(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2009-93670
(P2009-93670A)
(43)公開日　平成21年4月30日(2009.4.30)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	520A	5B017
G06F 21/20	(2006.01)	G06F	12/14	530B	5B082
G06F 12/00	(2006.01)	G06F	12/14	540A	5B285
H04L 9/32	(2006.01)	G06F	12/14	560B	5J104
		G06F	15/00	330A	

審査請求 有　請求項の数 5　ＯＬ　（全 23 頁）　最終頁に続く

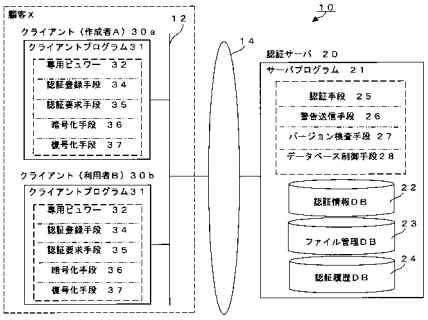
(21)出願番号　特願2008-308488 (P2008-308488)
(22)出願日　平成20年12月3日 (2008.12.3)
(62)分割の表示　特願2004-153945 (P2004-153945)の分割
原出願日　平成16年5月24日 (2004.5.24)
(31)優先権主張番号　特願2003-373340 (P2003-373340)
(32)優先日　平成15年10月31日 (2003.10.31)
(33)優先権主張国　日本国(JP)

(71)出願人　500003693
マルチネット株式会社
東京都新宿区西新宿２丁目４番１号
(74)代理人　110000187
特許業務法人ウィンテック
(72)発明者　大池　潔
東京都新宿区西新宿２丁目４番１号　マルチネット株式会社内

Ｆターム(参考)　5B017 AA03 BA06 BA07 BB09 CA16
5B082 GA11 HA08
5B285 AA02 BA07 CA02 CA12 CA16 CA41 CA43 CA45 CB02 CB52 CB53 CB55 CB62 CB73 CB83
5J104 AA07 AA16 EA04 EA15 EA16 KA01 KA02 KA04 MA01 MA05 NA02 NA27 NA37 PA14

(54)【発明の名称】ファイルのセキュリティー管理システムおよび認証サーバ、クライアント装置ならびにプログラムおよび記録媒体

(57)【要約】
【課題】ファイルを暗号化しまたは暗号化ファイルを利用するクライアント装置と認証サーバとからなるファイルのセキュリティー管理システムにおいて、セキュリティーを向上することのできる管理システム、認証サーバ等を提供する。
【解決手段】ファイル作成者（クライアント装置３０ａ）は、専用ビュワー３２を用いて暗号化するファイルと利用者と許可する利用権限を設定してこれを認証サーバ２０に登録する。暗号化ファイルを受け取った利用者（クライアント装置３０ｂ）は専用ビュワー３２を用いて認証サーバ２０の認証を受け、専用ビュワー３２上で、該利用者に許可された利用権限の範囲内で暗号化ファイルの復号、利用ができる。従って利用者の手元に鍵および復号化ファイルを残すことがなく、安全性が向上する。また、認証サーバは認証結果が否定であった場合にファイル作成者などに警告を送るから、関係者が直ちに原因を調査することができる。
【選択図】図２



【特許請求の範囲】
【請求項１】
認証サーバとネットワークを介して接続される専用ビュワーを有する複数のクライアント装置で構成されるファイルのセキュリティー管理システムにおいて、
ファイルを暗号化する際、専用ビュワーを介して該ファイルの利用者および該利用者に許可する利用権限を設定して該ファイルを暗号化する暗号化手段と、暗号化したファイルの識別情報、設定した利用者および利用権限情報とを認証サーバに登録する認証登録手段とを備えたクライアント装置であって、
受け取った暗号化ファイルを利用する際、前記専用ビュワーを介して前記認証サーバに認証を求める認証要求手段を備え、前記専用ビュワーを介して認証サーバから送信される利用権限情報と鍵情報に基づいて前記受け取った暗号化ファイルを復号化する復号化手段を備えたクライアント装置と、
ファイルを暗号化するユーザおよび／または暗号化されたファイルを利用するユーザを登録した認証情報データベースと、暗号化ファイルを復号化するための鍵情報と、前記クライアント装置から登録された暗号化ファイルの識別情報、利用者および利用権限情報とを記憶したファイル管理データベースと、クライアント装置からの認証要求に基づいて、前記データベースを参照してユーザおよび前記設定された利用者の認証を行う認証手段とを備え、認証結果が肯定である場合、当該暗号化ファイルに対して設定された利用権限情報と鍵情報とを前記クライアント装置に送信する認証サーバとからなることを特徴とするファイルのセキュリティー管理システム。
【請求項２】
ネットワークを介して接続される専用ビュワーを有する複数のクライアント装置に接続され、ファイルのセキュリティー管理の認証を行う認証サーバにおいて、
ファイルを暗号化する際、専用ビュワーを介して該ファイルの利用者および該利用者に許可する利用権限を設定して該ファイルを暗号化する暗号化手段と、暗号化したファイルの識別情報、設定した利用者および利用権限情報とを認証サーバに登録する認証登録手段とを備えたクライアント装置であって、
受け取った暗号化ファイルを利用する際、前記専用ビュワーを介して前記認証サーバに認証を求める認証要求手段を備え、前記専用ビュワーを介して認証サーバから送信される利用権限情報と鍵情報に基づいて前記受け取った暗号化ファイルを復号化する復号化手段を備えたクライアント装置との間で通信し、
ファイルを暗号化するユーザおよび／または暗号化されたファイルを利用するユーザを登録した認証情報データベースと、暗号化ファイルを復号化するための鍵情報と、前記クライアント装置から登録された暗号化ファイルの識別情報、利用者および利用権限情報とを記憶したファイル管理データベースと、クライアント装置からの認証要求に基づいて、前記データベースを参照してユーザおよび前記設定された利用者の認証を行う認証手段とを備え、認証結果が肯定である場合、当該暗号化ファイルに対して設定された利用権限情報と鍵情報とを前記クライアント装置に送信することを特徴とする認証サーバ。
【請求項３】
ファイルを暗号化する際、専用ビュワーを介して該ファイルの利用者および該利用者に許可する利用権限を設定して該ファイルを暗号化する暗号化手段と、暗号化したファイルの識別情報、設定した利用者および利用権限情報とを認証サーバに登録する認証登録手段とを備えたクライアント装置であって、
受け取った暗号化ファイルを利用する際、前記専用ビュワーを介して前記認証サーバに認証を求める認証要求手段を備え、前記専用ビュワーを介して認証サーバから送信される利用権限情報と鍵情報に基づいて前記受け取った暗号化ファイルを復号化する復号化手段を備えたクライアント装置との間で通信する認証サーバを構成するコンピュータに、
クライアント装置からの認証要求に基づいて、ファイルを暗号化するユーザおよび／または暗号化されたファイルを利用するユーザを登録した認証情報データベースと、暗号化ファイルを復号化するための鍵情報と、前記クライアント装置から登録された暗号化ファ

イルの識別情報、利用者および利用権限情報とを記憶したファイル管理データベースとを参照し、ユーザおよび前記設定された利用者の認証を行う認証手段としての機能を実行させ、

認証結果が肯定である場合、当該暗号化ファイルに対して設定された利用権限情報と鍵情報とを前記クライアント装置に送信する機能を実行させることを特徴とするプログラム。

【請求項４】

ファイルのセキュリティー管理の認証を行う認証サーバにネットワークを介して接続される専用ビュワーを有するクライアント装置において、

ファイルを暗号化するユーザおよび／または暗号化されたファイルを利用するユーザを登録した認証情報データベースと、暗号化ファイルを復号化するための鍵情報と、前記クライアント装置から登録された暗号化ファイルの識別情報、利用者および利用権限情報とを記憶したファイル管理データベースと、クライアント装置からの認証要求に基づいて、前記データベースを参照してユーザおよび前記設定された利用者の認証を行う認証手段とを備え、認証結果が肯定である場合、当該暗号化ファイルに対して設定された利用権限情報と鍵情報とを前記クライアント装置に送信する認証サーバとの間で通信し、

ファイルを暗号化する際、専用ビュワーを介して該ファイルの利用者および該利用者に許可する利用権限を設定して該ファイルを暗号化する暗号化手段と、暗号化したファイルの識別情報、設定した利用者および利用権限情報とを認証サーバに登録する認証登録手段とを備えたクライアント装置であって、

受け取った暗号化ファイルを利用する際、前記専用ビュワーを介して前記認証サーバに認証を求める認証要求手段を備え、前記専用ビュワーを介して認証サーバから送信される利用権限情報と鍵情報に基づいて前記受け取った暗号化ファイルを復号化する復号化手段とを備えたことを特徴とするクライアント装置。

【請求項５】

ファイルを暗号化するユーザおよび／または暗号化されたファイルを利用するユーザを登録した認証情報データベースと、暗号化ファイルを復号化するための鍵情報と、前記クライアント装置から登録された暗号化ファイルの識別情報、利用者および利用権限情報とを記憶したファイル管理データベースと、クライアント装置からの認証要求に基づいて、前記データベースを参照してユーザおよび前記設定された利用者の認証を行う認証手段とを備え、認証結果が肯定である場合、当該暗号化ファイルに対して設定された利用権限情報と鍵情報とを前記クライアント装置に送信する認証サーバとの間で通信するクライアント装置を構成するコンピュータに、

ファイルを暗号化する際、専用ビュワーを介して該ファイルの利用者および該利用者に許可する利用権限を設定して該ファイルを暗号化する暗号化手段と、暗号化したファイルの識別情報、設定した利用者および利用権限情報とを認証サーバに登録する認証登録手段としての機能を実行させ、

受け取った暗号化ファイルを利用する際、前記専用ビュワーを介して前記認証サーバに認証を求める認証要求手段と、前記専用ビュワーを介して認証サーバから送信される利用権限情報と鍵情報に基づいて前記受け取った暗号化ファイルを復号化する復号化手段としての機能を実行させることを特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、デジタルコンテンツを記録したファイルの不正利用を防止するセキュリティー管理システム、認証サーバ、クライアント装置ならびにプログラムおよび記録媒体に関するものであり、特に、クライアント装置と、該クライアント装置が利用者と利用者に許可する利用権限を設定して作成した暗号化ファイルを利用する利用者の認証を行い、その暗号化ファイルを復号化するための鍵情報の管理を行う認証サーバとから構成されるファイルのセキュリティー管理システムおよび認証サーバ、クライアント装置ならびにプログ

