(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2012-256253
(P2012-256253A)
(43)公開日　平成24年12月27日(2012.12.27)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330A	5B017
H04L 9/08	(2006.01)	H04L	9/00	601B	5B285
G06F 21/24	(2006.01)	H04L	9/00	601E	5J104
		G06F	12/14	540P	
		G06F	12/14	520F	

審査請求 未請求　請求項の数 5　ＯＬ　（全 28 頁）　最終頁に続く

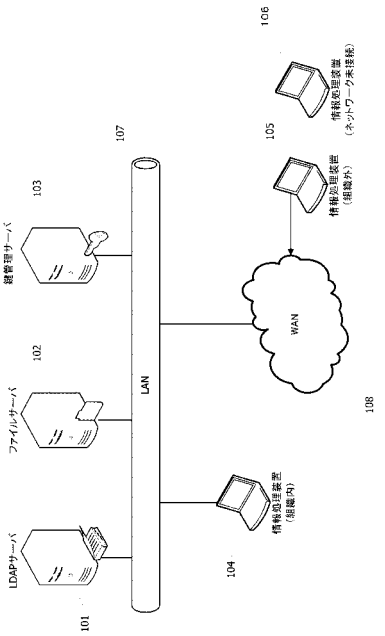
(21)出願番号　特願2011-129636 (P2011-129636)
(22)出願日　平成23年6月9日 (2011.6.9)

（特許庁注：以下のものは登録商標）
１．Ｌｉｎｕｘ

(71)出願人　390002761
キヤノンマーケティングジャパン株式会社
東京都港区港南２丁目１６番６号
(71)出願人　312000206
キヤノンＭＪアイティグループホールディングス株式会社
東京都品川区東品川２丁目４番１１号
(71)出願人　592135203
キヤノンＩＴソリューションズ株式会社
東京都品川区東品川２丁目４番１１号
(74)代理人　100126103
弁理士　伊藤　幹郎
(72)発明者　松田　雄介
東京都港区三田３丁目１１番２８号　キヤノンＩＴソリューションズ株式会社内
最終頁に続く

(54)【発明の名称】情報処理装置、情報処理方法、プログラム

(57)【要約】
【課題】　利便性を低減させずに、クライアント端末に記憶されたファイルに対するアクセスを制御し情報漏洩を防ぐこと
【解決手段】　情報処理装置のネットワークへの接続形態に応じて、当該情報処理装置に記憶されたファイルを復号する鍵を送信するか否かを判定するサーバと通信可能な情報処理装置であって、ネットワークへの接続形態を検出し、検出された接続形態を含む鍵取得要求をサーバに送信し、サーバから送信される復号鍵を取得し、当該復号鍵を用いて情報処理装置に記憶されたファイルを復号する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
ネットワークとの接続が可能であり、情報処理装置の復号鍵要求送信手段により送信された復号鍵要求に含まれる接続形態を示す情報に基づき、前記情報処理装置に対して復号鍵を送信するか否かを判定する外部サーバと接続可能な情報処理装置であって、
ネットワークへの接続形態を検出する検出手段と、
前記検出手段で検出された接続形態を示す情報を含む復号鍵要求を前記外部サーバに送信する復号鍵要求送信手段と、
前記外部サーバから復号鍵を取得する復号鍵取得手段と、
前記復号鍵取得手段により取得した復号鍵を用いて前記情報処理装置に記憶されたファイルを復号する復号手段と、
を備えることを特徴とする情報処理装置。
【請求項２】
前記復号鍵取得手段により取得した復号鍵を記憶する復号鍵記憶手段と、
前記情報処理装置に記憶されたファイルに対応する復号鍵が前記復号鍵記憶手段に記憶されているか否かを判定する判定手段とを備え、
前記復号手段は、前記判定手段により復号鍵が記憶されていると判定された場合、当該復号鍵を用いて、当該ファイルを復号することをさらに特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記復号鍵記憶手段は、前記復号鍵取得手段により取得した復号鍵と当該復号鍵の有効期間を対応付けて記憶することをさらに特徴とし、
前記判定手段により復号鍵が記憶されていると判定された場合、当該復号鍵が有効期間内であるか否かを判定する有効期間判定手段をさらに備え、
前記復号手段は、前記有効期間判定手段により有効期間内であると判定された復号鍵を用いてファイルを復号することをさらに特徴とする請求項１または２に記載の情報処理装置。
【請求項４】
ネットワークとの接続が可能であり、情報処理装置の復号鍵要求送信工程により送信された復号鍵要求に含まれる接続形態を示す情報に基づき、前記情報処理装置に対して復号鍵を送信するか否かを判定する外部サーバと接続可能な情報処理装置における情報処理方法であって、
前記情報処理装置の検出手段が、ネットワークへの接続形態を検出する検出工程と、
前記情報処理装置の復号鍵要求送信手段が、前記検出工程で検出された接続形態を示す情報を含む復号鍵要求を前記外部サーバに送信する復号鍵要求送信工程と、
前記情報処理装置の復号鍵取得手段が、前記外部サーバから復号鍵を取得する復号鍵取得工程と、
前記情報処理装置の復号手段が、前記復号鍵取得工程により取得した復号鍵を用いて前記情報処理装置に記憶されたファイルを復号する復号工程と、
を備えることを特徴とする情報処理方法。
【請求項５】
ネットワークとの接続が可能であり、情報処理装置の復号鍵要求送信手段により送信された復号鍵要求に含まれる接続形態を示す情報に基づき、前記情報処理装置に対して復号鍵を送信するか否かを判定する外部サーバと接続可能な情報処理装置で実行可能なプログラムあって、
前記情報処理装置を、
ネットワークへの接続形態を検出する検出手段と、
前記検出手段で検出された接続形態を示す情報を含む復号鍵要求を前記外部サーバに送信する復号鍵要求送信手段と、
前記外部サーバから復号鍵を取得する復号鍵取得手段と、

