(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2005-157881
(P2005-157881A)
(43)公開日　平成17年6月16日(2005.6.16)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 12/14	G06F 12/14	310K	5B017
G06F 12/00	G06F 12/14	320B	5B082
G06F 15/00	G06F 12/00	537A	5B085
	G06F 12/00	545A	
	G06F 15/00	330A	

審査請求 未請求　請求項の数 19　ＯＬ　（全 20 頁）

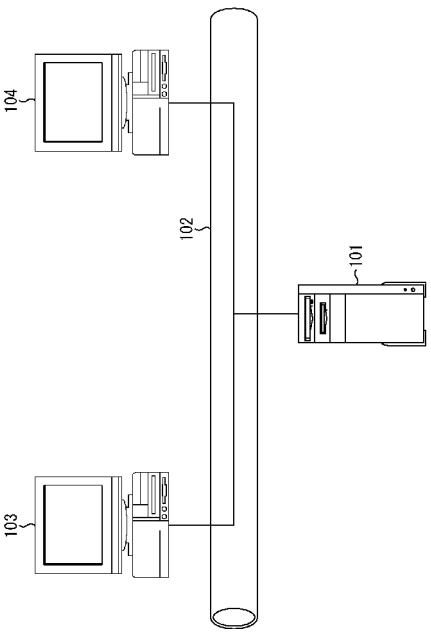
(21)出願番号　特願2003-397756 (P2003-397756)
(22)出願日　平成15年11月27日 (2003.11.27)

(71)出願人　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　100090273
弁理士　國分　孝悦
(72)発明者　横山　英彦
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

Ｆターム(参考)　5B017 AA07 BA06 BA07 CA16
5B082 EA11 HA05 HA08
5B085 AA08 AE09 AE23 BG01 BG04
BG07 CA02 CA04 CA06

(54)【発明の名称】サーバ端末装置、クライアント端末装置、オブジェクト管理システム、オブジェクト管理方法、コンピュータプログラム及び記録媒体

(57)【要約】
【課題】　オブジェクトを集中管理しているサーバ端末装置に登録しているユーザが所有するオブジェクトを、前記サーバ端末装置に登録していない第三者が安全に操作できるようにする。
【解決手段】　ユーザが管理するオブジェクトに対して権限委譲操作を行なうことが可能な権限委譲画面を生成して、前記オブジェクトを管理しているユーザのクライアント端末装置にネットワークを介して提供し、前記権限委譲画面を介して、前記オブジェクトに対する権限委譲操作が行なわれたら、前記ユーザに関連付けられたアクセスＵＲＬと、権限委譲ファイル及び前記権限委譲操作に関連付けられたアクセスチケットを生成し、これを自身の秘密鍵で暗号化した後で、前記アクセスＵＲＬと結合させてアクセストークンを生成するとともに、このアクセストークンを前記ユーザの公開鍵で暗号化して、前記ネットワークを介して前記ユーザに送信するようにする。
【選択図】　図１



【特許請求の範囲】
【請求項１】
ユーザが管理するオブジェクトに対して権限委譲操作を行なうことが可能な権限委譲画面を生成して、前記オブジェクトを管理しているユーザのクライアント端末装置にネットワークを介して提供する権限委譲画面提供手段と、
前記権限委譲画面提供手段によって提供された前記権限委譲画面を介して、前記オブジェクトに対する権限委譲操作が行なわれたら、前記ユーザに関連付けられたアクセスＵＲＬと、権限委譲ファイル及び前記権限委譲操作に関連付けられたアクセスチケットを生成するアクセスチケット生成手段と、
前記アクセスチケット生成手段によって生成されたアクセスチケットを自身の秘密鍵で暗号化した後で、前記アクセスＵＲＬと結合させてアクセストークンを生成するアクセストークン生成手段と、
前記アクセストークン生成手段によって生成されたアクセストークンを前記ユーザの公開鍵で暗号化して、前記ネットワークを介して前記ユーザに送信するアクセストークン送信手段とを有することを特徴とするサーバ端末装置。
【請求項２】
前記ユーザのアクセスＵＲＬに接続されて前記アクセスチケットが送られてきたときに、前記アクセスＵＲＬに関連付けられたユーザの公開鍵で前記アクセスチケットを復号する第１のアクセスチケット復号手段と、
前記アクセスチケット復号手段によって復号されたアクセスチケットを自身の秘密鍵で復号する第２のアクセスチケット復号手段と、
前記第２のアクセスチケット復号手段によって復号されたアクセスチケットと関連付けられたファイルに対して、関連付けられた操作を行なうことが可能な画面情報を生成する画面情報生成手段と、
前記画面情報生成手段によって生成された画面情報を、前記ネットワークを介して前記委譲先に送信する画面情報送信手段とを有することを特徴とする請求項１に記載のサーバ端末装置。
【請求項３】
ネットワークを利用して接続可能なクライアント端末装置と通信を行う通信手段と、前記通信手段により受信した認証情報を認証する認証手段と、前記認証手段により認証される識別情報を管理する管理手段と、前記認証手段により認証された状況に応じた画面情報を生成する画面情報生成手段と、オブジェクトの操作を行う操作手段と、前記オブジェクトの操作に関連付けられた権限参照情報を生成する権限参照情報生成手段と、各種情報を保存するデータ保存手段と、権限委譲元に関連付けられた接続情報を生成する接続情報生成手段と、前記権限参照情報を暗号化する第１の暗号化手段と、前記第１の暗号化手段により暗号化された権限参照情報と、前記接続情報とを結合してアクセストークンを生成するアクセストークン生成手段と、前記アクセストークン生成手段によって生成されたアクセストークンを暗号化する第２の暗号化手段と、前記画面情報生成手段により生成された画面情報及び前記第２の暗号化手段によって暗号化されたアクセストークンを、前記通信手段を用いて送信する送信手段とを備えることを特徴とするサーバ端末装置。
【請求項４】
前記接続情報が示す箇所への接続がなされた場合、前記データ保存手段により保存された、前記接続情報と関連付けられている権限委譲元を判定する権限委譲元判定手段と、前記権限委譲元判定手段により判定された権限委譲元の公開鍵を取得する公開鍵取得手段と、公開鍵取得手段により取得した公開鍵を用いて、接続と同時に受信したデータを復号する第１の復号手段と、前記第１の復号手段により復号したデータを、予め取得されて保存手段において保存されている秘密鍵を用いて復号する第２の復号手段と、前記第２の復号手段により復号されたデータを、前記保存手段により保存されている権限参照情報一覧から検出する検出手段と、前記検出手段により検出された権限参照情報を基に画面情報を生成する画面情報生成手段とを備えることを特徴とする請求項３に記載のサーバ端末装置。

【請求項５】
前記認証手段により認証される識別情報は、ユーザ識別子とパスワードの対であるか、接続情報の何れかであることを特徴とする請求項３または４に記載のサーバ端末装置。
【請求項６】
ネットワークに接続可能なクライアント端末装置において、
前記ネットワークを介してサーバ端末装置から送られてくるアクセストークンを受信するアクセストークン受信手段と、
前記アクセストークン受信手段によって受信したアクセストークンを自身の秘密鍵で復号して、前記アクセストークンの中からアクセスチケットを抽出するアクセスチケット抽出手段と、
前記アクセスチケット抽出手段によって抽出されたアクセスチケットを自身の秘密鍵で暗号化するアクセスチケット暗号化手段と、
前記アクセスチケット暗号化手段によって暗号化されたアクセスチケットを前記アクセストークンに戻した後で、権限委譲先の公開鍵で暗号化するアクセストークン暗号化手段と、
前記アクセストークン暗号化手段によって暗号化されたアクセストークンを、前記ネットワークを介して前記権限委譲先に送信するアクセストークン送信手段とを有することを特徴とするクライアント端末装置。
【請求項７】
ネットワークに接続可能な端末装置において、
ネットワークを利用して接続可能な端末装置と通信を行う通信手段と、前記通信手段により受信した画面生成情報を基に画面表示を行う画面表示手段と、前記画面表示手段により表示された画面に対してデータ入力を含む種々の操作を行う操作手段と、前記操作手段により入力された操作情報を、前記通信手段を用いて前記ネットワークに接続されたサーバ端末装置に送信する操作情報送信手段と、前記操作手段により権限委譲先への操作権限委譲操作を行った際に、前記通信手段より受信したアクセストークンを保存するデータ保存手段と、前記データ保存手段により保存したアクセストークンを、前記データ保存手段により予め保存されている暗号鍵を用いて復号する復号手段と、前記復号手段により復号されたアクセストークンから権限参照情報を抽出し、前記データ保存手段により予め保存されている暗号鍵を用いて暗号化する第１の暗号化手段と、前記権限委譲先の公開鍵を取得する公開鍵取得手段と、前記第１の暗号化手段により暗号化された権限参照情報を戻したアクセストークンを前記公開鍵取得手段により取得した公開鍵を用いて暗号化する第２の暗号化手段と、前記第２の暗号化手段で暗号化されたアクセストークンを、前記通信手段を用いて権限委譲先のクライアント端末装置に送信する送信手段を備えることを特徴とするクライアント端末装置。
【請求項８】
ネットワークに接続可能なクライアント端末装置において、
前記ネットワークを介して送られてくるアクセストークンを受信するアクセストークン受信手段と、
前記アクセストークン受信手段によって受信されたアクセストークンを自身の秘密鍵で復号するアクセストークン復号手段と、
前記アクセストークン復号手段によって復号されたアクセストークン中から抽出したアクセスＵＲＬに接続するとともに、前記アクセストークン中から抽出したアクセスチケットを送信するアクセスチケット送信手段とを有することを特徴とするクライアント端末装置。
【請求項９】
ネットワークに接続可能なクライアント端末装置において、
前記ネットワークを利用して接続可能な端末装置と通信を行う通信手段と、
前記通信手段により受信したアクセストークンを保存するデータ保存手段と、
前記データ保存手段により保存されたアクセストークンを、前記データ保存手段に予め