ラムおよび記録媒体に関するものである。

【背景技術】

【０００２】

近年の情報処理技術および通信ネットワーク技術の発展にともない、文書、図形、画像、データベースなど様々なデジタルコンテンツ（以下デジタル情報という）をネットワーク経由で販売したり、企業内の組織やプロジェクトに属する複数の人々がファイル形式で作成したデジタル情報を相互に利用しながら業務を進めたりすることが一般的になってきている。

【０００３】

しかしながら、これらのデジタル情報は複製が容易であり、かつ、何度も複製を重ねても情報の劣化がなく、正当な利用権限を取得せずに不正に複製物を作成し、利用することが容易であるという問題が存在する。また、企業内のデジタル情報には秘密性の高い情報も多く存在し、企業内のネットワークに不正に侵入して秘密情報を盗み出す行為も可能であり、企業内の関係者が秘密情報を複製して外部に持ち出すことも容易であるという問題点が存在する。更に、これらのデジタル情報をインターネットなどの通信ネットワークを介して関係者間で送受信する際に、第３者が当該デジタル情報をネットワークから盗み出す行為も一定の知識を持っていれば可能であるという問題点も存在する。

【０００４】

このような問題点に対処するために様々な技術が開発されており、なかでもデジタル情報の暗号化技術が多く採用されている。そのための暗号アルゴリズムも種々開発されており、一般的に広く用いられている暗号化技術は、通常の平文を容易に解読できない暗号文に変換したり、元に戻したりする。暗号化／復号化（平文化ともいう）の変換は暗号鍵によって制御される暗号アルゴリズムによって実行される。

【０００５】

代表的な暗号化方式として非対称公開鍵暗号といわれる方式がある。この公開鍵暗号方式は、各人（あるいは各端末）が、暗号化鍵と平文化鍵を一対ずつ作成し、暗号化鍵を公開（公開鍵ともいわれる）し、平文化鍵を秘密（秘密鍵ともいわれる）に保持する方式である。Ａ宛に暗号文を送信したい人は、誰でもＡが公開した公開鍵（暗号鍵）を用いて、平文を暗号文に変換するのである。その暗号文は秘密鍵（平文化鍵）を持つ受信者Ａのみが平文化できる。したがって、この方式では鍵を配送する必要がない。

【０００６】

また、暗号化と復号化時に共通な共通鍵を用いた非対象暗号系方式を採用し、暗号化されたデジタル情報と同時に暗号化した共通鍵をユーザに送り、共通鍵を知っているユーザのみが解読できるシステムを採用する方法も有る。更に、デジタル署名といわれる方式も知られており、この方式では、情報の秘匿と認証が同時に行われる。すなわち、送信者は、自己の秘密の平文化鍵で暗号化し、さらに、受信者の公開鍵で暗号化して送信する。受信者は、自己の秘密鍵で平文化し、さらに、送信者の公開鍵で平文化する。

【０００７】

しかしながら、これらの暗号アルゴリズムを用いてデジタル情報を暗号化する方式を採用した場合、共通鍵を利用する方法であっても、また公開鍵と秘密鍵を利用する方法であっても暗号化や平文化に必要になる鍵の管理が重要な問題である。すなわち、デジタル情報を記録したファイルの作成者、利用者の認証と、両者間で受け渡す暗号化したファイルと鍵の管理が適正になされないと、ファイルすなわちデジタル情報のセキュリティーを保つことはできない。

【０００８】

例えば、図１４に示すように、（Ｉ）作成者Ａがデジタルコンテンツを記録したファイルを作成し、これを暗号化して利用者Ｂに利用許可する場合、作成者Ａは、（III）暗号化した暗号化ファイルＣを利用者Ｂにネットワークその他の手段を介して送る。この時、（IV）暗号化ファイルを復号化するための鍵Ｄを別ルートで利用者Ｂに伝える方法がある。利用者Ｂは、受け取った暗号化ファイルを別ルートで受け取った鍵Ｄにより復号化する

ことによって、作成者Ａが作成したファイルを復元して利用することができる。また、作成者Ａは（II）鍵を自身で管理する。このような方式では、（V）利用者Ｂの手元には、鍵Ｄが残り、また、復号化したファイル情報も残すことができる。従って、利用者Ｂの手元から鍵や復号化したファイルが悪意の第３者に流出する危険性を排除することができない。これは、公開鍵と秘密鍵を用いる暗号化方式でも基本的には同じであり、秘密鍵が最初から利用者Ｂの手元にあるだけの相違である。

【０００９】

そこで、個々のユーザであるファイルの作成者、利用者との間に第３者機関である鍵センターを介在させ、鍵センターで各ユーザの個人認証をとった上で、ファイル作成者から利用者への鍵の通信を仲介する電子認証方式が下記の特許文献１に開示されている。すなわち、特許文献１に開示された電子認証方式は、個々のユーザとの間に鍵センターなる認証機関を設けたものであり、（Ｉ）ユーザはそれぞれ個人認証のための情報を鍵センターに登録しておく。（II）ユーザＡ（ファイル作成者）がユーザＢ（ファイル利用者）にファイルを送る場合、Ａは鍵センターにＢ宛の通信用鍵（暗号化した鍵）を送る。（III）ユーザＡは通信用鍵で暗号化したファイルをユーザＢに送る。（IV）鍵センターはユーザＢと通信してユーザＢの認証をとる。（V）鍵センターはユーザＢの認証がＯＫであればＡから預かったＢ宛の通信用鍵をＢに送る。（VI）ユーザＢは鍵センターから送られた通信用鍵を使ってＡから受信したファイル（通信用鍵で暗号化された）を復号化する。という手順をとるものである。

【００１０】

【特許文献１】特開２００１－１４４７４５号公報（図１）

【発明の開示】

【発明が解決しようとする課題】

【００１１】

しかしながら、上記特許文献１に開示された電子認証方式では、ファイル作成者とファイル利用者との間に鍵センターを介在させ、鍵センターがユーザ認証をとった上で、ファイル作成者から預かった鍵（暗号化ファイルを復号化するための鍵）をファイル利用者に送るものであり、ユーザ認証のステップが間に入ることによりセキュリティー機能は多少向上するものの、利用者の手元に鍵および復号化されたファイルが残るため、図１４で説明した問題を本質的に解決していないという問題点が存在する。

【００１２】

本願の発明者は、上記の問題点を解消すべく種々検討を重ねた結果、クライアント装置間に認証サーバを介在させること、クライアント装置は専用ビュワーで認証サーバと通信すること、暗号化ファイルに利用者とその利用権限情報を設定すること、利用者は専用ビュワー上で利用権限の範囲内の操作のみが行えるようにすること、を満たすようにファイルのセキュリティーシステムを構成することによって上記問題点を解決できることを見出し、本発明を完成するに至ったものである。

【００１３】

すなわち、本発明は、上記の問題点を解消することを課題とし、クライアント装置と、クライアント装置が利用者と利用者に許可する利用権限を設定して作成した暗号化ファイルを利用する利用者の認証を行い、その暗号化ファイルを復号化するための鍵情報の管理を行う認証サーバとから構成されるファイルのセキュリティー管理システムにおいて、セキュリティー機能を向上したシステムおよび認証サーバ、クライアント装置ならびにプログラムおよび記録媒体を提供することを目的とするものである。

【００１４】

また、本セキュリティーシステムの顧客の間で互いのユーザ情報を公開することなく相互に本セキュリティーサービスを利用できることが好ましい。あるいは、本セキュリティーサービスの顧客とサービス未加入の第３者との間で本セキュリティーサービスを利用できればなお利便性を向上することができる。このため、本発明は、顧客の枠を超えてファイルの暗号化、暗号化ファイルの利用を可能としたファイルのセキュリティーシステムお

よび認証サーバ、クライアント装置ならびにプログラムおよび記録媒体を提供することを第２の目的とする。

【課題を解決するための手段】

【００１５】

前記課題を解決するために、本願の請求項１に係る発明は、認証サーバとネットワークを介して接続される専用ビュワーを有する複数のクライアント装置で構成されるファイルのセキュリティー管理システムにおいて、

ファイルを暗号化する際、専用ビュワーを介して該ファイルの利用者および該利用者に許可する利用権限を設定して該ファイルを暗号化する暗号化手段と、暗号化したファイルの識別情報、設定した利用者および利用権限情報とを認証サーバに登録する認証登録手段とを備えたクライアント装置であって、

受け取った暗号化ファイルを利用する際、前記専用ビュワーを介して前記認証サーバに認証を求める認証要求手段を備え、前記専用ビュワーを介して認証サーバから送信される利用権限情報と鍵情報に基づいて前記受け取った暗号化ファイルを復号化する復号化手段を備えたクライアント装置と、

ファイルを暗号化するユーザおよび／または暗号化されたファイルを利用するユーザを登録した認証情報データベースと、暗号化ファイルを復号化するための鍵情報と、前記クライアント装置から登録された暗号化ファイルの識別情報、利用者および利用権限情報とを記憶したファイル管理データベースと、クライアント装置からの認証要求に基づいて、前記データベースを参照してユーザおよび前記設定された利用者の認証を行う認証手段とを備え、認証結果が肯定である場合、当該暗号化ファイルに対して設定された利用権限情報と鍵情報とを前記クライアント装置に送信する認証サーバとからなることを特徴とする。

【００１６】

また、本願の請求項２に係る発明は、ネットワークを介して接続される専用ビュワーを有する複数のクライアント装置に接続され、ファイルのセキュリティー管理の認証を行う認証サーバにおいて、

ファイルを暗号化する際、専用ビュワーを介して該ファイルの利用者および該利用者に許可する利用権限を設定して該ファイルを暗号化する暗号化手段と、暗号化したファイルの識別情報、設定した利用者および利用権限情報とを認証サーバに登録する認証登録手段とを備えたクライアント装置であって、

受け取った暗号化ファイルを利用する際、前記専用ビュワーを介して前記認証サーバに認証を求める認証要求手段を備え、前記専用ビュワーを介して認証サーバから送信される利用権限情報と鍵情報に基づいて前記受け取った暗号化ファイルを復号化する復号化手段を備えたクライアント装置との間で通信し、