前記復号鍵取得手段により取得した復号鍵を用いて前記情報処理装置に記憶されたファイルを復号する復号手段として機能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、ファイルへのアクセスを制御する技術に関する。
【背景技術】
【０００２】
近年、機密情報を格納した情報処理装置からの情報漏洩が増加しており、その対策として外部への情報処理装置の持ち出し禁止や、外部のネットワークへの接続を禁止するといった対策がとられている。しかし、業務形態によっては、情報処理装置を外部に持ち出すことが必要となったり、ネットワークに接続しなければならなかったりする場合も多く、一律な対策では業務効率の低下等不都合も生じている。
【０００３】
そこで、機密情報を暗号化して持ち出し、使用エリアによって復号を制限する方法が特許文献１で開示されている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００８－１４１５８１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、特許文献１に記載のシステムにおいては、使用エリアの特定にネットワーク装置が必要であり、外部利用に対する柔軟な対応が難しい。また、管理サーバが利用できない場合は機密ファイルを利用することができなくなる。
【０００６】
更に、資格情報の漏洩又は盗難により、なりすましによる不正利用が発生した場合、ファイルを暗号化している全ての鍵を更新しなければならず、多大なコストが発生する。
【０００７】
そこで本発明は、上記の課題を解決するためになされたものであり、利便性を低減させずに情報漏洩を防ぐことが可能な仕組みを提供することを目的とする。
【課題を解決するための手段】
【０００８】
本発明は、ネットワークとの接続が可能であり、情報処理装置の復号鍵要求送信手段により送信された復号鍵要求に含まれる接続形態を示す情報に基づき、前記情報処理装置に対して復号鍵を送信するか否かを判定する外部サーバと接続可能な情報処理装置であって、ネットワークへの接続形態を検出する検出手段と、前記検出手段で検出された接続形態を示す情報を含む復号鍵要求を前記外部サーバに送信する復号鍵要求送信手段と、前記外部サーバから復号鍵を取得する復号鍵取得手段と、前記復号鍵取得手段により取得した復号鍵を用いて前記情報処理装置に記憶されたファイルを復号する復号手段と、を備えることを特徴とする。
【０００９】
また、本発明は、ネットワークとの接続が可能であり、情報処理装置の復号鍵要求送信工程により送信された復号鍵要求に含まれる接続形態を示す情報に基づき、前記情報処理装置に対して復号鍵を送信するか否かを判定する外部サーバと接続可能な情報処理装置における情報処理方法であって、前記情報処理装置の検出手段が、ネットワークへの接続形態を検出する検出工程と、前記情報処理装置の復号鍵要求送信手段が、前記検出工程で検

出された接続形態を示す情報を含む復号鍵要求を前記外部サーバに送信する復号鍵要求送信工程と、前記情報処理装置の復号鍵取得手段が、前記外部サーバから復号鍵を取得する復号鍵取得工程と、前記情報処理装置の復号手段が、前記復号鍵取得工程により取得した復号鍵を用いて前記情報処理装置に記憶されたファイルを復号する復号工程と、を備えることを特徴とする。

【００１０】

また、本発明は、ネットワークとの接続が可能であり、情報処理装置の復号鍵要求送信手段により送信された復号鍵要求に含まれる接続形態を示す情報に基づき、前記情報処理装置に対して復号鍵を送信するか否かを判定する外部サーバと接続可能な情報処理装置で実行可能なプログラムあって、前記情報処理装置を、ネットワークへの接続形態を検出する検出手段と、前記検出手段で検出された接続形態を示す情報を含む復号鍵要求を前記外部サーバに送信する復号鍵要求送信手段と、前記外部サーバから復号鍵を取得する復号鍵取得手段と、前記復号鍵取得手段により取得した復号鍵を用いて前記情報処理装置に記憶されたファイルを復号する復号手段として機能させることを特徴とする。