保存された秘密鍵を用いて復号するアクセストークン復号手段と、
前記アクセストークン復号手段により復号されたアクセストークンを、接続情報と権限参照情報とに分離する分離手段と、
前記分離手段により分離された接続情報が示す場所へ通信手段を用いて接続して、前記権限参照情報を送信する接続手段とを備えることを特徴とするクライアント端末装置。
【請求項１０】
前記請求項１～５の何れか１項に記載のサーバ端末装置と、前記請求項６～９の何れか１項に記載のクライアント端末装置とを有することを特徴とするオブジェクト管理システム。
【請求項１１】
ユーザが管理するオブジェクトに対して権限委譲操作を行なうことが可能な権限委譲画面を生成して、前記オブジェクトを管理しているユーザのクライアント端末装置にネットワークを介して提供する権限委譲画面提供工程と、
前記権限委譲画面提供工程によって提供された前記権限委譲画面を介して、前記オブジェクトに対する権限委譲操作が行なわれたら、前記ユーザに関連付けられたアクセスＵＲＬと、権限委譲ファイル及び前記権限委譲操作に関連付けられたアクセスチケットを生成するアクセスチケット生成工程と、
前記アクセスチケット生成工程によって生成されたアクセスチケットを自身の秘密鍵で暗号化した後で、前記アクセスＵＲＬと結合させてアクセストークンを生成するアクセストークン生成工程と、
前記アクセストークン生成工程によって生成されたアクセストークンを前記ユーザの公開鍵で暗号化して、前記ネットワークを介して前記ユーザに送信するアクセストークン送信工程とを有することを特徴とするサーバ端末装置におけるオブジェクト管理方法。
【請求項１２】
ネットワークに接続可能なクライアント端末装置におけるオブジェクト管理方法において、
前記ネットワークを介してサーバ端末装置から送られてくるアクセストークンを受信するアクセストークン受信工程と、
前記アクセストークン受信工程によって受信したアクセストークンを自身の秘密鍵で復号して、前記アクセストークンの中からアクセスチケットを抽出するアクセスチケット抽出工程と、
前記アクセスチケット抽出工程によって抽出されたアクセスチケットを自身の秘密鍵で暗号化するアクセスチケット暗号化工程と、
前記アクセスチケット暗号化工程によって暗号化されたアクセスチケットを前記アクセストークンに戻した後で、権限委譲先の公開鍵で暗号化するアクセストークン暗号化工程と、
前記アクセストークン暗号化工程によって暗号化されたアクセストークンを、前記ネットワークを介して前記権限委譲先に送信するアクセストークン送信工程とを有することを特徴とするクライアント端末装置におけるオブジェクト管理方法。
【請求項１３】
ネットワークに接続可能なクライアント端末装置におけるオブジェクト管理方法において、
前記ネットワークを介して送られてくるアクセストークンを受信するアクセストークン受信工程と、
前記アクセストークン受信工程によって受信されたアクセストークンを自身の秘密鍵で復号するアクセストークン復号工程と、
前記アクセストークン復号工程によって復号されたアクセストークン中から抽出したアクセスＵＲＬに接続するとともに、前記アクセストークン中から抽出したアクセスチケットを送信するアクセスチケット送信工程とを有することを特徴とするクライアント端末装置におけるオブジェクト管理方法。

【請求項１４】
ネットワークに接続可能なクライアント端末装置におけるオブジェクト管理方法において、
前記ネットワークを利用して接続可能な端末装置と通信を行なう通信手段により受信したアクセストークンをデータ保存手段に保存するデータ保存工程と、
前記データ保存手段に保存されたアクセストークンを、前記データ保存手段に予め保存された秘密鍵を用いて復号するアクセストークン復号工程と、
前記アクセストークン復号工程により復号されたアクセストークンを、接続情報と権限参照情報とに分離する分離工程と、
前記分離工程により分離された接続情報が示す場所へ前記通信手段を用いて接続して、前記権限参照情報を送信する接続工程とを有することを特徴とするクライアント端末装置におけるオブジェクト管理方法。
【請求項１５】
ユーザが管理するオブジェクトに対して権限委譲操作を行なうことが可能な権限委譲画面を生成して、前記オブジェクトを管理しているユーザのクライアント端末装置にネットワークを介して提供する権限委譲画面提供工程と、
前記権限委譲画面提供工程によって提供された前記権限委譲画面を介して、前記オブジェクトに対する権限委譲操作が行なわれたら、前記ユーザに関連付けられたアクセスＵＲＬと、権限委譲ファイル及び前記権限委譲操作に関連付けられたアクセスチケットを生成するアクセスチケット生成工程と、
前記アクセスチケット生成工程によって生成されたアクセスチケットを自身の秘密鍵で暗号化した後で、前記アクセスＵＲＬと結合させてアクセストークンを生成するアクセストークン生成工程と、
前記アクセストークン生成工程によって生成されたアクセストークンを前記ユーザの公開鍵で暗号化して、前記ネットワークを介して前記ユーザに送信するアクセストークン送信工程とをサーバ端末装置においてコンピュータに実行させることを特徴とするコンピュータプログラム。
【請求項１６】
ネットワークに接続可能なクライアント端末装置におけるオブジェクト管理方法をコンピュータに実行させるプログラムにおいて、
前記ネットワークを介してサーバ端末装置から送られてくるアクセストークンを受信するアクセストークン受信工程と、
前記アクセストークン受信工程によって受信したアクセストークンを自身の秘密鍵で復号して、前記アクセストークンの中からアクセスチケットを抽出するアクセスチケット抽出工程と、
前記アクセスチケット抽出工程によって抽出されたアクセスチケットを自身の秘密鍵で暗号化するアクセスチケット暗号化工程と、
前記アクセスチケット暗号化工程によって暗号化されたアクセスチケットを前記アクセストークンに戻した後で、権限委譲先の公開鍵で暗号化するアクセストークン暗号化工程と、
前記アクセストークン暗号化工程によって暗号化されたアクセストークンを、前記ネットワークを介して前記権限委譲先に送信するアクセストークン送信工程とをクライアント端末装置においてコンピュータに実行させることを特徴とするコンピュータプログラム。
【請求項１７】
ネットワークに接続可能なクライアント端末装置におけるオブジェクト管理方法をコンピュータに実行させるプログラムにおいて、
前記ネットワークを介して送られてくるアクセストークンを受信するアクセストークン受信工程と、
前記アクセストークン受信工程によって受信されたアクセストークンを自身の秘密鍵で復号するアクセストークン復号工程と、

前記アクセストークン復号工程によって復号されたアクセストークン中から抽出したアクセスＵＲＬに接続するとともに、前記アクセストークン中から抽出したアクセスチケットを送信するアクセスチケット送信工程とを有することを特徴とするクライアント端末装置においてコンピュータに実行させることを特徴とするコンピュータプログラム。

【請求項１８】

ネットワークに接続可能なクライアント端末装置におけるオブジェクト管理方法をコンピュータに実行させるプログラムにおいて、

前記ネットワークを利用して接続可能な端末装置と通信を行なう通信手段により受信したアクセストークンをデータ保存手段に保存するデータ保存工程と、

前記データ保存手段に保存されたアクセストークンを、前記データ保存手段に予め保存された秘密鍵を用いて復号するアクセストークン復号工程と、

前記アクセストークン復号工程により復号されたアクセストークンを、接続情報と権限参照情報とに分離する分離工程と、

前記分離工程により分離された接続情報が示す場所へ前記通信手段を用いて接続して、前記権限参照情報を送信する接続工程とを有することを特徴とするクライアント端末装置においてコンピュータに実行させることを特徴とするコンピュータプログラム。