ファイルを暗号化するユーザおよび／または暗号化されたファイルを利用するユーザを登録した認証情報データベースと、暗号化ファイルを復号化するための鍵情報と、前記クライアント装置から登録された暗号化ファイルの識別情報、利用者および利用権限情報とを記憶したファイル管理データベースと、クライアント装置からの認証要求に基づいて、前記データベースを参照してユーザおよび前記設定された利用者の認証を行う認証手段とを備え、認証結果が肯定である場合、当該暗号化ファイルに対して設定された利用権限情報と鍵情報とを前記クライアント装置に送信することを特徴とする。

【００１７】

また、本願の請求項３に係る発明は、ファイルを暗号化する際、専用ビュワーを介して該ファイルの利用者および該利用者に許可する利用権限を設定して該ファイルを暗号化する暗号化手段と、暗号化したファイルの識別情報、設定した利用者および利用権限情報とを認証サーバに登録する認証登録手段とを備えたクライアント装置であって、

受け取った暗号化ファイルを利用する際、前記専用ビュワーを介して前記認証サーバに認証を求める認証要求手段を備え、前記専用ビュワーを介して認証サーバから送信される利用権限情報と鍵情報に基づいて前記受け取った暗号化ファイルを復号化する復号化手段

を備えたクライアント装置との間で通信する認証サーバを構成するコンピュータに、
クライアント装置からの認証要求に基づいて、ファイルを暗号化するユーザおよび／または暗号化されたファイルを利用するユーザを登録した認証情報データベースと、暗号化ファイルを復号化するための鍵情報と、前記クライアント装置から登録された暗号化ファイルの識別情報、利用者および利用権限情報とを記憶したファイル管理データベースとを参照し、ユーザおよび前記設定された利用者の認証を行う認証手段としての機能を実行させ、
認証結果が肯定である場合、当該暗号化ファイルに対して設定された利用権限情報と鍵情報とを前記クライアント装置に送信する機能を実行させることを特徴とするプログラムである。

【００１８】
本願の請求項４に係る発明は、ファイルのセキュリティー管理の認証を行う認証サーバにネットワークを介して接続される専用ビュワーを有するクライアント装置において、
ファイルを暗号化するユーザおよび／または暗号化されたファイルを利用するユーザを登録した認証情報データベースと、暗号化ファイルを復号化するための鍵情報と、前記クライアント装置から登録された暗号化ファイルの識別情報、利用者および利用権限情報とを記憶したファイル管理データベースと、クライアント装置からの認証要求に基づいて、前記データベースを参照してユーザおよび前記設定された利用者の認証を行う認証手段とを備え、認証結果が肯定である場合、当該暗号化ファイルに対して設定された利用権限情報と鍵情報とを前記クライアント装置に送信する認証サーバとの間で通信し、
ファイルを暗号化する際、専用ビュワーを介して該ファイルの利用者および該利用者に許可する利用権限を設定して該ファイルを暗号化する暗号化手段と、暗号化したファイルの識別情報、設定した利用者および利用権限情報とを認証サーバに登録する認証登録手段とを備えたクライアント装置であって、
受け取った暗号化ファイルを利用する際、前記専用ビュワーを介して前記認証サーバに認証を求める認証要求手段を備え、前記専用ビュワーを介して認証サーバから送信される利用権限情報と鍵情報に基づいて前記受け取った暗号化ファイルを復号化する復号化手段と、を備えたことを特徴とする。

【００１９】
また、本願の請求項５に係る発明は、ファイルを暗号化するユーザおよび／または暗号化されたファイルを利用するユーザを登録した認証情報データベースと、暗号化ファイルを復号化するための鍵情報と、前記クライアント装置から登録された暗号化ファイルの識別情報、利用者および利用権限情報とを記憶したファイル管理データベースと、クライアント装置からの認証要求に基づいて、前記データベースを参照してユーザおよび前記設定された利用者の認証を行う認証手段とを備え、認証結果が肯定である場合、当該暗号化ファイルに対して設定された利用権限情報と鍵情報とを前記クライアント装置に送信する認証サーバとの間で通信するクライアント装置を構成するコンピュータに、
ファイルを暗号化する際、専用ビュワーを介して該ファイルの利用者および該利用者に許可する利用権限を設定して該ファイルを暗号化する暗号化手段と、暗号化したファイルの識別情報、設定した利用者および利用権限情報とを認証サーバに登録する認証登録手段としての機能を実行させ、
受け取った暗号化ファイルを利用する際、前記専用ビュワーを介して前記認証サーバに認証を求める認証要求手段と、前記専用ビュワーを介して認証サーバから送信される利用権限情報と鍵情報に基づいて前記受け取った暗号化ファイルを復号化する復号化手段としての機能を実行させることを特徴とするプログラムである。

【発明の効果】
【００２０】
請求項１に係る発明においては、ファイル作成者（作成者側クライアント装置）は、専用ブラウザを用いて暗号化するファイルを設定し、暗号化したファイルを利用する利用者および利用者に許可する利用権限を設定してこれを認証サーバに登録する。暗号化ファイ

ルを受け取った利用者（利用者側クライアント装置）は専用ビュワーを用いて認証サーバの認証を受け、認証サーバが専用ビュワー上で該利用者に許可された利用権限の範囲内で暗号化ファイルの復号化、利用を行わせる。従って、利用者の手元に復号化の鍵情報が残ることがなく、また、利用者に復号化したファイルの閲覧権限しか与えられていない場合には利用者の手元に複合化したファイルも残ることがないため、セキュリティー機能は格段に向上する。また、認証サーバは、利用者から認証要求に対して、また、認証結果が否定であった場合には、ファイル作成者および／またはシステム管理者に警告を送るから、関係者が直ちに原因を調査することができるようになる。このため、認証サーバには、作成者が登録暗号化ファイルの利用者、利用権限の認証履歴を保存する認証履歴データベースを備えることが好ましい。

【００２１】

また、ファイル作成者はファイルの利用を許可する利用者およびその利用権限を設定して認証サーバに登録し、認証サーバはその利用権限の範囲内で利用者にファイルを利用させるものであるから、例えば、利用者への利用権限を復号化したファイルの閲覧のみ、保存を許可、編集保存を許可など複数の権限レベルを設定しておくことで、必要な利用者に必要な権限レベルを与えることができ、また、閲覧のみの権限レベルであっても、更に閲覧回数、閲覧有効期限などの詳細権限を設定できるようになせば、最小の閲覧権限を設定しておくことによって、他人が利用者になりすまして認証サーバの認証を得るようなことがあっても被害を最小限に抑えることができる。

【００２２】

請求項２に係る発明においては、請求項１に係る発明を構成する認証サーバを提供することができる。また、請求項３に係る発明においては、請求項２に係る発明の認証サーバを構成するコンピュータを機能させるプログラムを提供することができる。請求項４に係る発明においては、請求項１に係る発明を構成するクライアント装置を提供することができる。また、請求項５に係る発明においては、請求項４に係る発明のクライアント装置を構成するコンピュータを機能させるプログラムを提供することができる。

【発明を実施するための最良の形態】

【００２３】

以下、本発明の具体例を実施例及び図面を用いて詳細に説明する。図１は、本発明の実施例１に係るファイルのセキュリティー管理システムの基本的機能を示す概念図であり、、図２は、実施例１に係るファイルのセキュリティー管理システムの構成を示すブロック図である。図３は、図２のシステムにおけるファイル作成者側クライアント装置と認証サーバの処理手順を示すフローチャートであり、図４は図２のシステムにおけるファイル利用者側クライアント装置と認証サーバの処理手順を示すフローチャートである。

図５は、本発明の実施例２に係るファイルのセキュリティー管理システムの構成を示すブロック図である。

図６は、本発明の実施例３に係るファイルのセキュリティー管理システムの実施例３の構成を示すブロック図である。図７は、実施例３における認証情報ＤＢ２２と個人アドレス帳ＤＢ４０の構成を示す模式図であり、図８は、実施例３における個人アドレス帳ＤＢ４０への登録手順を示すフローチャートである。図９は、実施例３における認証サーバへのログイン画面の構成を示す図であり、図１０は、実施例３におけるファイル作成者側クライアント装置と認証サーバの処理手順を示すフローチャートである。図１１は、図１０の手順において専用ビュワーに表示される操作画面の一例を示す模式図である。図１２は、実施例３におけるファイル利用者側クライアント装置と認証サーバの処理手順を示すフローチャートでり、図１３は、ファイル利用者が認証サーバのサービスに加入していない場合における利用者側クライアント装置と認証サーバの処理手順を示すフローチャートである。

【実施例１】

【００２４】

本発明の実施例１に係るファイルのセキュリティー管理システムは、図１の概念図に示

すように、作成者Ａが（Ｉ）デジタルコンテンツを記録したファイルを作成し、これを暗号化して利用者Ｂに利用許可する場合、作成者Ａは、専用ビュワーを用いて認証サーバ２０にログインし、暗号化するファイルを指定するとともに、そのファイルの利用を許可する利用者Ｂと利用権限、例えば、利用者Ｂには一度だけの閲覧のみを許可するなどの利用権限を設定してファイルを暗号化する。そして、（II）認証サーバ２０に暗号化したファイルの識別情報（ファイル名など）と利用者および利用権限情報と、暗号化ファイルＣを復号化するための鍵情報Ｄを送信し、認証サーバ２０はこれらの情報をデータベースに登録する。そして、（III）作成者Ａは、利用者Ｂに電子メールその他の手段で暗号化ファイルＣを送る。

【００２５】

認証サーバ２０に登録する鍵情報Ｄは本システムが採用する暗号化方式により異なり、また、作成者Ａがファイルを暗号化する際に認証サーバ２０が鍵を発行する方式を採用することもでき、この場合、作成者Ａから認証サーバ２０に鍵情報Ｄを送る必要はない。

【００２６】

利用者Ｂは、（IV）受け取った暗号化ファイルＣを利用する場合、専用ビュワーを用いて認証サーバ２０にログインして認証を求める。認証サーバ２０には利用者Ｂや作成者Ａなどのユーザを認証するためのユーザ認証データベースがあり、また、作成者Ａが登録した暗号化ファイルの識別情報、その暗号化ファイルＣに対して設定した利用者および利用権限情報、鍵情報Ｄを記憶するファイル管理データベースがあり、各データベースを参照して（V）利用者Ｂのユーザおよび利用者認証がとれれば、該当する暗号化ファイルＣに対して登録された利用権限情報と鍵情報Ｄを利用者側のクライアント装置の専用ビュワーに渡す。