【発明の効果】

【００１１】

本発明によれば、利便性を低減させずに情報漏洩を防ぐことが可能な仕組みを提供することができる。

【図面の簡単な説明】

【００１２】

【図１】ファイルアクセス制御システムの構成の一例を示す図である。

【図２】ハードウエア構成の一例を示す図である。

【図３】図１で示した鍵管理サーバ１０３及び情報処理装置（１０４、１０５、１０６）の機能の一例を示す図である。

【図４】暗号化ファイルオープン時の処理の一例を示すフローチャートである。

【図５】鍵管理サーバが鍵を情報処理装置に発行する際の処理の一例を示すフローチャートである。

【図６】ファイル書き込み時の処理の一例を示すフローチャートである。

【図７】ファイル取得時の処理の一例を示すフローチャートである。

【図８】ファイルアップロード及び削除時の情報処理装置における処理の一例を示すフローチャートである。

【図９】ファイルアップロード時の鍵管理サーバにおける処理の一例を示すフローチャートである。

【図１０】アクセスルール情報変更時の処理の一例を示すフローチャートである。

【図１１】ファイル管理プログラムの画面の一例を示す図である。

【図１２】サーバ管理プログラムの画面の一例を示す図である。

【図１３】ネットワーク定義一覧画面の一例を示す図である。

【図１４】アクセスルール一覧画面の一例を示す図である。

【図１５】アクセスルール設定画面の一例を示す図である。

【図１６】鍵送信設定画面の一例を示す図である。

【図１７】ネットワーク定義情報の一例を示す図である。

【図１８】アクセスルール情報の一例を示す図である。

【図１９】アクセス制御情報の一例を示す図である。

【図２０】鍵発行情報の一例を示す図である。

【図２１】保持ファイル情報の一例を示す図である。

【発明を実施するための形態】

【００１３】

以下、図面を参照して本発明の実施形態を詳細に説明する。

【００１４】

図１は、本発明の実施形態におけるファイルアクセス制御システムの構成の一例を示す

図である。

【００１５】

以下、図面を参照して、本発明の実施形態を詳細に説明する。

【００１６】

なお、図１のネットワーク１０７上に接続される各種端末の構成は一例であり、用途や目的に応じて様々な構成例があることは言うまでもない。

【００１７】

１０１はＬＤＡＰ（Ｌｉｇｈｔｗｅｉｇｈｔ Ｄｉｒｅｃｔｏｒｙ Ａｃｃｅｓｓ Ｐｒｏｔｏｃｏｌ）サーバである。このＬＤＡＰサーバ１０１は、企業ネットワークを利用する組織や個人のディレクトリ情報を管理するディレクトリサービスを提供するものである。尚、本実施形態に適用可能なディレクトリサービスはＬＤＡＰに限られるものではなく、例えばＡｃｔｉｖｅ Ｄｉｒｅｃｔｏｒｙ等他のものであってもよい。

【００１８】

１０２はファイルサーバである。このファイルサーバは、業務で用いる機密ファイル及び機密でないファイルの保存機能を有している。

【００１９】

１０３は鍵管理サーバである。本発明にかかるシステムの利用者は、機密ファイルをファイルサーバから取得する際、直接ファイルサーバにアクセスせずに鍵管理サーバ１０３経由でファイルを取得する。この鍵管理サーバはファイルの暗号化・復号機能及び、鍵の発行機能及び、ＬＤＡＰサーバ１０１を用いた利用者認証機能を有する。

【００２０】

１０４は組織内ネットワークに接続された情報処理装置である。この情報処理装置は専用のプログラムによって鍵管理サーバ１０３とファイルの送受信及び、ネットワーク接続形態検出及び、鍵の保存処理及び、暗号化ファイルの復号処理を行う。

【００２１】

１０５は組織外のネットワークに接続された情報処理装置であり、組織内ネットワークに接続された情報処理装置１０４と同等の機能を有する情報処理装置である。なお、組織外ネットワークは別拠点の企業ネットワーク、情報処理装置所有者の個人ネットワーク、公衆ネットワーク等あらゆるネットワークが該当する。

【００２２】

１０６は鍵管理サーバ１０３に接続できない情報処理装置であり、情報処理装置１０４と同等の機能を有する情報処理装置である。情報処理装置１０６には、ネットワークに接続していない情報処理装置だけでなく、鍵管理サーバ１０３へ到達不可能なネットワークに接続されている情報処理装置も含まれる。

【００２３】

以下、図２を用いて、図１に示した各種サーバ（１０１、１０２、１０３）、情報処理装置（１０４、１０５、１０６）に適用可能な情報処理装置のハードウエア構成の一例について説明する。

【００２４】

図２において、２０１はＣＰＵで、システムバス２０４に接続される各デバイスやコントローラを統括的に制御する。また、ＲＯＭ２０３あるいは外部メモリ２１１には、ＣＰＵ２０１の制御プログラムであるＢＩＯＳ（Ｂａｓｉｃ Ｉｎｐｕｔ ／ Ｏｕｔｐｕｔ Ｓｙｓｔｅｍ）やオペレーティングシステムプログラム（以下、ＯＳ）や、各サーバ或いは各ＰＣの実行する機能を実現するために必要な各種プログラム等が記憶されている。

