８４】

利用者はキャビネットの利用を終えると、システムからログアウトするかどうか判断し、利用者がログアウトを選択する場合（Ｓ５０６－ＹＥＳ）、システムは正常に終了し、ユーザコンピュータ１０２に保持されていた利用者の初期認証情報並びにその利用者の認証ステータスは完全に破棄される。一方、利用者が一時的にキャビネットの利用を終えただけで、再びキャビネットの利用の望む場合、すなわちログアウトを選択しない場合は（Ｓ５０６－ＮＯ）、再びキャビネットのプロファイルを取得するステップＳ５０１処理を戻す。

【００８５】

＜初期認証シーケンス＞

図６は、図５キャビネット利用者の初期認証工程、ステップＳ５０３の詳細なシーケンスを説明したフローチャートである。

【００８６】

利用者がキャビネットにアクセスする際に、利用者が初期認証されていない場合は、必ずこの工程が実行される。利用者がキャビネットにアクセスすることによって図６のシーケンスが開始する（Ｓ６０１）。この工程が実施される段階において、利用者がどのキャビネットにアクセスしようとしているか、また、そのキャビネットの認証を行う認証サーバに関するデータは、既に図５のステップＳ５０１の処理により情報は得られている。

【００８７】

この認証サーバに関する情報から、その認証方法が特定され、認証ダイアログの表示工程が実行される（Ｓ６０３）。ここ表示される認証ダイアログに、利用者は自身が管理している初期認証情報を入力する。

【００８８】

ステップＳ６０４では、ダイアログに入力された利用者の初期任所情報をソフトウエア的にシステム内部に取り込む。

【００８９】

そして、ステップＳ６０５では、初期認証情報のハッシュを計算する。取り込んだ利用者の初期認証情報に所定のハッシュアルゴリズムを用いてハッシュを計算する。「ハッシュアルゴリズム」とは、任意の長さのデータを入力として固定長のデータ出力を得、かつ、出力データから入力データを復元することができないことを特徴とする演算アルゴリズムである、そのアルゴリズムに基づく関数を「ハッシュ」といい、これを一方向性関数と呼ぶ場合もある。

【００９０】

利用者の初期認証情報は、システムにおいて管理されているキャビネットに対するアクセスを許可する認証プロセスに供されるデータであり、極めて機密性の高い情報である。従って、そのままの形でネットワーク上に送出するわけにはいかないため、ステップＳ６０５において初期認証情報のハッシュを計算し、これを利用して認証サーバに認証を試みる