【請求項１９】

前記請求項１５～１８の何れか１項に記載のコンピュータプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明はサーバ端末装置、クライアント端末装置、オブジェクト管理システム、オブジェクト管理方法、コンピュータプログラム及び記録媒体に関し、特に、認証された使用者毎に管理される、文書ファイル等のオブジェクトに対して、削除・印刷等の操作を行なうオブジェクト管理プログラム及びそれを利用したシステムに関するものである。

【背景技術】

【０００２】

従来、サーバにおいて集中管理されたオブジェクト操作システムにおいて、特定のユーザが保有するオブジェクトを第三者から操作可能にする場合、前記サーバにアクセス可能なユーザとして登録し、当該ファイルへの特定操作を許可するのが一般的であった。

【０００３】

また、特許文献１では、分散環境におけるオブジェクトに対する操作権限の委譲に関して述べられているが、これによれば、クライアント端末装置において権限情報を生成し、これを暗号化して転送することにより、操作権限を安全に委譲できるようにすることを可能にしている。

【０００４】

【特許文献１】特開２００１－１０１０５４号公報

【発明の開示】

【発明が解決しようとする課題】

【０００５】

しかしながら、前述した従来の技術では、オブジェクトの操作を一時的にさせるだけの為にユーザ登録を行なうことは管理コストに見合わない問題点があった。また、別の方法として、ゲストユーザのように予め限定ユーザを作成することでは、柔軟な操作権限の設定が不可能であった。

【０００６】

また、特許文献１に挙げた先行例では、オブジェクトの管理元であるサーバとは異なるクライアント端末装置でアクセス権限情報を生成し、これを暗号化等の演算を施した後に転送しているが、悪意のある者により暗号が解かれると、アクセス権限が不正に操作されることが懸念される。

本発明は前述の問題点にかんがみ、オブジェクトを集中管理しているサーバ端末装置に登録しているユーザが所有するオブジェクトを、前記サーバ端末装置に登録していない第三者が安全に操作できるようにすることを目的とする。

【課題を解決するための手段】

【０００７】

本発明のサーバ端末装置は、ユーザが管理するオブジェクトに対して権限委譲操作を行なうことが可能な権限委譲画面を生成して、前記オブジェクトを管理しているユーザのクライアント端末装置にネットワークを介して提供する権限委譲画面提供手段と、前記権限委譲画面提供手段によって提供された前記権限委譲画面を介して、前記オブジェクトに対する権限委譲操作が行なわれたら、前記ユーザに関連付けられたアクセスＵＲＬと、権限委譲ファイル及び前記権限委譲操作に関連付けられたアクセスチケットを生成するアクセスチケット生成手段と、前記アクセスチケット生成手段によって生成されたアクセスチケットを自身の秘密鍵で暗号化した後で、前記アクセスＵＲＬと結合させてアクセストークンを生成するアクセストークン生成手段と、前記アクセストークン生成手段によって生成されたアクセストークンを前記ユーザの公開鍵で暗号化して、前記ネットワークを介して前記ユーザに送信するアクセストークン送信手段とを有することを特徴としている。

また、本発明の他の特徴とするところは、ネットワークを利用して接続可能なクライアント端末装置と通信を行う通信手段と、前記通信手段により受信した認証情報を認証する認証手段と、前記認証手段により認証される識別情報を管理する管理手段と、前記認証手段により認証された状況に応じた画面情報を生成する画面情報生成手段と、オブジェクトの操作を行う操作手段と、前記オブジェクトの操作に関連付けられた権限参照情報を生成する権限参照情報生成手段と、各種情報を保存するデータ保存手段と、権限委譲元に関連付けられた接続情報を生成する接続情報生成手段と、前記権限参照情報を暗号化する第１の暗号化手段と、前記第１の暗号化手段により暗号化された権限参照情報と、前記接続情報とを結合してアクセストークンを生成するアクセストークン生成手段と、前記アクセストークン生成手段によって生成されたアクセストークンを暗号化する第２の暗号化手段と、前記画面情報生成手段により生成された画面情報及び前記第２の暗号化手段によって暗号化されたアクセストークンを、前記通信手段を用いて送信する送信手段とを備えることを特徴としている。

【０００８】

本発明のクライアント端末装置は、ネットワークに接続可能なクライアント端末装置において、前記ネットワークを介してサーバ端末装置から送られてくるアクセストークンを受信するアクセストークン受信手段と、前記アクセストークン受信手段によって受信したアクセストークンを自身の秘密鍵で復号して、前記アクセストークンの中からアクセスチケットを抽出するアクセスチケット抽出手段と、前記アクセスチケット抽出手段によって抽出されたアクセスチケットを自身の秘密鍵で暗号化するアクセスチケット暗号化手段と、前記アクセスチケット暗号化手段によって暗号化されたアクセスチケットを前記アクセストークンに戻した後で、権限委譲先の公開鍵で暗号化するアクセストークン暗号化手段と、前記アクセストークン暗号化手段によって暗号化されたアクセストークンを、前記ネットワークを介して前記権限委譲先に送信するアクセストークン送信手段とを有することを特徴としている。

また、本発明の他の特徴とするところは、ネットワークに接続可能な端末装置において、ネットワークを利用して接続可能な端末装置と通信を行う通信手段と、前記通信手段により受信した画面生成情報を基に画面表示を行う画面表示手段と、前記画面表示手段により表示された画面に対してデータ入力を含む種々の操作を行う操作手段と、前記操作手段により入力された操作情報を、前記通信手段を用いて前記ネットワークに接続されたサーバ端末装置に送信する操作情報送信手段と、前記操作手段により権限委譲先への操作権限委譲操作を行った際に、前記通信手段より受信したアクセストークンを保存するデータ保存手段と、前記データ保存手段により保存したアクセストークンを、前記データ保存手段により予め保存されている暗号鍵を用いて復号する復号手段と、前記復号手段により復号

されたアクセストークンから権限参照情報を抽出し、前記データ保存手段により予め保存されている暗号鍵を用いて暗号化する第１の暗号化手段と、前記権限委譲先の公開鍵を取得する公開鍵取得手段と、前記第１の暗号化手段により暗号化された権限参照情報を戻したアクセストークンを前記公開鍵取得手段により取得した公開鍵を用いて暗号化する第２の暗号化手段と、前記第２の暗号化手段で暗号化されたアクセストークンを、前記通信手段を用いて権限委譲先のクライアント端末装置に送信する送信手段を備えることを特徴としている。

また、本発明の他の特徴とするところは、ネットワークに接続可能なクライアント端末装置において、前記ネットワークを介して送られてくるアクセストークンを受信するアクセストークン受信手段と、前記アクセストークン受信手段によって受信されたアクセストークンを自身の秘密鍵で復号するアクセストークン復号手段と、前記アクセストークン復号手段によって復号されたアクセストークン中から抽出したアクセスＵＲＬに接続するとともに、前記アクセストークン中から抽出したアクセスチケットを送信するアクセスチケット送信手段とを有することを特徴としている。

また、本発明のその他の特徴とするところは、ネットワークに接続可能なクライアント端末装置において、前記ネットワークを利用して接続可能な端末装置と通信を行う通信手段と、前記通信手段により受信したアクセストークンを保存するデータ保存手段と、前記データ保存手段により保存されたアクセストークンを、前記データ保存手段に予め保存された秘密鍵を用いて復号するアクセストークン復号手段と、前記アクセストークン復号手段により復号されたアクセストークンを、接続情報と権限参照情報とに分離する分離手段と、前記分離手段により分離された接続情報が示す場所へ通信手段を用いて接続して、前記権限参照情報を送信する接続手段とを備えることを特徴としている。

【０００９】

本発明のオブジェクト管理システムは、前記の何れかに記載のサーバ端末装置と、前記の何れかに記載のクライアント端末装置とを有することを特徴としている。

【００１０】

本発明のサーバ端末装置におけるオブジェクト管理方法は、ユーザが管理するオブジェクトに対して権限委譲操作を行なうことが可能な権限委譲画面を生成して、前記オブジェクトを管理しているユーザのクライアント端末装置にネットワークを介して提供する権限委譲画面提供工程と、前記権限委譲画面提供工程によって提供された前記権限委譲画面を介して、前記オブジェクトに対する権限委譲操作が行なわれたら、前記ユーザに関連付けられたアクセスＵＲＬと、権限委譲ファイル及び前記権限委譲操作に関連付けられたアクセスチケットを生成するアクセスチケット生成工程と、前記アクセスチケット生成工程によって生成されたアクセスチケットを自身の秘密鍵で暗号化した後で、前記アクセスＵＲＬと結合させてアクセストークンを生成するアクセストークン生成工程と、前記アクセストークン生成工程によって生成されたアクセストークンを前記ユーザの公開鍵で暗号化して、前記ネットワークを介して前記ユーザに送信するアクセストークン送信工程とを有することを特徴としている。