【００２５】

２０２はＲＡＭで、ＣＰＵ２０１の主メモリ、ワークエリア等として機能する。ＣＰＵ２０１は、処理の実行に際して必要なプログラム等をＲＯＭ２０３あるいは外部メモリ２１１からＲＡＭ２０２にロードして、該ロードしたプログラムを実行することで各種動作を実現するものである。

【００２６】

また、２０５は入力コントローラで、入力装置２０９等からの入力を制御する。２０６はビデオコントローラで、液晶ディスプレイ等のディスプレイ装置２１０への表示を制御する。なお、ディスプレイ装置は、液晶ディスプレイに限られず、ＣＲＴディスプレイなどであっても良い。これらは必要に応じてクライアントが使用するものである。

【００２７】

２０７はメモリコントローラで、ブートプログラム，各種のアプリケーション，フォントデータ，ユーザファイル，編集ファイル，各種データ等を記憶するハードディスク（ＨＤ）や、フレキシブルディスク（ＦＤ）、或いはＰＣＭＣＩＡカードスロットにアダプタを介して接続されるコンパクトフラッシュ（登録商標）メモリ等の外部メモリ２１１へのアクセスを制御する。

【００２８】

２０８は通信Ｉ／Ｆコントローラで、ネットワーク（例えば、図１に示したＬＡＮ４００）を介して外部機器と接続・通信するものであり、ネットワークでの通信制御処理を実行する。例えば、ＴＣＰ／ＩＰを用いた通信等が可能である。

【００２９】

なお、ＣＰＵ２０１は、例えばＲＡＭ２０２内の表示情報用領域へアウトラインフォントの展開（ラスタライズ）処理を実行することにより、ディスプレイ装置２１０上での表示を可能としている。また、ＣＰＵ２０１は、ディスプレイ装置２１０上の不図示のマウスカーソル等でのユーザ指示を可能とする。

【００３０】

ハードウエア上で動作する各種プログラムは、外部メモリ２１１に記録されており、必要に応じてＲＡＭ２０２にロードされることによりＣＰＵ２０１によって実行されるものである。

【００３１】

なお、全ての装置がこれらの構成を備えているわけではなく、必要なものを夫々備えていればよい。

【００３２】

図３は、図１で示した鍵管理サーバ１０３及び情報処理装置１０４、１０５、１０６の機能の一例を示す図である。

【００３３】

３０１は、鍵管理サーバ１０３上で稼働するアクセス制御管理サービスであり、ネットワーク定義情報管理部３０２、アクセスルール情報管理部３０３、鍵発行処理部３０４、通信制御部３０５の機能を提供するものである。

【００３４】

３０２は、ネットワーク定義情報管理部で、管理者が想定するネットワークの接続形態の追加・変更・削除の管理を行う機能を提供する。

【００３５】

３０３は、アクセスルール情報管理部で、管理者がアクセス制御の対象とするファイル及びディレクトリ、制限対象となる操作、制限対象のユーザを定義するための機能を提供する。