。
【００９１】
ディレクトリサーバ１０４を認証サーバの１つとして考えた場合、このディレクトリサーバに対する認証は、このサーバへ接続（bind）する工程（Ｓ６０６）で処理される。ここで、前述のハッシュがディレクトリサーバへ送られ、ＬＤＡＰによる接続（bind）処理によって認証が行われる。
【００９２】
ステップＳ６０６における接続で、利用者のハッシュが正常に認証されればディレクトリサーバ１０４へのコネクションが確立し、ＬＤＡＰによるデータの通信制御が可能になる。bindすなわち認証の結果はＬＤＡＰのbindレスポンスとしてユーザコンピュータ１０２に返り、バインド（認証）ステータス取得工程（Ｓ６０７）における処理に供される。レスポンスのあったbind（認証）のステータスは、ここで一時的に保持される。
【００９３】
ところで、本実施形態では初期認証情報のハッシュを計算し、このハッシュに基づいてbindオペレーションを実行する、いわゆるシンプルbindと呼ばれるオペレーションに該当する。しかし、強固なセキュリティを確保するために既存の暗号化通信プロトコル、例えばSSLやKerberosといった手法を用いた認証bind（ＳＡＳＬ　bindとも呼ぶ）を実施することも可能である。この場合は、改めて利用者の初期認証情報のハッシュを計算する工程（Ｓ６０５）を実施する必要が無いことは言うまでもない。いずれのbindオペレーションを実施するかは、システムの初期設定によって制御される。
【００９４】
bindオペレーションを実施し（Ｓ６０６）、その認証ステータスを取得すると（Ｓ６０７）、処理を次のステップＳ６０８に進め、ディレクトリサーバとの接続が解除（unbind）される。この段階では利用者の認証を確認することが目的であり、ディレクトリサーチなどを行う必要が無いためである。
【００９５】
接続を認証するbindステータスは一時的に保持され、利用者の初期認証フローは終了する（Ｓ６０９）。ここで、一時的に保持されたbindステータスは、図５認証ステータスを評価する工程（Ｓ５０４：図５）に供され、利用者のシステムへのログインの可否が判断される。
【００９６】
そして、利用者が初期認証情報に基づいて認証されると（Ｓ５０４－ＹＥＳ）、ファイル管理モジュール１００のキャビネットの利用が可能となる（Ｓ５０５）。
【００９７】
＜キャビネットの利用＞
図７は、利用者がキャビネットを利用する際の処理を説明するフローチャートである。図５、図６のフローチャートで説明したとおり、利用者の初期認証が正常に行なわれると、利用者が指定したキャビネットに対する利用フローが開始する（Ｓ７００）。
【００９８】
利用者がアクセスするキャビネットを指定することによって、キャビネット指定モジュール２０２は、そのキャビネットを認識し、ユーザがアクセスしたキャビネット名あるいは当該キャビネット固有のＩＤを取得する（Ｓ７０１）。
【００９９】
更に、ステップＳ７０２において、認証情報取得モジュール２０３は、初期認証情報に基づいて、システムにログインしているユーザ名を取得し、このユーザ名と、先に取得したキャビネット名あるいは当該キャビネット固有のＩＤと、を合わせて、これらの情報をキーとして所定のディレクトリサーバ１０４に対して、利用者認証情報を検索させ、その検索結果を取得する。ディレクトリサーバ１０４はＬＤＡＰをサポートするため、キャビネットの認証情報を取得する認証情報取得モジュール２０３はＬＤＡＰクライアントとしての機能を備え、ＬＤＡＰにより所定の利用者認証情報を取得することができる。このステ

ップＳ７０２の処理の詳細は後述する。
【０１００】
次に、ステップＳ７０３においては、先のステップで取得した利用者認証情報は前述した通り暗号化処理されているため、この暗号化された利用者認証情報を復号する。この復号化処理は、あらかじめ決められた復号・暗号アルゴリズムに基づいて、利用者の初期認証情報を暗号鍵として利用するものである。
【０１０１】
ステップＳ７０４において、復号された利用者認証情報は、対応するキャビネットの認証インターフェースに入力される。ここで、キャビネットの認証インターフェースは認証ダイアログボックスであり、このダイアログボックスへ復号化された利用者認証情報が自動入力される。
【０１０２】
なお、上述の「認証インターフェース」は、本発明にかかるシステムに対応するために、専用に設計したソフトウエアインターフェースを利用することも可能である。すなわち、キャビネットの認証情報を入力パラメータとするＡＰＩ（Application Program Interface)を、ファイル管理モジュール１００のユーザコンピュータに設計しておくことも可能である。
【０１０３】
そして、キャビネットの利用者認証情報を入力する入力モジュール２０５は、そのＡＰＩをコールすることで、キャビネットの利用者認証情報をソフトウエア処理としてファイル管理モジュール１００に渡すことが可能となる。この場合、キャビネットの認証ダイアログは不要となる。
【０１０４】
キャビネットへの利用者認証情報の入力が完了し、ファイル管理モジュール１００側で認証に成功すれば、利用者は指定したキャビネットへのアクセスが可能となる。そしてキャビネットを開いてユーザ作業を始めることができるようになる（Ｓ７０５）。
【０１０５】
ステップＳ７０６において、キャビネットの利用が終了すると、利用者がシステムからログアウトするか、それとも引き続きキャビネットを利用するかが判断される（Ｓ５０６：図５）。
【０１０６】
利用者は再び同一のキャビネットを利用する場合や、今度は別のキャビネットを利用するケースが考えられ、いずれの場合においても、図５のキャビネットのプロファイルを取得するステップＳ５０１に処理が戻される。例えば、利用者が認証サーバの異なるプロファイルを保持しているキャビネットへアクセスした場合、その利用者は前のキャビネットでは既に初期認証を得ているが、新しくアクセスしたキャビネットにおいてはまだ初期認証を完了していないことになる。よって、改めてキャビネット利用者の初期認証工程、ステップＳ５０３が実行されることとなる。
【０１０７】
利用者がシステムからログアウトしていなければ、利用者の初期認証情報と認証ステータスがユーザコンピュータ１０２の所定の記憶領域に保持されているため、これらの情報に基づいて利用者は再び認証が得られたキャビネットの利用は可能である（Ｓ５０５）。また、システムの利用を終了してログアウトを選択すると（Ｓ５０６－ＹＥＳ）、本発明にかかるシステムの利用が終了し、必要な終了処理が実施される（Ｓ５０７）。
【０１０８】
＜利用者認証情報の検索＞
ここで、図７のステップＳ７０２の処理で、ユーザ名及びキャビネット名をキー情報として利用者認証情報を検索し、ユーザコンピュータ１０２側に取得する処理工程の詳細を図８のフローチャートを用いて説明する。
【０１０９】