【００１１】

本発明のクライアント端末装置におけるオブジェクト管理方法は、ネットワークに接続可能なクライアント端末装置におけるオブジェクト管理方法において、前記ネットワークを介してサーバ端末装置から送られてくるアクセストークンを受信するアクセストークン受信工程と、前記アクセストークン受信工程によって受信したアクセストークンを自身の秘密鍵で復号して、前記アクセストークンの中からアクセスチケットを抽出するアクセスチケット抽出工程と、前記アクセスチケット抽出工程によって抽出されたアクセスチケットを自身の秘密鍵で暗号化するアクセスチケット暗号化工程と、前記アクセスチケット暗号化工程によって暗号化されたアクセスチケットを前記アクセストークンに戻した後で、権限委譲先の公開鍵で暗号化するアクセストークン暗号化工程と、前記アクセストークン暗号化工程によって暗号化されたアクセストークンを、前記ネットワークを介して前記権限委譲先に送信するアクセストークン送信工程とを有することを特徴としている。

また、本発明の他の特徴とするところは、ネットワークに接続可能なクライアント端末装置におけるオブジェクト管理方法において、前記ネットワークを介して送られてくるアクセストークンを受信するアクセストークン受信工程と、前記アクセストークン受信工程によって受信されたアクセストークンを自身の秘密鍵で復号するアクセストークン復号工程と、前記アクセストークン復号工程によって復号されたアクセストークン中から抽出したアクセスＵＲＬに接続するとともに、前記アクセストークン中から抽出したアクセスチケットを送信するアクセスチケット送信工程とを有することを特徴としている。

また、本発明の他の特徴とするところは、ネットワークに接続可能なクライアント端末装置におけるオブジェクト管理方法において、前記ネットワークを利用して接続可能な端末装置と通信を行なう通信手段により受信したアクセストークンをデータ保存手段に保存するデータ保存工程と、前記データ保存手段に保存されたアクセストークンを、前記データ保存手段に予め保存された秘密鍵を用いて復号するアクセストークン復号工程と、

前記アクセストークン復号工程により復号されたアクセストークンを、接続情報と権限参照情報とに分離する分離工程と、前記分離工程により分離された接続情報が示す場所へ前記通信手段を用いて接続して、前記権限参照情報を送信する接続工程とを有することを特徴としている。

【００１２】

本発明のコンピュータプログラムは、ユーザが管理するオブジェクトに対して権限委譲操作を行なうことが可能な権限委譲画面を生成して、前記オブジェクトを管理しているユーザのクライアント端末装置にネットワークを介して提供する権限委譲画面提供工程と、前記権限委譲画面提供工程によって提供された前記権限委譲画面を介して、前記オブジェクトに対する権限委譲操作が行なわれたら、前記ユーザに関連付けられたアクセスＵＲＬと、権限委譲ファイル及び前記権限委譲操作に関連付けられたアクセスチケットを生成するアクセスチケット生成工程と、前記アクセスチケット生成工程によって生成されたアクセスチケットを自身の秘密鍵で暗号化した後で、前記アクセスＵＲＬと結合させてアクセストークンを生成するアクセストークン生成工程と、前記アクセストークン生成工程によって生成されたアクセストークンを前記ユーザの公開鍵で暗号化して、前記ネットワークを介して前記ユーザに送信するアクセストークン送信工程とをサーバ端末装置においてコンピュータに実行させることを特徴としている。

また、本発明の他の特徴とするところは、ネットワークに接続可能なクライアント端末装置におけるオブジェクト管理方法をコンピュータに実行させるプログラムにおいて、前記ネットワークを介してサーバ端末装置から送られてくるアクセストークンを受信するアクセストークン受信工程と、前記アクセストークン受信工程によって受信したアクセストークンを自身の秘密鍵で復号して、前記アクセストークンの中からアクセスチケットを抽出するアクセスチケット抽出工程と、前記アクセスチケット抽出工程によって抽出されたアクセスチケットを自身の秘密鍵で暗号化するアクセスチケット暗号化工程と、前記アクセスチケット暗号化工程によって暗号化されたアクセスチケットを前記アクセストークンに戻した後で、権限委譲先の公開鍵で暗号化するアクセストークン暗号化工程と、前記アクセストークン暗号化工程によって暗号化されたアクセストークンを、前記ネットワークを介して前記権限委譲先に送信するアクセストークン送信工程とをクライアント端末装置においてコンピュータに実行させることを特徴としている。

また、本発明の他の特徴とするところは、ネットワークに接続可能なクライアント端末装置におけるオブジェクト管理方法をコンピュータに実行させるプログラムにおいて、前記ネットワークを介して送られてくるアクセストークンを受信するアクセストークン受信工程と、前記アクセストークン受信工程によって受信されたアクセストークンを自身の秘密鍵で復号するアクセストークン復号工程と、前記アクセストークン復号工程によって復号されたアクセストークン中から抽出したアクセスＵＲＬに接続するとともに、前記アクセストークン中から抽出したアクセスチケットを送信するアクセスチケット送信工程とを有することを特徴としている。クライアント端末装置においてコンピュータに実行させることを特徴としている。

また、本発明のその他の特徴とするところは、ネットワークに接続可能なクライアント端末装置におけるオブジェクト管理方法をコンピュータに実行させるプログラムにおいて、前記ネットワークを利用して接続可能な端末装置と通信を行なう通信手段により受信したアクセストークンをデータ保存手段に保存するデータ保存工程と、前記データ保存手段に保存されたアクセストークンを、前記データ保存手段に予め保存された秘密鍵を用いて復号するアクセストークン復号工程と、前記アクセストークン復号工程により復号されたアクセストークンを、接続情報と権限参照情報とに分離する分離工程と、前記分離工程により分離された接続情報が示す場所へ前記通信手段を用いて接続して、前記権限参照情報を送信する接続工程とを有することを特徴としている。

【００１３】

本発明の記録媒体は、前記の何れかに記載のコンピュータプログラムを記録したことを特徴としている。

【発明の効果】

【００１４】

本発明により、ユーザ登録をすることなしに、特定のオブジェクトに対する特定操作権限を任意の第三者に対して安全に委譲することができる。

【発明を実施するための最良の形態】

【００１５】

図１は、本発明のサーバ端末装置、クライアント端末装置、オブジェクト管理システム、オブジェクト管理方法、コンピュータプログラム及び記録媒体の一実施の形態を示すシステム構成図である。情報処理装置１０１はサーバ端末装置と呼ばれ、大容量の記憶装置を有し、複数のトランザクションを高速に処理することが出来るものである。サーバ端末装置１０１は、ＬＡＮ１０２と接続されており、ＬＡＮ１０２を介して、クライアント端末装置と呼ばれる第１の情報処理装置１０３及び第２の情報処理装置１０４と通信を行なうことが可能である。

【００１６】

図２は、本実施の形態におけるサーバ端末装置１０１を実現するモジュール群の内部構成例を示すブロック図である。図２に示したように、ネットワークポート２０１はＬＡＮ１０２と接続され、ＬＡＮ１０２をから受信した信号をデジタルデータに変換してプロトコルスタック２０２に渡したり、逆にプロトコルスタック２０２から受信したデータを信号に変換して、ＬＡＮ１０２に送信したりする。

【００１７】

ＨＴＴＰハンドラ２０３は、プロトコルスタック２０２で識別されたＨＴＴＰプロトコルを処理する。認証部２０５は、ＨＴＴＰハンドラ２０３から渡された認証情報を認証し、画面生成部２０４は、ＨＴＴＰハンドラ２０３の指示により、データ保存部２０７に保存された情報を元に、ＨＴＭＬのような画面情報を生成させる。

【００１８】

認証部２０５は、暗号処理部２０６により暗号データの復号や暗号データの生成を行なう。なお、ＳＳＬ（Secure Socket Layer）やＴＬＳ（Transport Layer Security）のように、プロトコルスタック２０２が暗号処理部２０６と協調動作することで、通信路の安全性を高めることも可能であるが、本発明を実現するためには必須ではない。

【００１９】

図８は、ログイン情報が認証された後に、送信される初期画面情報により構成された初期表示画面８００の一例を示す図である。図８にて示されている新規作成ボタン８０２を押下することにより文書を登録すると、登録文書表示欄８０１に表示される。８０３は更新ボタンであり、この更新ボタン８０３を押下することにより前記登録文書表示欄８０１で選択された文書を新しい文書で置き換えることが出来る。