【００３６】

３０４は、鍵発行処理部で、鍵の生成・送信及び鍵発行情報の追加・削除を行う機能を提供する。

【００３７】

３０５は、通信制御部で、情報処理装置１０４、１０５、１０６と各種情報のやり取りを制御する。

【００３８】

３０６は、ネットワーク定義情報であり、図１７に示すテーブルに対応する。

【００３９】

３０７は、アクセスルール情報であり、図１８に示すテーブルに対応する。

【００４０】
３０８は、アクセス制御情報であり、図１９に示すテーブルに対応する。
【００４１】
３０９は、鍵発行情報であり、図２０に示すテーブルに対応する。
【００４２】
３１３は、情報処理装置１０４、１０５、１０６上で稼働するファイル管理プログラムで、鍵要求処理部３１４、ファイル送受信処理部３１５、前処理部３１６、後処理部３１７の機能を提供するものである。
【００４３】
３１４は、鍵要求処理部で、ネットワーク接続形態の検出及び鍵管理サーバへ暗号化ファイルを復号する鍵の要求を行う機能を提供する。
【００４４】
３１５は、ファイル送受信処理部で、鍵管理サーバから機密ファイルの取得及び、機密ファイルを鍵管理サーバへ送信する機能を提供する。
【００４５】
３１６は、前処理部で、暗号化ファイルをオープンする際の処理を制御する。
【００４６】
３１７は、後処理部で、ファイル書き込み時の処理を制御する。
【００４７】
３１９は、保持ファイル情報であり、図２１に示すテーブルに対応する。
【００４８】
次に、図４を用いて、本発明の実施形態において情報処理装置（１０４、１０５、１０６）が行う暗号化ファイルをオープンする際の処理について説明する。
【００４９】
なお、図４のフローチャートで示す処理については、情報処理装置のＣＰＵ２０１が所定の制御プログラムを読み出して実行する処理である。
【００５０】
ステップＳ４０１では、情報処理装置のＣＰＵ２０１は、ユーザからの情報処理装置の記憶領域に記憶されたファイルに対するオープン要求を受け付ける。
【００５１】
ステップＳ４０２では、情報処理装置のＣＰＵ２０１は、ステップＳ４０１でオープン要求を受けたファイルのハッシュ値を計算する。なお、ハッシュ値の計算にはＭＤ５（Ｍｅｅｓａｇｅ　Ｄｉｇｅｓｔ　Ａｌｇｏｒｉｔｈｍ５）などの公知技術を用いて、本発明におけるシステム全体で統一されたハッシュ関数を用いる。
【００５２】
ステップＳ４０３では、情報処理装置のＣＰＵ２０１は、ステップＳ４０２で算出されたハッシュ値が保持ファイル情報３１９（図２１）にあるか否かを判断する。
【００５３】
ステップＳ４０３であると判断された場合（ステップＳ４０３：ＹＥＳ）は、処理をステップＳ４０５に移行する。
【００５４】
ステップＳ４０３でないと判断された場合（ステップＳ４０３：ＮＯ）は、処理をステップＳ４０４に移行する。
【００５５】
ステップＳ４０４では、情報処理装置のＣＰＵ２０１は、ステップＳ４０２で計算されたハッシュ値が保持ファイル情報にないことから、当該ファイルは、鍵管理サーバ１０３で管理されている機密ファイルではないと判断し、ファイルオープン処理をＯＳに委譲する。そして、本フローチャートに示す処理を終了する。
【００５６】
ステップＳ４０５では、情報処理装置のＣＰＵ２０１は、ステップＳ４０１でユーザか

らオープン要求を受けたファイルに対応する保持ファイル情報に、当該ファイルの鍵情報があるか否かを判断する。

【００５７】

鍵情報がある場合（ステップＳ４０５：ＹＥＳ）は、処理をステップＳ４１３に移行する。

【００５８】

ステップＳ４１３では、情報処理装置のＣＰＵ２０１は、当該鍵情報の有効期限を確認し、有効期限内であるか否かを判断する。

【００５９】

有効期限内であると判断された場合（ステップＳ４１３：ＹＥＳ）は、処理をステップＳ４１０に移行する。

【００６０】

ステップＳ４１０では、情報処理装置のＣＰＵ２０１は、鍵管理サーバ１０３への確認をせずに復号をしてもよいファイルであると判断し、当該鍵情報を用いて、当該ファイルを復号する。なお、本発明において利用する暗号化方式は、共通鍵暗号方式と呼ばれるものであり、例えばＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｉｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）などの公知技術を用いて、システム全体で統一された暗号化処理を行う。

【００６１】

有効期限内ではないと判断された場合（ステップＳ４１３：ＮＯ）は、本フローチャートの処理を終了する。なお、この時点で、保持ファイル情報から鍵情報を削除する処理を実行するようにしても良い。

【００６２】

鍵情報がない場合（ステップＳ４０５：ＮＯ）は、処理をステップＳ４０６に移行する。

【００６３】

ステップＳ４０６では、情報処理装置のＣＰＵ２０１は、鍵管理サーバ１０３への鍵要求が必要であると判断し、鍵管理サーバ１０３への接続を試み、接続の可否を判断する。

【００６４】

鍵管理サーバ１０３への接続が不可能であると判断された場合（ステップＳ４０６：ＮＯ）は、鍵情報の取得が不可能であると判断し、ユーザへその旨の通知（エラーメッセージの表示等）を行い、本フローチャートに示す処理を終了する。

【００６５】

鍵管理サーバ１０３への接続が可能であると判断された場合（ステップＳ４０６：ＹＥＳ）は、処理をステップＳ４０７に移行する。

【００６６】

ステップＳ４０７では、情報処理装置のＣＰＵ２０１は、ネットワークへの接続形態を検出する。ネットワークの接続形態を検出する方法としては、例えばＯＳに付属されたネットワーク構成ツール（Ｗｉｎｄｏｗｓ（登録商標）であればｉｐｃｏｎｆｉｇ、Ｌｉｎｕｘであればｉｆｃｏｎｆｉｇ）などの公知技術を用いて検出する。

【００６７】

ステップＳ４０８では、情報処理装置のＣＰＵ２０１は、保持ファイル情報から取得できるファイルＩＤおよびファイル管理プログラム３１３の起動時にユーザによって入力されたユーザ情報およびステップＳ４０７で検出したネットワーク接続形態情報を鍵管理サーバ１０３に送信する。

【００６８】

ここで、図５を用いて、図４のステップＳ４０８にて情報処理装置から鍵管理サーバ１０３に対してファイルＩＤ、ユーザ情報、ネットワーク接続形態が送信された場合における、鍵管理サーバ１０３が実行する鍵発行処理について説明する。