図５のステップＳ５０５におけるキャビネットの利用工程において利用者が利用するキャビネット名あるいは当該キャビネット固有のＩＤを取得すると（Ｓ７０１）、利用者認証情報の検索工程が開始する（Ｓ８００）。この利用者認証情報の検索工程（Ｓ８００）は、ＬＤＡＰのsearchオペレーションを実行することで実現する。そのために、先ず利用者の初期認証情報を使ってＬＤＡＰのbind（認証）オペレーションを実施する必要がある。そして、ステップＳ８０５において、利用者の初期認証情報を記憶領域から取得する。この初期認証情報は、bindオペレーションで基礎となるデータとなる。

【０１１０】

ステップＳ８０１で取得した利用者の初期認証情報は、所定のハッシュアルゴリズムを用いてハッシュが算出される（Ｓ８０２）。このハッシュは前述の説明におけるbind（認証）ステータスを取得するbindオペレーションにおける認証値に該当するものである。図２におけるキャビネットの認証情報を取得する認証情報取得モジュール２０３は、そのハッシュを用いてディレクトリサーバに接続（bind）する（Ｓ８０３）。

【０１１１】

そして、ステップＳ８０４において、bindオペレーションのレスポンス待って、バインド（認証）が成功したか否かが判断される。ここで、バインドオペレーションに失敗した場合（Ｓ８０４－ＮＯ）、利用者は再び初期認証情報の取得が必要なため、図５キャビネット利用者の初期認証工程、ステップＳ５０３へ移行する。一方、認証に成功した場合（Ｓ８０４－ＹＥＳ）、処理をステップＳ８０５に進め、実際にキャビネットの利用者認証情報の取得を実施する。

【０１１２】

利用者認証情報の取得は、オブジェクトクラス名及び属性名を指定して、所定の利用者認証情報を取得する。本実施形態においては、図４で説明したとおり、オブジェクトクラス名は「cabinetPerson」の値、属性名は「encryptedPass」の値がそれぞれ指定される。そして、searchオペレーションの結果、所定のキャビネットに関連付けされた暗号化された利用者認証情報がディレクトリサーバ１０４において検索され、取得される。

【０１１３】

ここで取得された利用者認証情報は、暗号化されたデータとして、ＬＤＡＰプロトコルにより認証情報取得モジュール２０３に送信される。

【０１１４】

この後、ＬＤＡＰ処理はディレクトリサーバ接続解除（unbind）工程に移行する（Ｓ８０６）。これによって利用者認証情報の取得に関する一連のＬＤＡＰオペレーションの処理が終了する（Ｓ８０７）。

【０１１５】

以降、暗号化された利用者認証情報は上述のステップＳ７０３からＳ７０５の処理で復号され、認証インタフェースに入力され、指定したキャビネットに対する利用者のアクセスが可能となる。

【０１１６】

＜他の実施形態＞

なお、本発明は、複数の機器(例えばホストコンピュータ、インタフェース機器、リーダ、プリンタなど）から構成されるシステムに適用しても、一つの機器からなる装置（複写機、プリンタ、ファクシミリ装置など）に適用してもよい。