【００２７】

（VI）利用者Ｂは、これによって専用ビュワー上で暗号化ファイルを復号化することができ、その復号化されたファイルを利用することができる。利用者に許可された権限がファイルの閲覧のみの場合、認証サーバ２０から利用者Ｂのクライアント装置に送られた利用権限情報に従って専用ビュワーの操作が制限され、印刷ボタンやファイル保存ボタン、上書き保存ボタンなどの機能は無効にされるため利用者の手元には復号化されたファイルを残すことはできない。同様に復号化の鍵情報Ｄは専用ビュワーによって暗号化ファイルＣの復号化に使われるだけであって、利用者Ｂが暗号化ファイルＣの復号化操作に関与することもなく、また利用者Ｂがこの鍵情報Ｄをクライアント装置に保存する操作を行うこともできない。従って利用者Ｂの手元から復号化されたファイルＣや鍵情報Ｄが流出する危険を防止することができる。

【００２８】

また、図１には図示していないが、認証サーバ２０は、利用者Ｂの認証結果が否定であった場合には、何らかの不都合が生じているものであり、ファイル作成者Ａおよび／または管理者に警告情報を送る。警告を送る管理者は、本システム全体の管理を行うシステム管理者やファイル作成者Ａや利用者Ｂが属する企業内のネットワーク管理者、あるいは、ＩＴ環境監査を担当する部署の管理者などである。これにより関係者は不都合の原因を調査することができる。このため、認証サーバ２０には認証履歴を保存する認証履歴データベースを備えることが好ましい。

【００２９】

図２は、本発明に係るファイルのセキュリティー管理システムの構成を示すブロック図である。図２に示すように本発明に係るファイルのセキュリティー管理システム１０は、認証サーバ２０とクライアント装置３０ａ、３０ｂ等がネットワークを介して接続される構成になっている。図２の場合、認証サーバ２０はＡＳＰ提供業者（Application Service Provider）が運営し、顧客Ｘに対してセキュリティー管理システムのアプリケーションを提供する形態を表している。このため、クライアント装置３０ａ、３０ｂはＬＡＮなどのイントラネット１２に接続され、インターネット１４を介して認証サーバ２０に接続される構成としている。イントラネット１２とインターネット１４の間にはファイヤーウォ

ールを設けたゲートウェイ（図示省略）が介在する。本システムはこのような形態に限らず、１顧客内にクローズしたシステムとして運用することもでき、その場合は認証サーバ２０とクライアント装置３０ａ、３０ｂがイントラネット１２に接続された構成になる。

【００３０】

認証サーバ２０には、サーバプログラム２１がインストールされており、クライアント装置３０ａ、３０ｂを使用するユーザ（ファイル作成者Ａや暗号化ファイルの利用者Ｂ）が登録したユーザＩＤ、パスワードなどの認証情報を記憶した認証情報データベース（認証情報ＤＢ）２２、暗号化ファイルの識別情報（ファイル名）毎に後述の利用者および利用権限の情報を記憶するファイル管理データベース（ファイル管理ＤＢ）２３、ユーザ（クライアント装置）からの認証要求に対する認証の履歴を記憶する認証履歴データベース（認証履歴ＤＢ）２４を有している。

【００３１】

認証サーバ２０を構成するコンピュータはサーバプログラム２１により、認証手段２５、警告送信手段２６、バージョン検査手段２７、データベース制御手段２８の機能を実行する。なお、インターネット１４を介してクライアント装置３０ａ、３０ｂと通信するための通信インタフェース機能などは図示を省略している。

【００３２】

クライアント装置３０ａ、３０ｂはファイルの作成者Ａ、利用者Ｂなどのユーザが使用するものであって、同一の構成をしており、クライアントプログラム３１がインストールされている。クライアント装置３０ａ、３０ｂを構成するコンピュータは、クライアントプログラム３１により機能する専用ビュワー３２を介して認証サーバ２０と通信を行う。また、コンピュータは、クライアントプログラム３１により認証登録手段３４、認証要求手段３５、暗号化手段３６、復号化手段３７の機能を実行する。これらの機能は、ファイルの作成者として利用する場合に使用される機能と、ファイルの利用者として利用する場合に使用される機能とがある。従って、クライアントプログラムをファイル作成者用とファイル利用者用とで別のプログラムとして提供することも可能である。

【００３３】

なお、イントラネット１２、インターネット１４を介して認証サーバ２０と通信するための通信インタフェース機能などは図示を省略している。専用ビュワー３２は特定のアプリケーションを実行するサーバ・クライアント間で通信し、クライアントから情報を入力してサーバに送り、あるいはサーバから受け取った情報を表示したり、印刷したりするためのものであり、ブラウザといわれることもある。以下の説明では、クライアント装置３０ａをファイルの作成者Ａが使用し、クライアント装置３０ｂをファイル（作成者Ａが暗号化したファイル）の利用者Ｂが使用するものとして説明する。

【００３４】

作成者Ａがデジタルコンテンツを記録したファイルを作成し、これを暗号化して利用者Ｂに利用許可する場合、作成者Ａはクライアント装置３０ａを使用し、専用ビュワー３２を用いて認証サーバ２０にログインし、暗号化するファイルを指定するとともに、そのファイルの利用を許可する利用者Ｂと利用権限、例えば、利用者Ｂには一度だけの閲覧のみを許可するなどの利用権限を設定してファイルを暗号化する。この場合、図示は省略するが、専用ビュワー画面にログイン画面が表示され、ユーザＩＤ、パスワード、暗号化するファイルの識別情報（ファイル名）を入力して認証サーバ２０に送信する。

【００３５】

認証サーバ２０が認証情報ＤＢ２２を参照してユーザ認証を行い、ユーザ認証が得られる（認証結果が肯定である）と、作成者Ａは、専用ビュワー３２の利用者設定欄、利用権限設定欄に利用者Ｂおよび利用者Ｂに許可する利用権限を入力する。利用権限とは、例えば、利用者に暗号化ファイルの閲覧のみ許可、復号化したファイルの保存まで許可、復号化したファイルを更新して保存まで許可などの複数の権限レベルである。詳細設定画面で閲覧回数や利用可能期間を設定できるように構成するとなお好適である。

【００３６】

指定したファイルの暗号化は、システムに採用されている暗号化方式に従って暗号化手段３６により行われる。そして、認証登録手段３４により、認証サーバ２０に暗号化したファイルの識別情報（ファイル名など）と利用者および利用権限情報と、暗号化ファイルＣを復号化するための鍵情報を登録する。また、作成者Ａは、利用者Ｂに電子メールその他の手段で暗号化ファイルと暗号化ファイルの識別情報を送る。

【００３７】

認証サーバ２０はクライアント装置３０ａから送信されたファイルの識別情報（ファイル名など）と利用者および利用権限情報と、暗号化ファイルＣを復号化するための鍵情報とをファイル管理ＤＢ２３に記憶する。ファイル管理ＤＢ２３の検索キーはファイルの識別情報である。

【００３８】

利用者Ｂは、受け取った暗号化ファイルを利用する場合、クライアント装置３０ｂを使用し、専用ビュワー３２を用いて認証サーバ２０にログインして認証要求手段３５により認証を求める。この場合、専用ビュワー３２の画面にログイン画面が表示され、ユーザＩＤ、パスワード、利用する暗号化ファイルの識別情報（ファイル名）を入力して認証サーバ２０に送信する。

【００３９】

認証サーバ２０は、クライアント装置３０ｂから送信されたユーザＩＤ、パスワードなどの個人認証情報に基づいてデータベース制御手段２８により認証情報ＤＢ２２を参照して認証手段２５により個人認証を行う。認証が得られると、ファイルの識別情報に基づいてファイル管理ＤＢ２３から当該ファイルに登録された利用者Ｂおよび利用者Ｂに許可された利用権限情報、鍵情報を読み出す。この時、利用者Ｂと個人認証のユーザＩＤが不一致の場合には認証結果は否定でありその旨クライアント装置３０ｂに通知する。また認証サーバ２０は、警告送信手段２６により認証がとれないファイルアクセスがあった旨の警告をファイル作成者Ａや管理者に送信する。認証結果が肯定であると、クライアント装置３０ｂに利用権限情報、鍵情報を送信する。

【００４０】

クライアント装置３０ｂは、認証サーバ２０から送られた利用権限情報、鍵情報を専用ビュワー３２上で受け、専用ビュワー３２は、鍵情報に基づいて復号化手段３７を機能させて暗号化ファイルを復号化するとともに、利用者Ｂに許可された利用権限情報の範囲内での利用者Ｂの操作のみ有効とし、利用権限以外の利用者Ｂによる操作を無効とするように動作する。例えば、利用者Ｂに許可された利用権限が閲覧のみの場合、専用ビュワー３２は、復号化されたファイルを利用者Ｂが表示させる表示ボタンの操作は有効とするが、表示したファイルを印刷する印刷ボタン、保存する保存ボタン、書込み操作する書込みボタン、書込みしたファイルを上書き保存する更新保存ボタンなどの操作を無効とする。

【００４１】

従って、利用者Ｂは、作成者Ａの設定した利用権限の範囲内でのみ作成者Ａから受け取った暗号化ファイルを利用することが可能となる。利用者Ｂに与えられた権限が閲覧のみの場合は復号化したファイルをクライアント装置３０ｂに保存することはできず、また、鍵情報は専用ビュワー３２上で暗号化ファイルを復号化するものであって、利用者Ｂは復号化の操作を意識する必要はない。専用ビュワー３２は鍵情報を操作する復号化ボタンなどを有さず、利用者Ｂが鍵情報をクライアント装置３０ｂに保存する操作もできない。これによって、復号化ファイルや鍵情報が利用者Ｂ以外の第三者に流出する可能性を低減することができセキュリティーを格段に向上することができる。

【００４２】

上記の処理手順において、利用者Ｂがクライアント装置３０ｂを使用し、専用ビュワー３２を起動して認証サーバ２０にログインする際、該専用ビュワー３２のバージョン情報を認証サーバ２０に送信し、認証サーバ２０はバージョン検査手段２７で最新バージョンの専用ビュワーであるかを検査する。最新バージョンでない場合、認証サーバ２０は、利用者Ｂに与えられた利用権限に更に制限を加えた利用権限情報をクライアント装置３０ｂ