【００６９】

なお、図５のフローチャートで示す処理については、鍵管理サーバ１０３のＣＰＵ２０

１が所定の制御プログラムを読み出して実行する処理である。
【００７０】
ステップＳ５０１では、鍵管理サーバ１０３のＣＰＵ２０１は、情報処理装置から送信されたファイルＩＤ、ユーザ情報、ネットワーク接続形態を受信する。
【００７１】
ステップＳ５０２では、鍵管理サーバ１０３のＣＰＵ２０１は、受信したユーザ情報が正当なものであるか否かを判断する。具体的には、例えばＬＤＡＰサーバ１０１等を利用して、当該ユーザ情報が登録されているか否かによって判断する。
【００７２】
正当なものであると判断された場合（ステップＳ５０２：ＹＥＳ）は、処理をステップＳ５０４に移行する。
【００７３】
正当なものではないと判断された場合（ステップＳ５０２：ＮＯ）は、ステップＳ５０３にて鍵の送信を拒絶し、本フローチャートに示す処理を終了する。
【００７４】
ステップＳ５０４では、鍵管理サーバ１０３は、ユーザ情報が正当であると判断されたユーザに対してステップＳ５０１で受信したファイルＩＤに対応する鍵が発行されているか否かを判断する。具体的には、鍵発行情報（図２０）に登録されたユーザ名とファイルＩＤとをもとにして判断する。
【００７５】
鍵が発行されていると判断された場合（ステップＳ５０４：ＹＥＳ）は、処理をステップＳ５０５に移行する。
【００７６】
鍵が発行されていないと判断された場合（ステップＳ５０４：ＮＯ）は、ステップＳ５０３にて鍵の送信を拒絶し、本フローチャートに示す処理を終了する。
【００７７】
ステップＳ５０５では、鍵管理サーバ１０３は、鍵発行情報（図２０）からステップＳ５０１で取得したユーザ情報、ファイルＩＤに対応するエントリを取得する。
【００７８】
ステップＳ５０６では、鍵管理サーバ１０３は、ステップＳ５０５で取得したエントリの鍵の有効期限が切れていないかを判断する。具体的には、現在時刻と有効期限とを比較することで判断する。
【００７９】
有効期限が切れていると判断された場合（ステップＳ５０６：ＮＯ）は、ステップＳ５０３の処理を実行し、本フローチャートに示す処理を終了する。
【００８０】
有効期限が切れていないと判断された場合（ステップＳ５０６：ＹＥＳ）は、処理をステップＳ５０７に移行する。
【００８１】
ステップＳ５０７では、鍵管理サーバ１０３は、ステップＳ５０１で情報処理装置から受信したネットワーク接続形態がネットワーク定義情報３０６（図１７）にあるか否かを判断する。
【００８２】
ネットワーク定義情報にあると判断された場合（ステップＳ５０７：ＹＥＳ）は、処理をステップＳ５０８に移行する。
【００８３】
ネットワーク定義情報にないと判断された場合（ステップＳ５０７：ＮＯ）は、管理者が想定していないネットワークからの接続であると判断され、ステップ５０３の処理を経て本フローチャートに示す処理を終了する。
【００８４】

ステップＳ５０８では、鍵管理サーバ１０３のＣＰＵ２０１は、アクセス制御情報３０８（図１９）からステップＳ５０１で受信したファイルＩＤに対応するエントリを取得する。

【００８５】

ステップＳ５０９では、鍵管理サーバ１０３のＣＰＵ２０１は、ステップＳ５０８で取得したエントリに基づき、ステップＳ５０１で取得したユーザＩＤにより識別されるユーザが、ステップＳ５０１で取得したネットワーク接続形態において、ステップＳ５０１で取得したファイルＩＤで識別されるファイルに対してアクセス可能か否かを判断する。

【００８６】

アクセス可能であると判断された場合（ステップＳ５０９：ＹＥＳ）は、処理をステップＳ５１０に移行する。

【００８７】

アクセス不可であると判断された場合（ステップＳ５０９：ＮＯ）は、ステップＳ５０３の処理を実行し、本フローチャートに示す処理を終了する。

【００８８】

ステップＳ５１０では、鍵管理サーバ１０３のＣＰＵ２０１は、ステップＳ５０９でアクセス可能と判断されたファイルおよびユーザから特定される鍵（鍵発行情報（図２０）を用いて、ファイルＩＤ，ユーザから鍵を特定する）と、アクセス制限情報とアクセスルールＩＤにより当該ファイルに対して許可されている操作のリストを情報処理装置に送信する。そして、本フローチャートに示す処理を終了する。

図４に示すフローチャートの説明に戻る。

【００８９】

ステップＳ４０９では、情報処理装置のＣＰＵ２０１は、鍵管理サーバ１０３から鍵情報の応答があるか否かを判断する。具体的には、ステップＳ５１０の処理が実行された場合には、鍵管理サーバ１０３からの応答あり（ステップＳ４０９：ＹＥＳ）と判断される。他方、ステップＳ５０３の処理が実行された場合には、鍵管理サーバ１０３からの応答なし（ステップＳ４０９：ＮＯ）と判断される。