【０１１７】

また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記憶した記憶媒体を、システムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読出し実行することによっても、達成される。

【０１１８】

この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成すること

になる。

【０１１９】

プログラムコードを供給するための記憶媒体としては、例えば、フロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、磁気テープ、不揮発性のメモリカード、ＲＯＭなどを用いることができる。

【０１２０】

また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているＯＳ（オペレーティングシステム）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれる。

【０１２１】

更に、記憶媒体から読出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれる。

【０１２２】

【発明の効果】

以上説明したように、本発明にかかる情報管理装置及び情報管理方法によれば、それぞの格納領域に対応する認証情報によって、それぞれの格納領域に格納されているデータへのアクセスを制御する場合において、利用者は一度認証を行うだけで、複数回の認証を行うことなく、複数の格納領域のそれぞれに格納されているデータへアクセスすることができ、格納領域に格納されているデータの機密性が維持されたまま、利用者の利便性が向上する。

【０１２３】

具体的には、以上説明したように、本発明にかかる情報管理装置及び情報管理方法によれば、既存のデジタル複合機やファイル管理モジュールの、個々のキャビネットの認証において、利用者は一度の認証のみ行うだけで複数のキャビネットに自由にアクセスすることが可能となる。これによってキャビネットの機密性を維持したまま、利用者の利便性を向上させることができる。

【０１２４】

そして、前述の効果を得るにあたって、既存のデジタル複合機やファイル管理モジュールに対して、新たな機種の導入やバージョンへの置き換えなど、基本的には不要であり、利用者の新たな負担を発生させることもない。

【０１２５】

一方、本発明にかかる装置及び方法が、国際標準プロトコルと暗号処理アルゴリズムを利用することから、特定のシングルサインオンシステムの仕様に依存するといった制約から開放される。従って、装置やアプリケーションの開発者は、柔軟な製品仕様に基づく製品開発が可能となる。

【０１２６】

なお、キャビネット固有の利用者認証情報は、利用者のみが知りうる初期認証情報によって暗号化されてディレクトリサーバに保持されるため、ネットワーク上、あるいはディレクトリサーバを管理するためにあらゆる利用者のデータにアクセス可能な権限を有する管理者に対しても、その機密性を確保する事ができるのである。

【図面の簡単な説明】

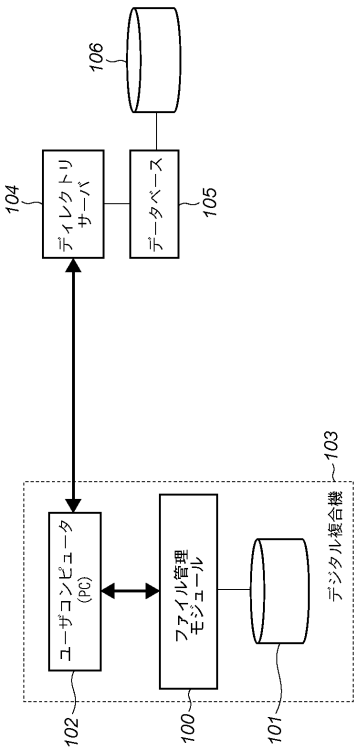
【図１】本発明の実施形態にかかる全体のシステム構成を説明する図である。

【図２】本発明の実施形態にかかるユーザコンピュータの詳細な構成について説明する図である。

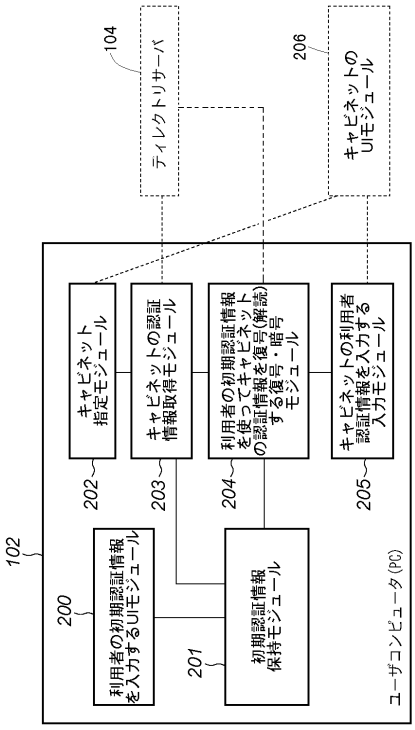
【図３】本発明の実施形態にかかるファイル管理モジュールにおけるキャビネットの構成を説明する図である。