に送信する。例えば、利用権限が復号化したファイルの保存までを許可する権限であった場合、利用権限を更に制限して閲覧のみの利用権限にする。このようにすることにより、何らかの原因によって専用ビュワー３２によるセキュリティーに穴（セキュリティーホール）が生じた場合に専用ビュワー３２をバージョンアップして迅速に対応することができるようになる。

【００４３】

図３および図４は上述の処理手順を示すフローチャートであり、図３は、作成者Ａのクライアント装置３０ａと認証サーバ２０の処理手順を示すフローチャート、図４は、利用者Ｂのクライアント装置３０ｂと認証サーバ２０の処理手順を示すフローチャートである。

【００４４】

作成者Ａがデジタルコンテンツを記録したファイルを作成し、これを暗号化して利用者Ｂに利用許可する場合、作成者Ａはクライアント装置３０ａを使用し、先ず、ステップＳ１０で利用者Ａは、専用ビュワー３２を起動し、ステップＳ１１で認証サーバ２０にログインする。すなわち、専用ビュワー３２を起動するとログイン画面が表示され、その入力欄にユーザＩＤ、パスワードを入力して認証サーバ２０に送信する。認証サーバ２０が認証情報ＤＢ２２を参照して登録されている認証情報（ユーザ情報）と照合し、作成者Ａの個人認証を行い、認証がＯＫであると、作成者Ａは、ステップＳ１２で専用ビュワー３２の次画面（図示せず）から暗号化するファイルを指定する入力を行う。次いで作成者Ａは、ステップＳ１３でそのファイルの利用を許可する利用者Ｂを入力し、ステップＳ１４で利用者Ｂに許可する利用権限、例えば、利用者Ｂには一度だけの閲覧のみを許可するなどの利用権限を設定する。

【００４５】

利用者Ｂを入力するにあたって、作成者Ａは専用ビュワー３２の参照ボタンを操作することによって、認証サーバ２０の認証情報ＤＢ２２を参照して登録されているユーザ情報から利用者を選択して設定することもできる。認証情報ＤＢ２２が提供する参照情報は個々のユーザの他、グループ情報、例えば、特定の部、課、プロジェクトの構成員をグループ化して登録したグループ情報であってもよい。グループ情報を利用すれば、同一グループの複数人を一度に利用者として設定することができるようになる。

【００４６】

次いで、クライアント装置３０ａは暗号化手段３６により指定したファイルをステップＳ１５で暗号化し、ステップＳ１６で暗号化したファイルを保存し、暗号化ファイルの識別情報（ファイル名）をステップＳ１７で認証サーバ２０に送信し、ステップＳ１８で利用者および利用権限の情報を送信し、ステップＳ１９で暗号化ファイルを復号化するための鍵情報を送信する。

【００４７】

認証サーバ２０は、クライアント装置３０ａから送信された暗号化ファイルの識別情報（ファイル名）、利用者および利用権限の情報、暗号化ファイルを復号化するための鍵情報をステップＳ３３～３５で受信し、ステップＳ３６でファイル管理ＤＢ２３に記憶する。そして、作成者Ａはステップ２０で認証サーバ２０からログアウトし、ステップＳ２１で専用ビュワー３２を終了させる。この後、作成者Ａは保存した暗号化ファイルを利用者（ステップＳ１３で設定した利用者Ｂ）に送信する。利用者Ｂへの暗号化ファイルの配信手段はネットワーク（電子メールなど）に限るものでなく、フロッピィディスクなどの媒体による配信であってもよい。

【００４８】

次に、図４のフローチャートを参照して利用者Ｂがクライアント装置３０ｂを使用して作成者Ａから受け取った暗号化ファイルを利用する手順を説明する。利用者Ｂは、ステップＳ４０で受け取った暗号化ファイルを利用する場合、クライアント装置３０ｂを使用し、ステップＳ４１で専用ビュワー３２を起動し、ステップＳ４２で認証サーバ２０にログインする。認証サーバ２０が利用者Ｂの個人認証を行い、認証がＯＫであると、利用者Ｂ

は、ステップＳ４３で専用ビュワー３２の次画面（図示せず）から利用する暗号化ファイルの識別情報（ファイル名）を入力し、クライアント装置３０ｂは認証要求手段３５によりファイルの識別情報を認証サーバ２０に送信し、ステップＳ４４で認証サーバ２０に利用者認証要求を送信する。

【００４９】

認証サーバ２０は、ファイルの識別情報を受信すると、ステップＳ５１でファイル管理ＤＢ２３を参照し、該当するファイルに対して登録されている利用者および利用権限情報を読み出し、ステップＳ５２で利用者Ｂと一致するか利用者認証処理を行う。ステップＳ５３の利用者認証の結果、利用者Ｂと個人認証のユーザＩＤが不一致の場合には認証結果は否定（Ｎ０）であり、その旨クライアント装置３０ｂに通知する。また認証サーバ２０は、ステップＳ５６でその認証履歴を認証履歴ＤＢ２４に記録し、ステップＳ５７で警告送信手段２６により認証がとれないファイルアクセスがあった旨の警告をファイル作成者Ａや管理者に送信する。

【００５０】

認証結果が肯定（ＹＥＳ）であると、認証サーバ２０は、ステップＳ５４、Ｓ５５でクライアント装置３０ｂに利用権限情報、鍵情報を送信する。クライアント装置３０ｂは、ステップＳ４５、Ｓ４６で認証サーバ２０から送られた利用権限情報、鍵情報を専用ビュワー３２上で受け、専用ビュワー３２は、ステップＳ４７で鍵情報に基づいて復号化手段３７を機能させて暗号化ファイルを復号化する。そして利用者Ｂはステップ Ｓ４８で復号化されたファイルを閲覧することができる。この時、前述したように専用ビュワー３２は、利用者Ｂに許可された利用権限情報の範囲内での利用者Ｂの操作のみ有効とし、利用権限以外の操作を無効とするように動作する。

【００５１】

例えば、利用者Ｂに許可された利用権限が閲覧のみの場合、専用ビュワー３２は、利用者Ｂが復号化されたファイルを表示させる表示ボタンの操作は有効とするが、表示したファイルを印刷する印刷ボタン、保存する保存ボタン、書込み操作する書込みボタン、書込みしたファイルを上書き保存する更新保存ボタンの操作を無効とする。この場合、利用者Ｂは、復号化されたファイルを保存することはできない。利用者Ｂは、復号化されたファイルを作成者Ａの設定した利用権限の範囲内で利用し終えると、ステップＳ４９で認証サーバ２０からログアウトし、ステップＳ６０で専用ビュワー３２を終了し、処理を終える。なお、このフローチャートにおいて、専用ビュワー３２のバージョン検査とそれに関連する処理ステップは図示を省略している。

【実施例２】

【００５２】

図５は本発明に係るファイルのセキュリティー管理システムの他の実施例を示す図である。この実施例は、認証サーバ２０が複数の顧客Ｘ～Ｚに対してセキュリティーサービスアプリケーションを提供する構成になっている。各顧客Ｙ、Ｚは顧客Ｘと同様の構成をしており、認証サーバ２０は課金手段２９を備えるとともに、認証情報ＤＢ２２、ファイル管理ＤＢ２３、認証履歴ＤＢ２４の各々のデータベースは、顧客対応に区画され、顧客毎のデータを区分して記憶するように構成されている。その他の構成は図１の実施例と同様であり、その部分の説明は省略する。課金方法は定額の課金、従量制の課金、それらを併用した課金の何れでもよく、課金手段２９は、従量制の課金を行う場合、認証サーバ２０は、顧客Ｘ～Ｙのクライアント装置（作成者、利用者）からログインがあった場合にその回数、ログイン～ログアウトまでのサービス時間などを計数して顧客毎に集計するようになせばよい。

【００５３】

図５の構成によれば、ＡＳＰ提供業者（Application Service Provider）が認証サーバ２０を運営して複数の顧客にファイルのセキュリティー管理システムをサービスするビジネスモデルを構築することができる。これにより、顧客Ｘ～Ｙは他の顧客と共通するようなシステムカスタマイズを依頼する場合、ＡＳＰ提供業者に支払う開発コスト負担額を低

減することができるようになる。また、本発明に係るプログラム提供にソフトウェア開発会社が介在する場合、当該ソフトウェア開発会社はＡＳＰ提供業者が提供するＡＳＰサービスによって容易に製品販売先顧客を拡大することができるようになる。

【実施例３】

【００５４】

以上説明した実施例２に係るファイルのセキュリティー管理システムは、顧客（Ｘ～Ｚ）のそれぞれの内部におけるクライアント間のファイルセキュリティーを管理するシステムであった。しかしながら、顧客を超えてファイルセキュリティーの管理サービスを利用できればより好都合である。例えば、顧客Ｘのクライアントであるａと顧客Ｙのクライアントであるｅとの間で、認証サーバ２０が提供するサービスを利用して機密性の高いファイルの通信ができれば顧客にとって利便性が向上する。すなわち、本発明に係る認証サーバ２０が提供するセキュリティー管理のサービスに加入している顧客同士で取引があり、双方のクライアントの間で同様のサービスが受けられれば、情報の漏洩を心配することなく、重要度の高いファイルの通信が可能になり利便性を向上することができる。このためには、各顧客、全クライアントの認証情報ＤＢを共通のものとして運用すればよいが、この場合、それぞれの顧客のクライアント情報が相互に公開されることになる。すなわち、この方法ではクライアントである顧客従業員情報が漏洩することになり、顧客に受け入れられる方法とは言い難いものであって、これを解決する仕組みが必要である。

【００５５】

図６は、本発明の実施例３に係るファイルのセキュリティー管理システム１０の構成を示す図である。図６のセキュリティー管理システム１０は、顧客を超えてファイルセキュリティーの管理サービスを利用できるように構成したシステムのブロック図を示すものである。理解を容易とするため、図６においては、実施例１、実施例２と同じ構成要素には同一の参照符号を付してある。このセキュリティー管理システム１０においては認証サーバ２０に個人アドレス帳ＤＢ（データベース）４０が設けられており、クライアント装置３０ａ、３０ｂ側のクライアントプログラム３１にユーザ登録手段３８が設けられている点が実施例２のセキュリティー管理システム１０と異なる。

【００５６】

すなわち、実施例３のセキュリティー管理システム１０においては、顧客（Ｘ～Ｚ）毎に当該顧客のクライアントの認証を行うための認証情報ＤＢ２２とは別に、各クライアント毎に、当該クライアントが本セキュリティー管理サービスを利用させる相手を登録するための個人アドレス帳ＤＢ４０を認証サーバ２０に設けている。本実施例においては、この個人アドレス帳ＤＢ４０を用いてそれぞれのクライアントが登録した相手に対して本セキュリティーサービスの利用を許可するようにしたものである。ここで、認証情報ＤＢ２２と個人アドレス帳ＤＢ４０の構成について説明する。