【００２０】

８０４は削除ボタン、８０５は印刷ボタンであり、これらのボタンを押下すると、それぞれ、登録文書表示欄８０１で選択された文書の削除または印刷を、それぞれのボタンの

押下に応じて行なうことができる。８０７はログアウトボタンであり、押下すると、図７のログイン画面７００が表示される。８０６は、委譲ボタンであり、登録文書表示欄８０１で文書を選択した後に押下すると、図９に示すような権限委譲画面が表示される。

【００２１】

図９は、権限委譲画面９００の構成例を示す図である。図９において、ＯＫボタン９０１を押下することにより、図８の画面において選択した文書に対して、委譲項目欄の印刷９０３、更新９０４、削除９０５のチェックボックスでチェックされた操作を、アクセス回数入力域９０６に設定された回数だけ可能にする。キャンセルボタン９０２を押下すると、現在の設定を破棄して、図８の初期画面表示８００に遷移する。

【００２２】

図１０は、図９の権限委譲画面９００で、ＯＫボタン９０１が押下された場合に生成されるアクセストークンのデータフォーマットである。アクセストークン１００１は、暗号化されたアクセスチケット１００４と、アクセスチケット１００４へのオフセット１００２、及びアクセスチケット１００４に対応した権限を操作可能な画面へのアクセスを識別するアクセスＵＲＬ１００３とから構成されている。

【００２３】

以下、図３～図６のフローチャートを用いて、本発明のオブジェクト管理システムの具体例を説明する。

図３は、本発明を実現するサーバと呼ばれる情報処理装置（図１のサーバ端末装置１０１に相当）におけるログイン処理を示したフローチャートである。通常、サーバ端末装置１０１に登録されたユーザがサーバーバ端末装置１０１に接続した場合は、図７に示すようなログイン画面７００が表示され、それぞれ適切なログイン名とパスワードを入力し、ログインボタン７０３を押下することにより、サーバ端末装置１０１にログインし、文書（オブジェクト）に対する操作を行なうことが出来る。

【００２４】

まず、最初のステップＳ３０１では、図７のログイン画面７００からログイン処理が行われたかどうかを判定する。この判定の結果、ログイン処理が行われた場合にはステップＳ３０２に進み、入力されたログイン名とパスワードが正当かどうかを判定する。この判定の結果、正当であればステップＳ３０３に進み、図８に示した初期表示画面８００のような、オブジェクトに対する全ての操作が可能である画面（フル画面）情報を送信する。なお、画面情報はＨＴＭＬ（Hyper Text Markup Language）のような、クライアント端末装置（ユーザ）側で画面表示が容易な形式が望まれるが、特に、ＨＴＭＬに限定するものではない。

【００２５】

ステップＳ３０３でフル画面情報を送信した後、ステップＳ３１３に進み、画面情報に対して行われた操作に関する処理を行なう。この処理の一例は、図４のフローチャートを用いて後述する。

【００２６】

一方、ステップＳ３０２の判定の結果、入力された情報が登録されたものと異なる場合は、ステップＳ３１１に進み、サーバ端末装置１０１へのアクセスが拒絶されたことを報知する画面情報を送信し、ステップＳ３０１の処理へ戻る。

【００２７】

一方、ステップＳ３０１でログイン画面からのログインでは無いと判定されると、ステップＳ３０４に進み、図１１の１１０１に示すような、限定された操作権限でサーバ端末装置１０１に接続するためのＵＲＬ（アクセスＵＲＬ）に対して接続が行われたかどうかを判定する。この判定の結果、アクセスＵＲＬへの接続でなければ、ステップＳ３０５に進み、終了通知が送られたかどうかを判定し、送られた場合には処理を終了し、送られていなければ、ステップＳ３０１の処理へ戻る。終了通知は、サーバ管理者等により、本発明を実現するプログラムに対して終了操作が行われたことを示す。

【００２８】

ステップＳ３０４の判定の結果、アクセスＵＲＬへの接続であると判定されると、ステップＳ３０６に進み、図１１に示すようなリストを検索し、接続されたＵＲＬがアクセスＵＲＬとしてリストに登録されているかどうかを判定する。リストに登録されていなければ、ステップＳ３１１に進み、登録されているとステップＳ３０７に進む。

【００２９】

ステップＳ３０７では、図１１の１１０２に示すような、アクセスＵＲＬに対応するユーザの公開鍵の保存場所から公開鍵を取得し、ステップＳ３０８で、取得した公開鍵を用いて、アクセスＵＲＬへの接続と同時に受信したアクセスチケット（図１０の１００４に相当）を復号化する。

【００３０】

次に、ステップＳ３０９において、復号化したデータをさらにサーバ端末装置１０１の秘密鍵を用いて復号化する。次に、ステップＳ３１０では、ステップＳ３０９で復号したデータが、図１２に示すアクセスチケットリスト１２０１に登録されているかどうかを判定する。この判定の結果、アクセスチケットリスト１２０１に登録されていなければ、ステップＳ３１１に進み、登録されているとステップＳ３１２に進む。ステップＳ３１２では、後述する限定画面送信処理を行い、ステップＳ３１３の画面に対応する操作処理へと進む。

【００３１】

また、ステップＳ３０４でアクセスＵＲＬへの接続があると、図１０の１００４に示すようなアクセスチケット１００４を受信する。前記アクセスチケット１００４は、ＤＥＳのような共通鍵暗号方式を用いて生成した、サーバ端末装置１０１の秘密鍵で暗号化された後、ファイルの所有者により、ＲＳＡのような公開鍵暗号方式を用いて生成した、所有者の秘密鍵でさらに暗号化されている。

【００３２】

前記公開鍵暗号方式においては、ある秘密鍵で暗号化されたデータは、秘密鍵に対応した公開鍵を用いなければ復号化できず、逆にある公開鍵で正常に復号されるデータは、それに対応した秘密鍵で暗号化する必要があることから、ステップ３０４で受信したデータが不正に生成されたデータであった場合、ステップＳ３０８及びＳ３０９で復号されたデータは不当なものとなる。

【００３３】

図４は、図３のステップ３１２において行なわれる限定画面生成処理を示したフローチャートである。

限定画面生成処理が開始されると、最初のステップＳ４０１で、サーバ端末装置１０１のデータ保存部２０７に保存されている限定画面の雛型となる限定画面テンプレートを選択する。この限定画面テンプレートは、ＨＴＭＬのような画面情報フォーマットを用いて予め作成されたものである。前記限定画面テンプレートは、図８に示したような、初期表示画面８００のうち、委譲ボタン８０６を取り除いた画面を生成するような画面情報である。

【００３４】

次に、ステップＳ４０２に進み、印刷フラグがＯＮになっているか否かを判定する。前記印刷フラグは、図３のステップＳ３０９で復号されたアクセスチケット１００４に対応した、図１２に示すようなアクセスフラグ欄１２０２において、印刷欄が「ＴＲＵＥ」と記載されているか否かによって判定する。この判定の結果、印刷フラグがＯＮで無ければ（印刷欄が「ＦＡＬＳＥ」と記載されていれば）、ステップ４０３に進み、ステップＳ４０１で選択したテンプレートから印刷ボタンに関する情報を削除する。

【００３５】

ステップＳ４０２の判定の結果、印刷フラグがＯＮになっている場合にはステップＳ４０４に進み、削除フラグがＯＮかどうかを判定する。この判定の結果、削除フラグがＯＮで無ければ、ステップＳ４０５に進み、テンプレートから削除ボタンに関する情報を削除する。また、ステップＳ４０４の判定の結果、削除フラグがＯＮになっている場合にはス

テップＳ４０６に進む。

【００３６】

ステップＳ４０６では、更新フラグがＯＮかどうかを判定し、ＯＮで無ければステップＳ４０７に進んで更新ボタンに関する情報を削除し、その後、ステップＳ４０８に進む。一方、ステップＳ４０６の判定の結果、更新フラグがＯＮであった場合にはステップＳ４０８に進む。

【００３７】

ステップＳ４０８においては、アクセスチケットに対応したファイル名を、図１２のファイル名欄１２０３から取得して、テンプレートの文書一覧に相当する情報に設定する。その後、ステップＳ４０９に進み、テンプレートを接続元の情報処理装置（クライアント端末装置）に送信することにより、アクセスチケット１２０１に対応する委譲された権限のみが操作可能な画面がクライアント端末装置で表示されることになる。

【００３８】

図５は、図３のフローチャートにおけるステップＳ３１３に示す画面操作処理のうち、図８の委譲ボタン８０６を押下した際の処理を示すフローチャートである。

処理が開始されると、最初のステップＳ５０１において、図８の登録文書表示覧８０１において文書が選択されているかどうかを判定する。この判定の結果、文書が選択されていなければ、ステップＳ５０２で選択無しエラー画面情報を送信後、ステップＳ５１５で初期画面を送信して処理を終了する。また、ステップＳ５０１の判定の結果、文書が選択されていると、ステップＳ５０３に進み、図９に示したような権限委譲画面９００を表示するような画面情報を送信する。