【図４】本発明の実施形態にかかるディレクトリサーバにおけるスキーマの定義を具体的に説明する図である。
【図５】本発明の実施形態にかかる情報管理の全体的な処理の流れを説明するフローチャートである。
【図６】本発明の実施形態において、情報管理における初期認証処理の流れを説明するフローチャートである。
【図７】本発明の実施形態において、情報管理におけるキャビネットの利用のための認証処理の流れを説明するフローチャートである。
【図８】本発明の実施形態において、情報管理における利用者認証情報の検索処理の流れを説明するフローチャートである。

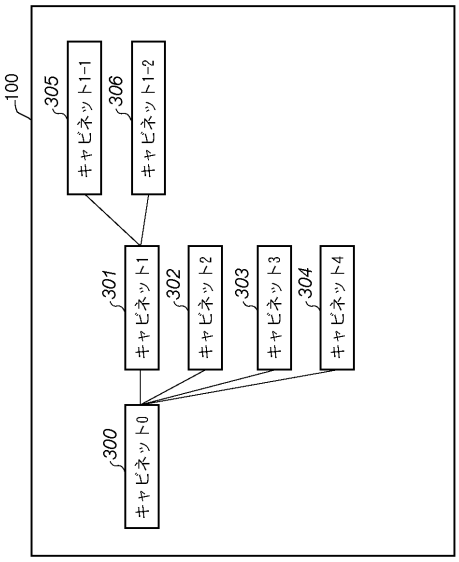
【図１】



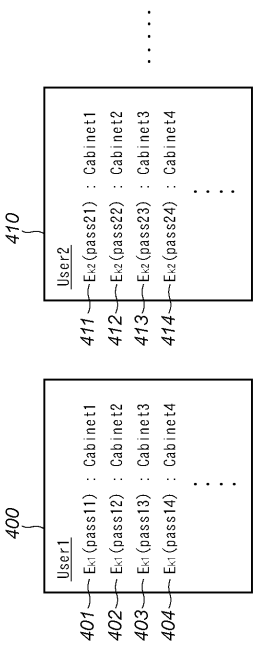
【図２】



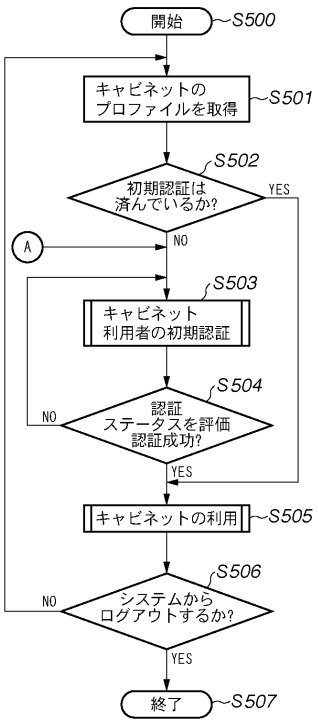
【図３】


100
305
キャビネット1-1
306
キャビネット1-2
301
キャビネット1
302
キャビネット2
303
キャビネット3
304
キャビネット4
300
キャビネット0

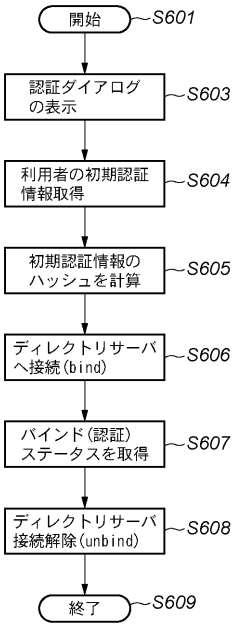
【図４】


410
User2
Ext(pass21) : Cabinet1
Ext(pass22) : Cabinet2
Ext(pass23) : Cabinet3
Ext(pass24) : Cabinet4
411
412
413
414
400
User1
Ext(pass11) : Cabinet1
Ext(pass12) : Cabinet2
Ext(pass13) : Cabinet3
Ext(pass14) : Cabinet4
401
402
403
404