【００５７】

図７は、認証情報ＤＢ２２と個人アドレス帳ＤＢ４０の構成を示す模式図であり、（Ａ）は認証情報ＤＢ２２の構成、（Ｂ）は個人アドレス帳ＤＢの構成を示す図である。図７（Ａ）に示すように認証情報ＤＢ２２は、認証サーバ２０によるファイルのセキュリティーサービスの提供を受ける顧客Ｘ～Ｙ毎に区画が独立しており、各顧客のクライアント（ユーザ）Ａ～Ｃ、Ｅ～Ｆ、Ｉ～Ｋが登録されている。ユーザ毎の登録情報は、「ユーザ氏名」、所属部署や所属プロジェクト等の「グループ」、「ユーザＩＤ」、「パスワード」、「メールアドレス」等である。他にユーザの役職等、他の情報を加えることもできる。

【００５８】

一方、個人アドレス帳ＤＢ４０は、顧客Ｘ～Ｙの各クライアント（ユーザ）Ａ～Ｃ、Ｅ～Ｆ、Ｉ～Ｋ毎に区画が独立しており、クライアント（ユーザ）Ａ～Ｃ、Ｅ～Ｆ、Ｉ～Ｋがそれぞれ、本セキュリティーサービスを利用してファイルの通信を行いたい相手を登録することができる。登録にあたっては、クライアントＡは、認証サーバ２０にログインして個人アドレス帳ＤＢ４０を呼出し、ユーザ登録手段３８によりＡ自身の個人アドレス帳４０に相手方の情報を登録する。登録するデータは、例えば、被登録者である相手の氏名

、メールアドレスである。メールアドレスは個人と１対１に対応する情報であり、また、このメールアドレスを介して暗号化ファイルの通信が行われ、該暗号化ファイルの利用に際しての認証データとなるため、登録データとして必須である。

【００５９】

図６のファイルのセキュリティーシステム１０を利用して異なる顧客におけるクライアント（ユーザ）の間で、暗号化ファイルの作成、利用を行う場合について、以下に説明する。例えば、顧客Ｘのクライアント Ａと顧客Ｙのクライアント Ｅが取引上のプロジェクトの一員であり、Ａが作成した機密性の高いファイルを認証サーバ２０を使用して暗号化し、閲覧のみの利用権限を付してＥに送り、Ｅが認証サーバ２０にログインして暗号化ファイルの閲覧をする場合である。

【００６０】

顧客Ｘのクライアント Ａは、認証サーバ２０の利用に先立ってまず、専用ビュワー３２を起動して認証サーバ２０にログインする。ログインのプロセスで認証サーバ２０は、認証情報ＤＢ２２を参照して顧客Ｘの認証情報に従って、クライアント Ａが顧客Ｘの正規のクライアントであることを認証するとメニュー画面を表示し、メニュー画面から個人アドレス帳への登録処理を選択する。個人アドレス帳ＤＢ４０への登録処理を選択すると、認証サーバ２０はクライアント Ａの個人アドレス帳ＤＢ４０へのアクセスを許可し、クライアント Ａは、ユーザ登録手段３８により個人アドレス帳ＤＢ４０（クライアント Ａのユーザ区画）にクライアント Ｅを登録する。図７（Ｂ）に示すように、登録するデータは被登録ユーザ（クライアント）の氏名あるいはＩＤと電子メールのメールアドレスである。

【００６１】

図８は、各個人が暗号化するファイルを利用許可する相手ユーザを、個人アドレス帳ＤＢ４０に登録する上記の手順を示すフローチャートである。まずクライアント Ａは、ステップＳ６１で専用ビュワー３２を起動し、ステップＳ６２でユーザＩＤ、パスワードを入力して認証サーバ２０にログインする。ログイン画面は例えば、図９に示すような画面であり一般的なサーバへのログイン画面と同様の構成である。次いで、クライアント Ａは、ステップＳ６３で個人アドレス帳ＤＢ４０を呼出して、ステップＳ６４で利用を許可する利用者氏名と電子メールのメールアドレスを登録する。

【００６２】

登録が完了すると、クライアント Ａはファイルを作成し（作成済みのファイルであってもよい）、専用ビュワー３２を起動して認証サーバ２０にログインする。ログイン認証の手順は前述の登録処理の場合と同様である。次に、クライアント Ａは、メニュー画面に表示されたファイル指定欄に暗号化の対象とするファイルを指定し、次いで、メニュー画面の遷移に従って、ファイルの利用者を設定するために認証情報ＤＢ２２またはクライアント Ａの個人アドレス帳ＤＢ４０を選択する。ここでは、クライアント Ａは、個人アドレス帳ＤＢ４０を選択し、先の手順で登録したクライアント Ｅを指定する。そして、メニュー画面の遷移に従って、クライアント Ｅに対する利用権限を設定する。ここでは、Ｅに対して暗号化されたファイルの閲覧のみを許可する指定を行う。なお、上記の手順ではファイルの指定が最初のメニュー画面で行われる手順としたが、利用者、利用権限の設定の後にファイルを指定する手順とすることもできる。

【００６３】

これらの指定が完了すると、クライアント Ａの作成したファイルがクライアント Ａのコンピュータ（クライアント３０ａ）上で所定の暗号化方式で暗号化され、保存される。また、認証サーバ２０は、先の手順で指定された暗号化対象ファイルのファイル名（ファイル識別情報）、利用者、利用権限情報をファイル管理ＤＢ２３に登録する。そしてクライアント Ａは、暗号化されたファイルを電子メールでクライアント Ｅに送信する。

【００６４】

電子メールを受信したクライアント Ｅは、専用ビュワー３２を起動して認証サーバ２０にログインして認証を得る。ここで、クライアント Ｅは、顧客Ｙの登録クライアントであるから、認証サーバ２０は、認証情報ＤＢ２２を参照してユーザ認証を行う。この手順は

クライアントＡの認証手順と同様である。そしてクライアントＥは、受信した暗号化ファイルをコンピュータ（クライアント３０ｂ）上で指定すると、認証サーバ２０にファイル名（ファイル識別情報）が送られ、認証サーバ２０は、ファイル管理ＤＢ２３を参照し、設定された利用者、利用権限をチェックして利用権限情報と復号化の鍵情報をクライアントＥ（３０ｂ）に送信する。

【００６５】

クライアント３０ｂは利用権限情報と復号化の鍵情報を受け、専用ビュワー３２は、鍵情報に基づいて復号化手段３７を機能させて暗号化ファイルを復号化するとともに、利用者Ｅに許可された利用権限情報の範囲内での利用者Ｅの操作のみ有効とし、利用権限以外の利用者Ｅによる操作を無効とするように動作する。例えば、利用者Ｅに許可された利用権限が閲覧のみであるから、専用ビュワー３２は、復号化されたファイルを利用者Ｅが表示させる表示ボタンの操作は有効とするが、表示したファイルを印刷する印刷ボタン、保存する保存ボタン、書込み操作する書込みボタン、書込みしたファイルを上書き保存する更新保存ボタンなどの操作を無効とする。

【００６６】

図１０は、上述の処理手順を示すフローチャートであり、作成者Ａのクライアント装置３０ａと認証サーバ２０の処理手順を示すフローチャートである。また、図１１は、図１０の手順において専用ビュワー３２に表示される操作画面の一例を模式的に併記した模式図である。入力作成者Ａがデジタルコンテンツを記録したファイルを作成し、これを暗号化して利用者Ｅに利用許可する場合、作成者Ａはクライアント装置３０ａを使用し、先ず、ステップＳ７０で作成者Ａは、専用ビュワー３２を起動し、ステップＳ７１で認証サーバ２０にログインする。すなわち、専用ビュワー３２を起動するとログイン画面が表示され、その入力欄にユーザＩＤ、パスワードを入力して認証サーバ２０に送信する。認証サーバ２０が認証情報ＤＢ２２を参照して登録されている認証情報（ユーザ情報）と照合し作成者Ａの個人認証を行い、認証がＯＫであると、作成者Ａは、ステップＳ７２で専用ビュワー３２の次画面（図示せず）から暗号化するファイルを指定する入力を行う（図１１のＳＴＥＰ１参照）。次いで作成者Ａは、ステップＳ７３でそのファイルの利用を許可する利用者Ｂを入力し、ステップＳ７４で利用者Ｅに許可する利用権限、例えば、利用者Ｂには一度だけの閲覧のみを許可するなどの利用権限を設定する（図１１のＳＴＥＰ２参照）。そして、最後に画面下部の「暗号化」ボタンを操作することにより対象ファイルが暗号化される。

【００６７】

利用者Ｅを入力するにあたって、作成者Ａは専用ビュワー３２の参照ボタンを操作することによって、認証サーバ２０の個人アドレス帳ＤＢ４０を参照して登録されているユーザ情報から利用者Ｅを選択して設定する。次いで、クライアント装置３０ａは暗号化手段３６により指定したファイルをステップＳ７５で暗号化し、ステップＳ７６で暗号化したファイルを保存し、暗号化ファイルの識別情報（ファイル名）をステップＳ７７で認証サーバ２０に送信し、ステップＳ７８で利用者および利用権限の情報を送信し、ステップＳ７９で暗号化ファイルを復号化するための鍵情報を送信する。

【００６８】

認証サーバ２０は、クライアント装置３０ａから送信された暗号化ファイルの識別情報（ファイル名）、利用者および利用権限の情報、暗号化ファイルを復号化するための鍵情報をステップＳ９３～９５で受信し、ステップＳ９６でファイル管理ＤＢ２３に記憶する。そして、作成者Ａはステップ８０で認証サーバ２０からログアウトし、ステップＳ８１で専用ビュワー３２を終了させる。この後、ステップＳ８２で、作成者Ａは保存した暗号化ファイルを利用者Ｅ（ステップＳ７３で設定した利用者Ｅ）に送信する。利用者Ｅへの暗号化ファイルの配信手段はネットワーク（電子メールなど）に限るものでなく、フロッピィディスクなどの媒体による配信であってもよい。