【００９０】

鍵管理サーバ１０３からの応答があった場合（ステップＳ４０９：ＹＥＳ）は、処理をステップＳ４１０に移行する。

【００９１】

鍵管理サーバ１０３からの応答がなかった場合（ステップＳ４０９：ＮＯ）は、本フローチャートに示す処理を終了する。

【００９２】

ステップＳ４１０では、情報処理装置のＣＰＵ２０１は、鍵管理サーバ１０３から送信された鍵を用いて、ステップＳ４０１でオープン要求をされたファイルを復号する。

【００９３】

ステップＳ４１１では、情報処理装置のＣＰＵ２０１は、ステップＳ４１０で復号したファイルを開く適切なプログラムを子プロセスとして起動する。

【００９４】

ステップＳ４１２では、情報処理装置のＣＰＵ２０１は、ステップＳ４０９で受信した鍵、許可操作リストおよびファイルの情報とプロセスの対応をメモリに記録する。ここで記録する各種情報は、後述するファイル書き込み時の処理（図６）において利用する。

【００９５】

図４及び図５に示すフローチャートの処理により、情報処理装置が接続しているネットワークに応じて、ファイルを復号するための鍵を取得できるか否かが判断されため、ネットワーク接続形態によっては、ファイルを復号することが不可能となり、情報漏洩やファイルの改竄等の可能性を低減することが可能となる。

【００９６】

また、一度復号鍵を取得した場合は、一定期間であれば当該鍵をサーバから取得するこ

となくファイルを復号することが可能となるため、ネットワークに接続できない状態においてもファイルの利用が可能となり、利便性も確保することができる。

【００９７】

次に、図６を用いて、本発明の実施形態において情報処理装置（１０４、１０５、１０６）が実行するファイル書き込み時の処理について説明する。

【００９８】

なお、図６のフローチャートで示す処理については、情報処理装置のＣＰＵ２０１が所定の制御プログラムを読み出して実行する処理である。

【００９９】

ステップＳ６０１では、情報処理装置のＣＰＵ２０１は、ステップＳ４１２において管理・監視されている子プロセスによる、ステップＳ４１０で復号されたファイルへの情報の書き込みを検知する。

【０１００】

ステップＳ６０２では、情報処理装置のＣＰＵ２０１は、ステップＳ４１２において記録した許可操作リストに基づき、ステップＳ４１１にて起動したプロセスによる当該ファイルへの書き込みが許可されているか否かを判断する。

【０１０１】

許可されていると判断された場合（ステップＳ６０２：ＹＥＳ）は、処理をステップＳ６０４に移行する。

【０１０２】

許可されていないと判断された場合（ステップＳ６０２：ＮＯ）は、処理をステップＳ６０３に移行する。

【０１０３】

ステップＳ６０３では、情報処理装置のＣＰＵ２０１は、ステップＳ４１１で起動したプロセスによる書き込み処理を中止し、本フローチャートに示す処理を終了する。

【０１０４】

ステップＳ６０４では、情報処理装置のＣＰＵ２０１は、ステップＳ４１１で起動したプロセスによる書き込み処理が終了した後、当該プロセスに対応する鍵でファイルを暗号化する。

【０１０５】

ステップＳ６０５では、情報処理装置のＣＰＵ２０１は、ステップＳ６０４で暗号化された後のファイルのハッシュ値を計算する。

【０１０６】

ステップＳ６０６では、情報処理装置のＣＰＵ２０１は、ステップＳ６０５でハッシュ値を計算したファイルについての保持ファイル情報のハッシュ値を、ステップＳ６０５で計算したハッシュ値に更新する。

そして、本フローチャートに示す処理を終了する。

【０１０７】

以上の処理により、保持ファイル情報を当該書き込み後のファイルに更新することで、ファイルに書き込み処理が行われた場合にも、一定期間であれば再度復号鍵をサーバから取得することなく、従来の復号鍵を用いてファイルを復号することができる。これにより、ネットワークに接続できない場合等でもセキュリティを確保しつつ作業の利便性を確保することが可能となる。

【０１０８】

次に、図７を用いて、本発明の実施形態において情報処理装置（１０４、１０５、１０６）が鍵管理サーバ１０３からファイルを取得する際の情報処理装置（１０４、１０５、１０６）および鍵管理サーバ１０３の処理について説明する。