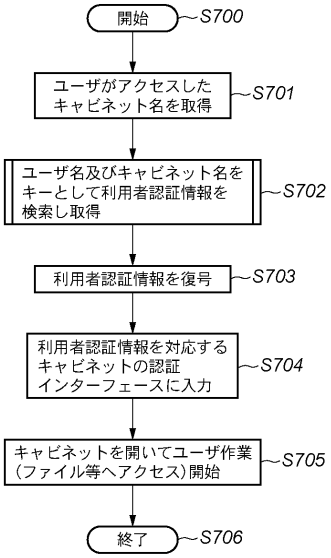
【図５】


開始
S500
キャビネットの
プロファイルを取得
S501
S502
初期認証は
済んでいるか?
YES
NO
A
S503
キャビネット
利用者の初期認証
S504
認証
ステータスを評価
認証成功?
NO
YES
キャビネットの利用
S505
S506
システムから
ログアウトするか?
NO
YES
終了
S507

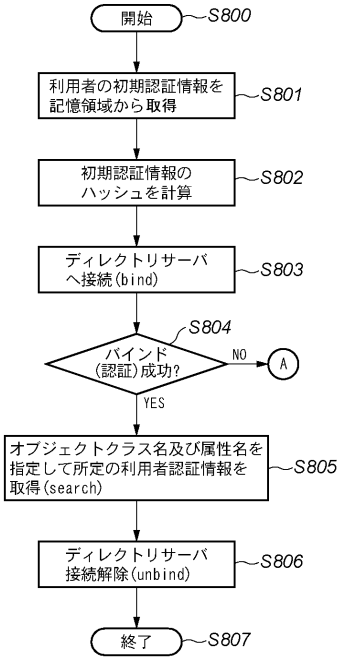
【図６】


開始
S601
認証ダイアログ
の表示
S603
利用者の初期認証
情報取得
S604
初期認証情報の
ハッシュを計算
S605
ディレクトリサーバ
へ接続(bind)
S606
バインド(認証)
ステータスを取得
S607
ディレクトリサーバ
接続解除(unbind)
S608
終了
S609

【図７】


開始
S700
ユーザがアクセスした
キャビネット名を取得
S701
ユーザ名及びキャビネット名を
キーとして利用者認証情報を
検索し取得
S702
利用者認証情報を復号
S703
利用者認証情報を対応する
キャビネットの認証
インターフェースに入力
S704
キャビネットを開いてユーザ作業
(ファイル等へアクセス)開始
S705
終了
S706

【図８】


開始
S800
利用者の初期認証情報を
記憶領域から取得
S801
初期認証情報の
ハッシュを計算
S802
ディレクトリサーバ
へ接続(bind)
S803
S804
バインド
(認証)成功?
NO
A
YES
オブジェクトクラス名及び属性名を
指定して所定の利用者認証情報を
取得(search)
S805
ディレクトリサーバ
接続解除(unbind)
S806
終了
S807

フロントページの続き

審査官　高橋　克

(56)参考文献　特開平１１－１１０３５０（ＪＰ，Ａ）
特開平０１－２７６３５２（ＪＰ，Ａ）
特開２０００－２３１５２３（ＪＰ，Ａ）
特開２０００－３４７９９４（ＪＰ，Ａ）
特開平１１－２３２１７７（ＪＰ，Ａ）
特開平０９－０７３４１６（ＪＰ，Ａ）
特開平０１－２１７５８７（ＪＰ，Ａ）
特開平０１－１６１４５７（ＪＰ，Ａ）
特開昭６３－１５５２４３（ＪＰ，Ａ）
中島　募，シングル・サインオン，日経インターネットテクノロジー　第２９号　Nikkei Internet Technology，日本，日経ＢＰ社　Nikkei Business Publications,Inc.，１９９９年１１月２２日，p.156-165

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　21/20-24
G06F　12/00
H04L　 9/10
H04L　 9/32