【００６９】

なお、利用者Ｅが作成者Ａから受信した暗号化ファイルを利用する手順は、図１２のフ

ローチャートに示す手順となる。図１２のフローチャートにおいて、認証サーバ２０が利用者Ｅの認証を行う処理（ステップＳ１２２）において、認証情報ＤＢ２２、個人アドレス帳ＤＢ４０を参照して利用者Ｅの認証を行う点を除き、その他の処理ステップは、図４のフローチャートに示す手順と同様の手順となる。なお、作成者Ａから電子メールで利用者Ｅが暗号化ファイルを受信した場合、暗号化ファイルであることを示すアイコンを利用者Ｅのクライアント装置３０ｂのデスクトップ上に表示し、このアイコンを利用者Ｅが操作することによって専用ビュワー３２が起動するように構成すると操作性が良いシステムとすることができる。

【００７０】

図１０および図１２の手順は、利用者Ｅが本セキュリティーサービスに加入している顧客Ｙにおけるクライアント Ｅであったが、セキュリティーサービスに加入していない個人との間で同様のサービスを提供できるとなお利便性が増す。例えば、顧客Ｘのクライアント Ａが任意の個人（サービス未加入）Ｍとの間で暗号化ファイルの通信を行う場合である。この場合、クライアント Ａが図８の手順で個人アドレス帳ＤＢ４０におけるＡのユーザ区画に、利用者Ｍを登録しておく。この手順はクライアント Ｅを利用者として登録する場合と同様である。そしてクライアント Ａは、登録した利用者Ｍに対して図１０のフローチャートで説明した手順でファイルを暗号化した上で、暗号化ファイルを利用者Ｍにメール等の手段で受け渡しする。この場合、必要情報として認証サーバ２０のＵＲＬを利用者Ｍに伝える必要がある。なぜならば、利用者Ｍは本セキュリティーシステムの顧客ではないため認証サーバ２０にログインできるようにする必要があるからである。

【００７１】

このため、認証サーバ２０は、クライアント Ａから暗号化ファイル名、利用者および権限情報等を受信（図１０のフローチャートのステップＳ９３～Ｓ９４）すると、設定された利用者Ｍに、認証サーバ２０のＵＲＬ、ログインのためのユーザＩＤ、仮パスワードを設定し、これらの情報を個人アドレス帳ＤＢ４０に登録された利用者Ｍのメールアドレスに送信する。これらの情報の送信は、図１０のフローチャートのステップＳ９６で暗号化ファイルの情報をファイル管理ＤＢ２４に保存する際に行ってもよく、ステップＳ９３、Ｓ９４でクライアント Ａから暗号化ファイル名、利用者および権限情報を受信した際に行ってもよい。なお、利用者Ｍに対する認証サーバ２０のＵＲＬ、ログインのためのユーザＩＤ、仮パスワードの情報の通知は前述のように認証サーバ２０から利用者Ｍに通知する方法に限らず、これらの情報をクライアント Ａに通知し、クライアント Ａが暗号化ファイルを利用者Ｍに受け渡しする際に付加情報として通知するように構成することもできる。

【００７２】

一方、利用者Ｍが作成者Ａから受信した暗号化ファイルを利用する場合は、図１３に示すフローチャートの手順に従って処理を行う。すなわち、図１３は、本サービスの顧客内のクライアントと顧客でない個人との間で本サービスを利用する場合の利用者側の処理手順を示すフローチャートである。先ず、利用者Ｍは、ステップＳ１３１でＡから暗号化ファイルを受信するとステップＳ１３２で付加として受取ったＵＲＬに基づいて認証サーバ２０に接続して該ＵＲＬに表示される入力画面からユーザ氏名、メールアドレスを入力する。ステップＳ１５１で認証サーバ２０は、入力されたユーザ氏名、メールアドレスの情報をクライアント Ａが個人アドレス帳ＤＢ４０に登録した情報と比較し、クライアント Ａが登録した利用者であるか否かをチェックし、登録利用者である場合には、ステップＳ１５２で利用者Ｍに専用ビュワー３２を送信し、ステップＳ１３３で利用者Ｍは専用ビュワー３２を受信し専用ビュワーのダウンロードが完了する。

【００７３】

専用ビュワー３２のダウンロードが完了すると利用者Ｍは専用ビュワー３２を起動して認証サーバにログインしてクライアント Ａにより設定された利用権限に従って暗号化ファイルを復号化して利用することができる。この場合、認証サーバ２０が利用者Ｍの認証を行うために個人アドレス帳ＤＢ４０を参照する処理（ステップＳ１５５）が行われる点を除き、図１３のフローチャートにおける他の処理手順、ステップＳ１３４ないしステップ

Ｓ１４３（認証サーバ２０の処理ステップＳ１５３ないしステップＳ１６０を含む）は、図１２に示したフローチャートの手順と同様の手順である。

【００７４】

なお、利用者として本サービスに加入していない個人等を前述のようにして登録した場合、認証サーバ２０を運営する事業体は、登録したクラインアトＡが属する顧客Ｘのクライアントが１名増加したものとして顧客Ｘに課金することができる。このため、図６の課金手段２９は、利用者の認証を行った際に、個人アドレス帳ＤＢ４０の参照結果に基づいて課金を行うように構成すればよい。

【００７５】

以上説明した実施例３においては、顧客に属する個人毎の個人アドレス帳ＤＢ４０を設けているため、顧客がプロバイダであり、数万人のユーザが加入しているような場合であっても膨大なユーザリストのようなものを利用することなく、個人アドレス帳を利用するものであるから、一覧を表示する場合にも個人毎の登録情報のみが表示され使い勝手をよくすることができる。また、本発明における「個人アドレス帳」という用語は必ずしも電子メールアドレスのみを登録したデータを意味するものでなく、利用者を特定することのできる情報を登録したものであればよく、電子メールアドレスは登録された利用者とクライアントＡ等、認証サーバ２０等が通信するためのデータとして使用するものであってもよい。

【００７６】

また、図１、図５の実施例においては、ファイル作成者側のクライアント装置３０ａでファイルを暗号化し、暗号化ファイルの識別情報、利用者および利用権限情報とともに利用者が暗号化ファイルを復号化するための鍵情報を認証サーバ２０に登録する構成を説明したが、本発明に係るファイルのセキュリティー管理システムは、この構成に限られるものではない、例えば、ファイル作成側のクライアント装置３０ａから専用ビュワー３２を用いて認証サーバ２０にログインし、暗号化するファイルが指定されたら、認証サーバ２０が暗号化、復号化の鍵を発行し、ファイル識別情報、利用者および利用権限情報とともにファイル管理データベースに登録する構成であってもよい。

【００７７】

また、暗号化方式として公開鍵と秘密鍵との鍵ペアを使用し、ファイル作成者側のクライアント装置３０ａで利用を許可する利用者と利用権限を設定する際に、該利用者の公開鍵を使用してファイルを暗号化し、認証サーバ２０にはファイルの復号化のための鍵情報として利用者の公開鍵を使用したことを登録する構成とすることもできる。利用者側のクライアント装置３０ｂが専用ビュワー３２を用いて認証サーバ２０にログインして認証要求した際、認証サーバ２０は、利用権限情報とともに鍵情報をクライアント装置３０ｂに送り、利用者側クライアント装置３０ｂは鍵情報から暗号化に自分の公開鍵が使用されたことを識別し、暗号化ファイルを復号化することができる。

【００７８】

以上のように、本発明に係るファイルのセキュリティー管理システムにおける暗号化方式は、既知の種々の暗号化方式を使用した構成とすることが可能である。

【図面の簡単な説明】

【００７９】

【図１】本発明に係るファイルのセキュリティー管理システムの基本的機能を示す概念図である。

【図２】本発明に係るファイルのセキュリティー管理システムの実施例１の構成を示すブロック図である。

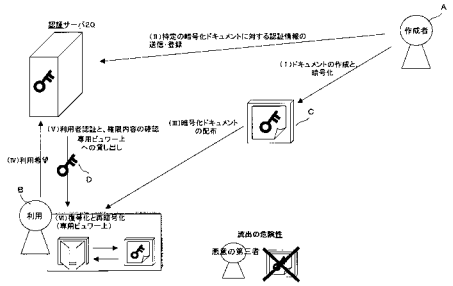
【図３】実施例１におけるファイル作成者側クライアント装置と認証サーバの処理手順を示すフローチャートである。

【図４】実施例１におけるファイル利用者側クライアント装置と認証サーバの処理手順を示すフローチャートである。

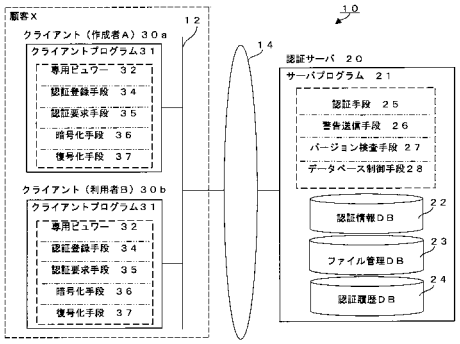
【図５】本発明に係るファイルのセキュリティー管理システムの実施例２の構成を示すブ

ロック図である。
【図６】本発明に係るファイルのセキュリティー管理システムの実施例３の構成を示すブロック図である。
【図７】実施例３における認証情報ＤＢ２２と個人アドレス帳ＤＢ４０の構成を示す模式図である。
【図８】実施例３における個人アドレス帳ＤＢ４０への登録手順を示すフローチャートである。
【図９】認証サーバへのログイン画面の構成を示す図である。
【図１０】実施例３におけるファイル作成者側クライアント装置と認証サーバの処理手順を示すフローチャートである。
【図１１】図１０の手順において専用ビュワーに表示される操作画面の一例を示す模式図である。
【図１２】実施例３におけるファイル利用者側クライアント装置と認証サーバの処理手順を示すフローチャートである。
【図１３】ファイル利用者が認証サーバのサービスに加入していない場合における利用者側クライアント装置と認証サーバの処理手順を示すフローチャートである。
【図１４】一般の暗号化ファイルによるセキュリティー管理の基本形態を示す概念図である。
【符号の説明】
【００８０】
１０・・・ファイルのセキュリティー管理システム
１２・・・イントラネット
１４・・・インターネット
２０・・・認証サーバ
２１・・・サーバプログラム
２２・・・認証情報ＤＢ
２３・・・ファイル管理ＤＢ
２４・・・認証履歴ＤＢ
２５・・・認証手段
２６・・・警告送信手段
２７・・・バージョン検査手段
２８・・・データベース制御手段
２９・・・課金手段
３０ａ、３０ｂ・・・クライアント装置
３１・・・クライアントプログラム
３２・・・専用ビュワー
３４・・・認証登録手段
３５・・・認証要求手段
３６・・・暗号化手段
Ｘ～Ｙ・・・顧客