【００３９】

次に、ステップＳ５０４に進み、図９のＯＫボタン９０１が押下されたかどうかを判定し、押下されていなければ、ステップＳ５０５に進んでキャンセルボタン９０２が押下されたかどうかを判定する。この判定の結果、キャンセルボタン９０２が押下されていなければ、ステップＳ５０４の処理に戻る。また、キャンセルボタン９０２が押下されていると、ステップＳ５１６で初期画面情報を送信して処理を終了する。

【００４０】

一方、ステップＳ５０４の判定の結果、ＯＫボタンが押下されると、ステップＳ５０６に進み、図１０に示したアクセスチケット１００４を生成し、図１２のアクセスチケットリストに追加する。アクセスチケット１００４は、サーバ端末装置１０１の起動中に、決して重複しない任意のバイト列である。

【００４１】

次に、ステップＳ５０７で委譲項目を設定する。前記委譲項目の設定においては、図９の委譲項目欄で、チェックボックスにチェックがされている項目に対応する、図１２のアクセスチケットリスト１２０１のアクセスフラグ欄にＴＲＵＥを設定し、チェックされていない項目に対応するアクセスフラグ欄にＦＡＬＳＥを設定して行なう。

【００４２】

次のステップＳ５０８では、アクセスＵＲＬを生成し、図１１のリストに追加する。次に、ステップＳ５０９では、ステップＳ５０６で生成したアクセスチケットを、ＤＥＳのような共通鍵暗号方式を用いて生成したサーバ端末装置１０１の暗号鍵で暗号化する。

【００４３】

次に、ステップＳ５１０では、アクセスチケットへのオフセットと、ステップＳ５０８で生成したアクセスＵＲＬ、そしてステップＳ５０９で暗号化したアクセスチケットとを結合した、図１０に示したような、非暗号化アクセストークン１００１を生成する。

【００４４】

次に、ステップＳ５１１に進み、図１１のリストに記載された情報に基づき、接続ユーザに対応した公開鍵を取得して、この取得した公開鍵を用いて前記非暗号化アクセストークン１００１を暗号化する。

【００４５】

次に、ステップＳ５１２で、暗号化したアクセストークンを接続ユーザが使用しているクライアント端末装置に保存させるような情報を記載した、アクセストークン保存画面情報を送信する。次に、ステップＳ５１３で、ＯＫボタンが押下されたか否かを判定し、押下されるとステップＳ５１４で、クライアント端末装置にアクセストークンを送信した後、図８のような初期画面情報を送信して処理を終了する。

【００４６】

ユーザが操作権限を第三者に委譲する場合には、以下に説明する操作を行なう。

アクセストークンを受信したユーザが、第三者に対してこのアクセストークンに設定された操作を委譲したい場合には、まず、自身の暗号鍵を用いてアクセストークンを復号する。そして、復号したアクセストークンを取り出し、これを自身の暗号鍵を用いて暗号化し、オフセット１００２とアクセスＵＲＬ１００３とを結合して、非暗号化アクセストークン１００１を生成後、第三者の公開鍵を用いて、前記非暗号化アクセストークン１００１を暗号化して、電子メールなどを用いて第三者に受け渡す。

【００４７】

図６のフローチャートに示すように、アクセストークンを受け取った第三者は、ステップＳ６０１でアクセストークンを、自身の秘密鍵で復号した後、ステップＳ６０２でアクセスＵＲＬ１００３とアクセスチケット１００４とに分離し、次に、ステップＳ６０３でアクセスＵＲＬに対して接続し、ステップＳ６０４でアクセスチケット１００４を送信する。

【００４８】

アクセスＵＲＬに接続を受けたサーバ端末装置１０１は、前記図３のステップＳ３０６以降の処理を実行することで、アクセスチケットに対応した操作を可能とする画面情報を前記第三者に送信することが可能となる。これにより、前記第三者は特定の操作を実行することを委譲されたことになる。

【００４９】

図１３に、前記クライアント端末装置１０３、１０４を構成可能なコンピュータシステムの一例を示す。

【００５０】

図１３において、１３００はコンピュータＰＣである。ＰＣ１３００は、ＣＰＵ１３０１を備え、ＲＯＭ１３０２またはハードディスク（ＨＤ）１３１１に記憶された、あるいはフレキシブルディスクドライブ（ＦＤ）１３１２より供給されるデバイス制御ソフトウェアを実行し、システムバス１３０４に接続される各デバイスを総括的に制御する。

【００５１】

前記ＰＣ１３００のＣＰＵ１３０１，ＲＯＭ１３０２またはハードディスク（ＨＤ）１３１１に記憶されたプログラムにより、本実施の形態の各機能手段が構成される。

【００５２】

１３０３はＲＡＭで、ＣＰＵ１３０１の主メモリ、ワークエリア等として機能する。１３０５はキーボードコントローラ（ＫＢＣ）であり、キーボード（ＫＢ）１３０９から入力される信号をシステム本体内に入力する制御を行なう。１３０６は表示コントローラ（ＣＲＴＣ）であり、表示装置（ＣＲＴ）１３１０上の表示制御を行なう。１３０７はディスクコントローラ（ＤＫＣ）で、ブートプログラム（起動プログラム：パソコンのハードやソフトの実行（動作）を開始するプログラム）、複数のアプリケーション、編集ファイル、ユーザファイルそしてネットワーク管理プログラム等を記憶するハードディスク（ＨＤ）１３１１、及びフレキシブルディスク（ＦＤ）１３１２とのアクセスを制御する。

【００５３】

１３０８はネットワークインタフェースカード（ＮＩＣ）で、ＬＡＮ１３２０を介して、ネットワークプリンタ、他のネットワーク機器、あるいは他のＰＣと双方向のデータのやり取りを行なう。

【００５４】

以上、説明したように、本実施の形態のオブジェクト管理システムによれば、サーバ端

末装置と呼ばれる情報処理装置において、登録されたユーザからの指定ファイルの権限委譲要求に対して、委譲権限に対応するアクセスチケットと、登録ユーザに対応するアクセスＵＲＬを生成及び管理し、アクセスチケットをサーバ端末装置１０１が有する暗号鍵により暗号化した後、オフセット情報及びアクセスＵＲＬと結合し（これをアクセストークンと呼ぶ）、登録ユーザの公開鍵で暗号化して、ユーザに送信する。

【００５５】

アクセストークンを受信したユーザは、アクセストークンに関連付けられたサーバ端末装置１０１上のファイルの特定操作を第三者に委譲することを所望する際に、アクセストークンを自身の暗号鍵で復号し、アクセストークンに含まれるアクセスチケットを取り出し、自身の暗号鍵で暗号化を行ったのち、アクセストークンに戻し、アクセストークン全体を、特定操作権限を委譲する第三者の公開鍵で暗号化して、前記特定操作権限を委譲する第三者に送信する。

【００５６】

第三者は、アクセストークンを自身の秘密鍵で復号し、前記復号したアクセストークンをアクセスＵＲＬ１００３とアクセスチケット１００４とに分離する。次いで、アクセスＵＲＬに接続してアクセスチケット１００４を送信する。

【００５７】

前記アクセスチケット１００４を受け取ると、サーバ端末装置１０１は、アクセスＵＲＬに関連付けられたユーザの公開鍵を使ってアクセスチケットを復号した後、さらに自身の秘密鍵で復号したものをリストから検索することで、アクセスチケットに関連付けられたファイルの特定操作を可能にする画面情報を、第三者に対して送信する。これにより、第三者はアクセスチケットに関連付けられたファイルの特定を行なうことを可能にするものである。

【００５８】

この際、本実施の形態のオブジェクト管理システムにおいては、アクセスチケットを暗号化して送信するようにしているので、サーバ端末装置１０１と登録ユーザとの間、登録ユーザと操作権限を委譲する第三者との間、そして第三者とサーバ端末装置１０１との間で、権限委譲データを安全に送受信することができることを最大の特徴としている。

【００５９】

（本発明の他の実施の形態）

前述した実施の形態の機能を実現するべく各種のデバイスを動作させるように、前記各種デバイスと接続された装置あるいはシステム内のコンピュータに対し、前記実施の形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステムあるいは装置のコンピュータ（ＣＰＵあるいはＭＰＵ）に格納されたプログラムに従って前記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

【００６０】

また、この場合、前記ソフトウェアのプログラムコード自体が前述した実施の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自体、およびそのプログラムコードをコンピュータに供給するための手段、例えば、かかるプログラムコードを格納した記録媒体は本発明を構成する。かかるプログラムコードを記録する記録媒体としては、例えばフレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【００６１】

また、コンピュータが供給されたプログラムコードを実行することにより、前述の実施の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がコンピュータにおいて稼働しているＯＳ（オペレーティングシステム）あるいは他のアプリケーションソフト等と共同して前述の実施の形態の機能が実現される場合にもかかるプログラムコードは本発明の実施の形態に含まれる。

【００６２】

さらに、供給されたプログラムコードがコンピュータの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格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等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の形態の機能が実現される場合にも本発明に含まれる。

【図面の簡単な説明】

【００６３】

【図１】本発明の実施の形態を示し、システム構成図である。

【図２】本発明の実施の形態を示し、サーバにおけるモジュール構成図である。

【図３】本発明の実施の形態を示し、サーバにおける認証処理手順の一例を示すフローチャートである。

【図４】本発明の実施の形態を示し、サーバにおける限定画面生成処理手順の一例を示すフローチャートである。

【図５】本発明の実施の形態を示し、サーバにおけるアクセストークン生成処理手順の一例を示すフローチャートである。

【図６】本発明の実施の形態を示し、操作権限委譲先におけるサーバ接続処理手順の一例を示すフローチャートである。

【図７】本発明の実施の形態を示し、ログイン画面の一例を示す図である。

【図８】本発明の実施の形態を示し、初期画面の一例を示す図である。

【図９】本発明の実施の形態を示し、権限委譲画面の一例を示す図である。

【図１０】本発明の実施の形態を示し、アクセストークンのデータ形式例を示す図である。

【図１１】本発明の実施の形態を示し、サーバで管理されるアクセスＵＲＬリストの一例を示す図である。

【図１２】本発明の実施の形態を示し、サーバで管理されるアクセスチケットリストの一例を示す図である。

【図１３】本発明の実施の形態を示し、クライアント端末装置を構成可能なコンピュータシステムの一例を示すブロック図である。

【符号の説明】

【００６４】

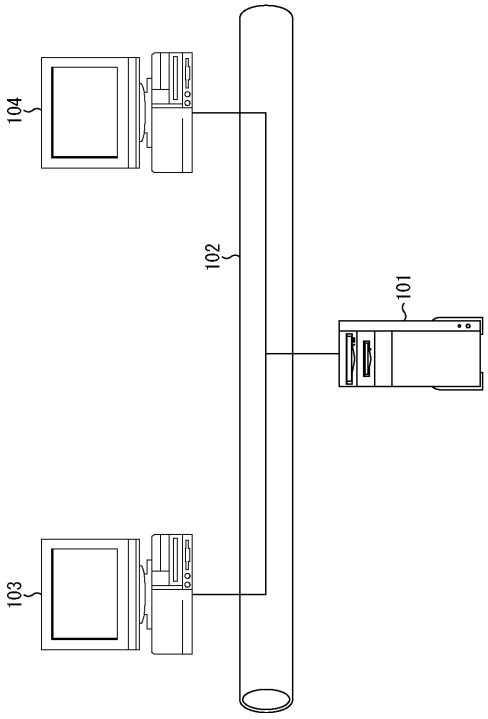
１０１　サーバ端末装置

１０２　ＬＡＮ

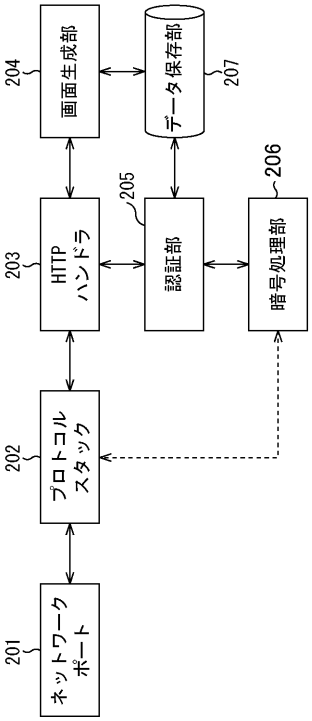
１０３　クライアント端末装置

１０４　クライアント端末装置

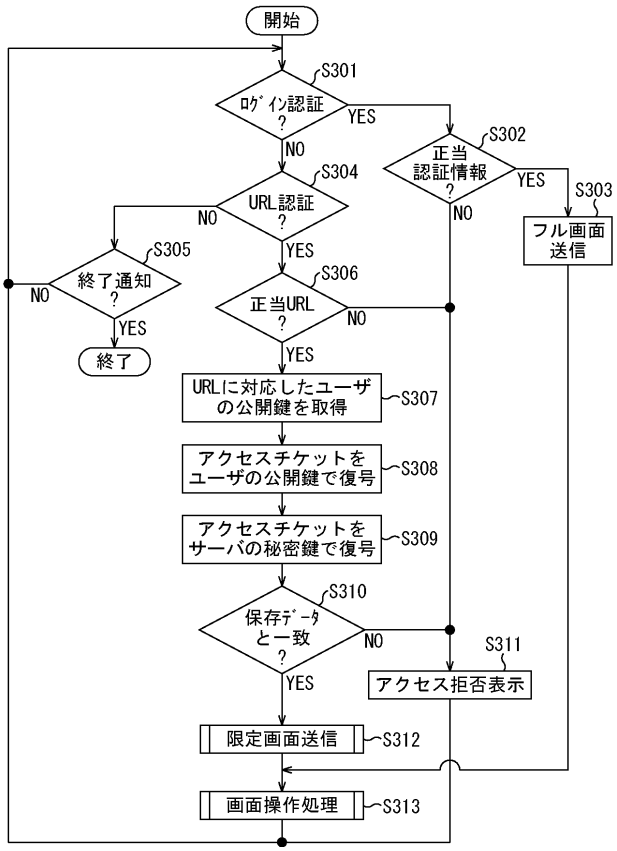
【図１】


104
102
101
103

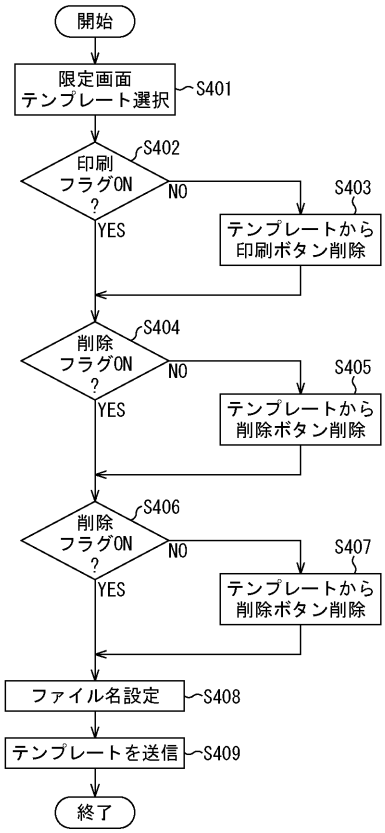
【図２】


204
画面生成部
データ保存部
207
205
206
203
HTTP
ハンドラ
認証部
暗号処理部
202
プロトコル
スタック
201
ネットワーク
ポート

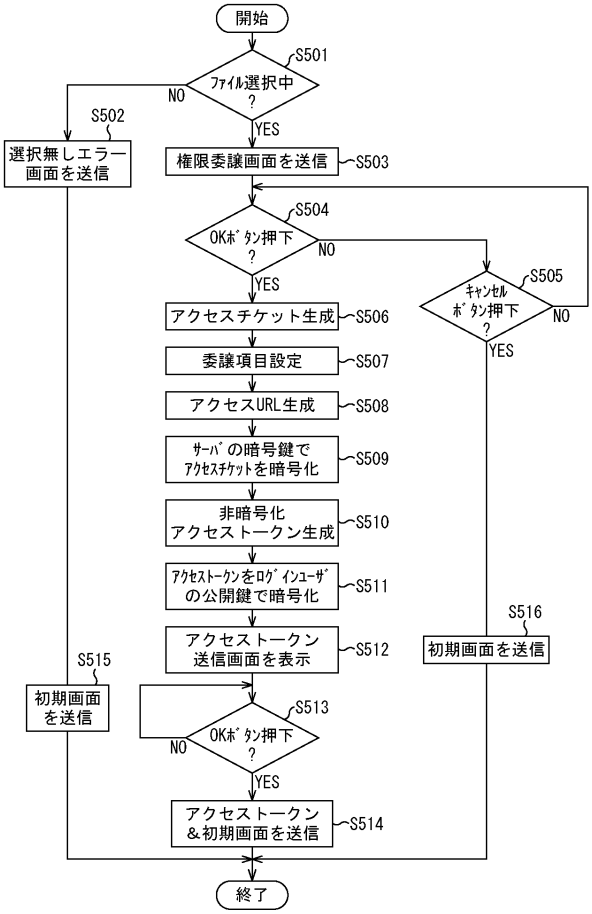
【図３】


開始
S301
ﾛｸﾞｲﾝ認証
?
YES
NO
S302
正当
認証情報
?
YES
NO
S303
フル画面
送信
S304
URL認証
?
NO
YES
S305
終了通知
?
NO
YES
終了
S306
正当URL
?
NO
YES
URLに対応したユーザ
の公開鍵を取得
S307
アクセスチケットを
ユーザの公開鍵で復号
S308
アクセスチケットを
サーバの秘密鍵で復号
S309
S310
保存ﾃﾞｰﾀ
と一致
?
NO
YES
S311
アクセス拒否表示
限定画面送信
S312
画面操作処理
S313