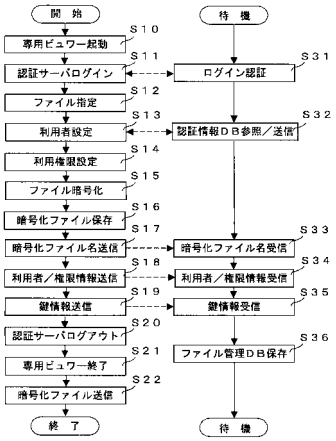
【図１】


認証サーバ20
作成者
A
(II)特定の暗号化ドキュメントに対する認証情報の送信・登録
(I)ドキュメントの作成と暗号化
C
(V)利用者認証と、権限内容の確認
専用ビューワー上への貼りだし
(III)暗号化ドキュメントの配布
(IV)利用希望
D
B
利用
(VI)復号化と認証写化（専用ビューワー上）
流出の危険性
悪意の第三者

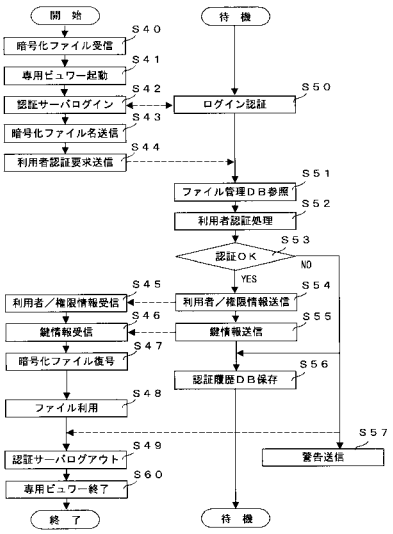
【図２】


顧客X
12
クライアント（作成者A）30a
クライアントプログラム31
専用ビューワー 32
認証登録手段 34
認証要求手段 35
暗号化手段 36
復号化手段 37
クライアント（利用者B）30b
クライアントプログラム31
専用ビューワー 32
認証登録手段 34
認証要求手段 35
暗号化手段 36
復号化手段 37
10
14
認証サーバ 20
サーバプログラム 21
認証手段 25
警告送信手段 26
バージョン検査手段 27
データベース制御手段28
認証情報DB
22
ファイル管理DB
23
認証履歴DB
24

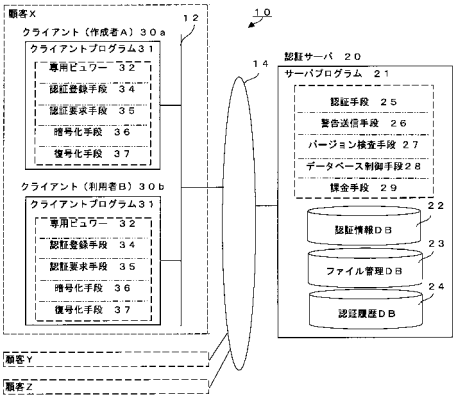
【図３】


開 始
専用ビューワー起動
S10
認証サーバログイン
S11
ファイル指定
S12
利用者設定
S13
利用権限設定
S14
ファイル暗号化
S15
暗号化ファイル保存
S16
暗号化ファイル名送信
S17
利用者／権限情報送信
S18
鍵情報送信
S19
認証サーバログアウト
S20
専用ビューワー終了
S21
暗号化ファイル送信
S22
終 了
待 機
ログイン認証
S31
認証情報DB参照／送信
S32
暗号化ファイル名受信
S33
利用者／権限情報受信
S34
鍵情報受信
S35
ファイル管理DB保存
S36
待 機

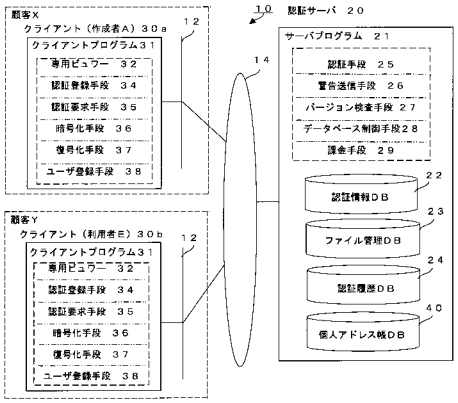
【図４】


開 始
暗号化ファイル受信
S40
専用ビューワー起動
S41
認証サーバログイン
S42
暗号化ファイル名送信
S43
利用者認証要求送信
S44
利用者／権限情報受信
S45
鍵情報受信
S46
暗号化ファイル復号
S47
ファイル利用
S48
認証サーバログアウト
S49
専用ビューワー終了
S60
終 了
待 機
ログイン認証
S50
ファイル管理DB参照
S51
利用者認証処理
S52
認証OK
S53
NO
YES
利用者／権限情報送信
S54
鍵情報送信
S55
認証履歴DB保存
S56
警告送信
S57
待 機

【図５】


顧客X
12
クライアント（作成者A）30a
クライアントプログラム31
専用ビューワー 32
認証登録手段 34
認証要求手段 35
暗号化手段 36
復号化手段 37
クライアント（利用者B）30b
クライアントプログラム31
専用ビューワー 32
認証登録手段 34
認証要求手段 35
暗号化手段 36
復号化手段 37
10
14
認証サーバ 20
サーバプログラム 21
認証手段 25
警告送信手段 26
バージョン検査手段 27
データベース制御手段28
課金手段 29
認証情報DB
22
ファイル管理DB
23
認証履歴DB
24
顧客Y
顧客Z

【図６】



【図７】

認証情報DB 22

顧客区画	ユーザ氏名	グループ	ユーザID	パスワード	メールアドレス
	A				
X	B				
	C				
	E				
Y	F				
	G				
	I				
Z	J				
	K				

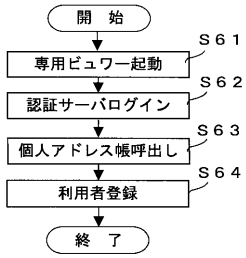
(A)

個人アドレス帳DB 40

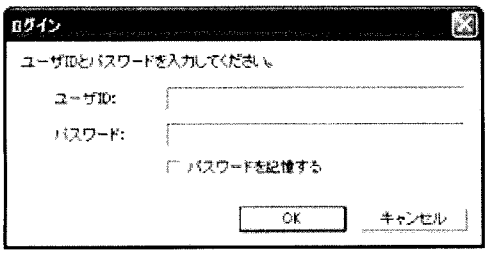
ユーザ区画	被登録ユーザ	メールアドレス
A(X)	E	*******
B(X)		
C(X)		
E(Y)		
F(Y)		
G(Y)		
I(Z)		
J(Z)		
K(Z)		

(B)

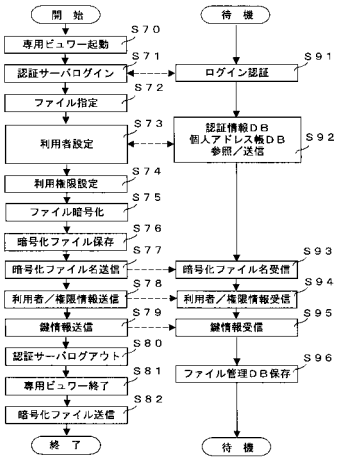
【図８】



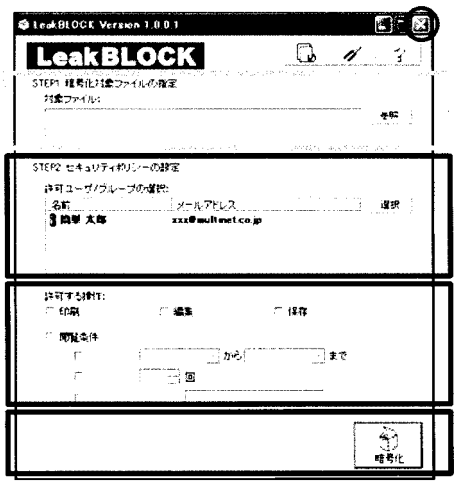
【図９】



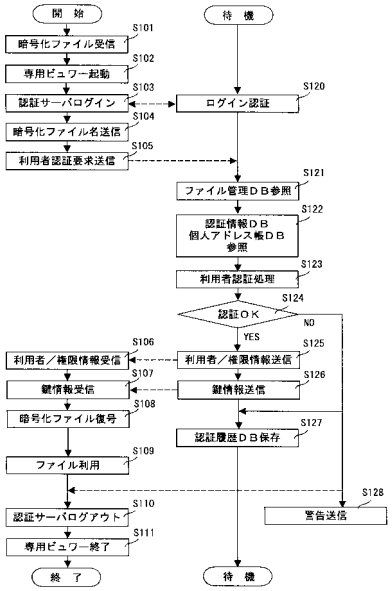
【図１０】



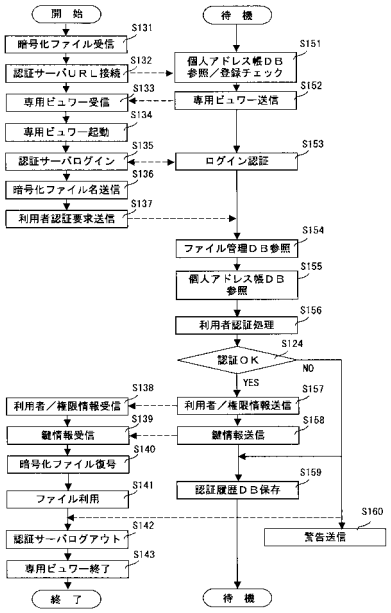
【図１１】



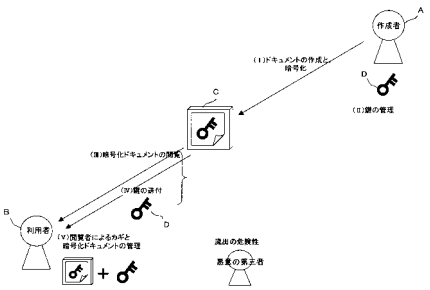
【図１２】



【図１３】



【図１４】



フロントページの続き

(51)Int.Cl.	FI		テーマコード（参考）
	G06F 12/00	537H	
	H04L 9/00	675D	