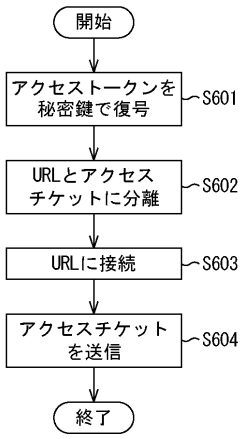
【図４】


開始
限定画面
テンプレート選択
S401
S402
印刷
フラグON
?
NO
YES
S403
テンプレートから
印刷ボタン削除
S404
削除
フラグON
?
NO
YES
S405
テンプレートから
削除ボタン削除
S406
削除
フラグON
?
NO
YES
S407
テンプレートから
削除ボタン削除
ファイル名設定
S408
テンプレートを送信
S409
終了

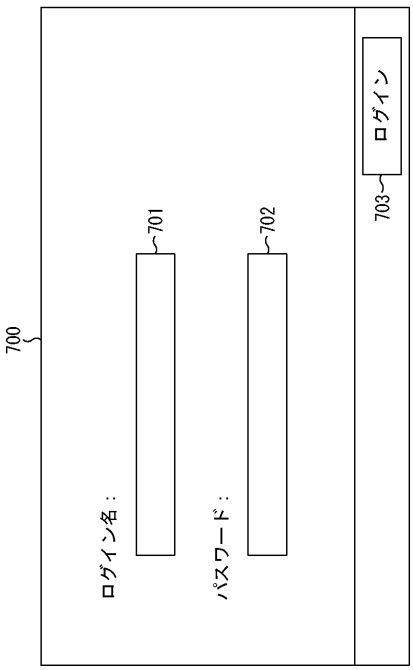
【図５】


開始
S501
ﾌｧｲﾙ選択中？
NO
YES
S502
選択無しエラー画面を送信
権限委譲画面を送信
S503
S504
OKﾎﾞﾀﾝ押下？
NO
YES
S505
ｷｬﾝｾﾙﾎﾞﾀﾝ押下？
NO
YES
アクセスチケット生成
S506
委譲項目設定
S507
アクセスURL生成
S508
ｻｰﾊﾞの暗号鍵でｱｸｾｽﾁｹｯﾄを暗号化
S509
非暗号化アクセストークン生成
S510
ｱｸｾｽﾄｰｸﾝをﾛｸﾞｲﾝﾕｰｻﾞの公開鍵で暗号化
S511
アクセストークン送信画面を表示
S512
S513
OKﾎﾞﾀﾝ押下？
NO
YES
アクセストークン＆初期画面を送信
S514
S515
初期画面を送信
S516
初期画面を送信
終了

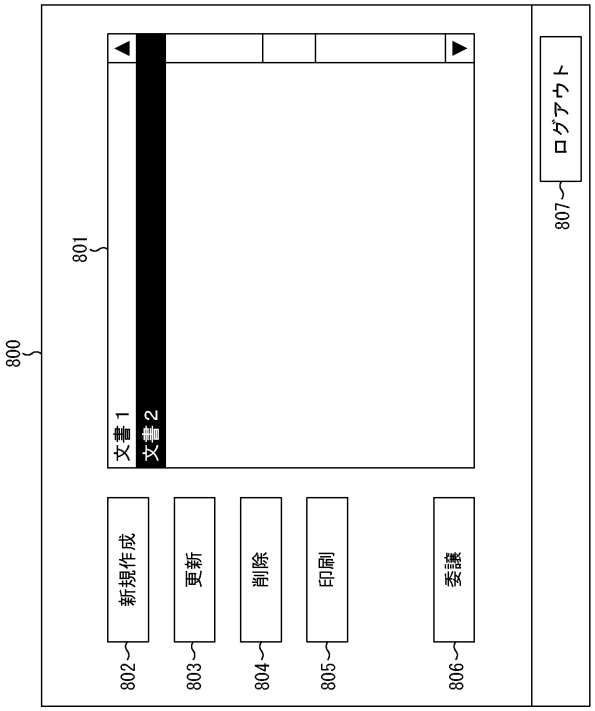
【図６】


開始
アクセストークンを秘密鍵で復号
S601
URLとアクセスチケットに分離
S602
URLに接続
S603
アクセスチケットを送信
S604
終了

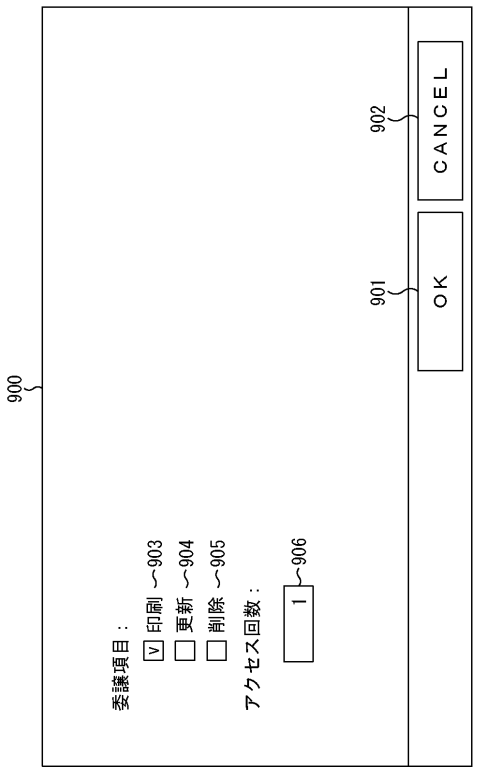
【図７】


700
701
702
703
ログイン
ログイン名：
パスワード：

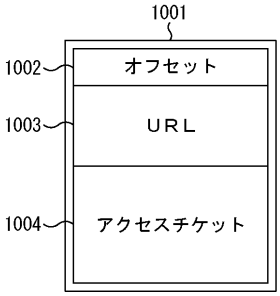
【図８】


800
801
807
ログアウト
文書1
文書2
新規作成
更新
削除
印刷
委譲
802
803
804
805
806

【図９】



【図１０】

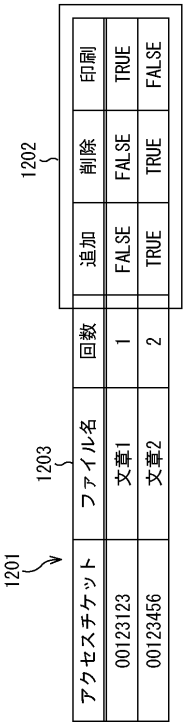


【図１１】

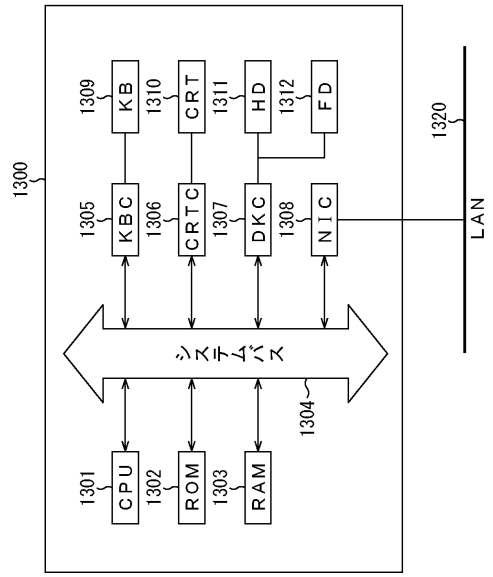
1101 1102

ユーザ名	アクセス URL	公開鍵保存先
User1@foo.com	http://foo.com/service1/ABCDE	http://foo.bar/service1/ABCDE
User2@bar.com	http://foo.com/service2/ZYXWV	file://c:/repository/user2

【図１２】



【図１３】


1300
1309
KB
1310
CRT
1311
HD
1312
FD
1320
LAN
1305
KBC
1306
CRTC
1307
DKC
1308
NIC
システムバス
1304
1301
CPU
1302
ROM
1303
RAM