【０１０９】

なお、図７のフローチャートで示すＳ７０１、Ｓ７０４、Ｓ７０５、Ｓ７１０、Ｓ７１１、Ｓ７１４～Ｓ７１６の処理については、情報処理装置のＣＰＵ２０１が所定の制御プ

ログラムを読み出して実行する処理である。
【０１１０】
Ｓ７０２、Ｓ７０３、Ｓ７０６～Ｓ７０９、Ｓ７１２、Ｓ７１３の処理については、鍵管理サーバ１０３のＣＰＵ２０１が所定の制御プログラムを読み出して実行する処理である。
【０１１１】
ステップＳ７０１では、情報処理装置のＣＰＵ２０１は、鍵管理サーバ１０３に対して、資格情報（ユーザ名、パスワード等、鍵管理サーバ１０３へのログインに必要なユーザ識別情報）を送信する。
【０１１２】
ステップＳ７０２では、鍵管理サーバ１０３のＣＰＵ２０１は、ステップＳ７０１で情報処理装置から送信された資格情報を、ＬＤＡＰサーバ１０１を用いて照合する。
【０１１３】
ステップＳ７０３では、鍵管理サーバ１０３のＣＰＵ２０１は、ＬＤＡＰサーバ１０１を用いた照合結果をもとに、ステップＳ７０１で情報処理装置から送信された資格情報が正当であるか否か（鍵管理サーバ１０３へのログインが許可されるユーザであるか否か）を判断する。
【０１１４】
正当であると判断された場合（ステップＳ７０３：ＹＥＳ）は、当該結果を情報処理装置に送信して、処理をステップＳ７０６に移行する。
【０１１５】
正当ではないと判断された場合（ステップＳ７０３：ＮＯ）は、当該結果を情報処理装置に送信して、本フローチャートに示す処理を終了する。
【０１１６】
ステップＳ７０４では、情報処理装置のＣＰＵ２０１は、ステップＳ７０３で鍵管理サーバ１０３から送信された結果からログインに成功したか否かを判断する。
【０１１７】
ログインに成功した場合（ステップＳ７０４：ＹＥＳ）は、処理をステップＳ７０５に移行する。
【０１１８】
ログインに失敗した場合（ステップＳ７０４：ＮＯ）は、本フローチャートに示す処理を終了する。
【０１１９】
ステップＳ７０５では、情報処理装置のＣＰＵ２０１は、鍵管理サーバ１０３に対してファイル取得要求を送信する。このファイル取得要求には、取得するファイルを特定する情報（ファイルＩＤやファイルパス等）や鍵情報の要求有無に関する情報が含まれる。
【０１２０】
ステップＳ７０６では、鍵管理サーバ１０３のＣＰＵ２０１は、情報処理装置からの取得要求を受信する。
【０１２１】
ステップＳ７０７では、鍵管理サーバ１０３のＣＰＵ２０１は、ステップＳ７０６で情報処理装置から取得要求がなされたファイルがファイルサーバ１０２から取得可能であるか否かを判断し、その結果を情報処理装置に送信する。
【０１２２】
なお、ステップＳ７０７におけるファイル取得可否の判断は、ファイルの作成者やサーバ、部門の管理者等がファイルに対して設定したアクセスルールに従って判断される。例えば、ファイルに対して「一般者によるファイル取得は禁止」というアクセスルールが設定されていた場合は、ログインユーザが一般者であればファイルの取得は不可能であると判断されることになる。また、設定によっては複数のルールに該当する可能性もあるが、その場合、少なくとも１つ以上のルールでファイルの取得が許可されていれば、ファイル

の取得が可能となる。

【０１２３】

ファイルを取得可能と判断された場合（ステップＳ７０７：ＹＥＳ）は、処理をステップＳ７０８に移行する。

【０１２４】

ファイル取得が不可能と判断された場合（ステップＳ７０７：ＮＯ）は、本フローチャートに示す処理を終了する。

【０１２５】

ステップＳ７０８では、鍵管理サーバ１０３のＣＰＵ２０１は、当該ファイルを暗号化するための暗号鍵を作成し、鍵発行情報３０９（図２０）を更新する。そして、当該暗号鍵で当該ファイルを暗号化する。

【０１２６】

なお、暗号鍵を作成する場合は、同じ鍵で異なるファイルを復号できないようにするため、以前に発行されたものとは重複しないようにする。

【０１２７】

ステップＳ７０９では、鍵管理サーバ１０３のＣＰＵ２０１は、ステップＳ７０８で暗号化されたファイルを情報処理装置へ送信する。

【０１２８】

ステップＳ７１０では、情報処理装置のＣＰＵは、ステップ７０７で鍵管理サーバ１０３から送信された取得可否の結果を受信し、取得の可否を判断する。

【０１２９】

ファイルの取得が可能であると判断された場合（ステップＳ７１０：ＹＥＳ）は、処理をステップＳ７１１に移行する。

【０１３０】

ファイルの取得が不可能であると判断された場合（ステップＳ７１０：ＮＯ）は、本フローチャートに示す処理を終了する。

【０１３１】

ステップＳ７１１では、情報処理装置のＣＰＵ２０１は、ステップＳ７０９で鍵管理サーバ１０３から送信された暗号化されたファイルを受信する。

【０１３２】

ステップＳ７１２では、鍵管理サーバ１０３のＣＰＵ２０１は、ステップＳ７０５で情報処理装置から送信されたファイル取得要求に鍵情報の要求が含まれ、かつ当該取得要求がされたファイルについて、当該取得要求をしたユーザに対する鍵情報の送信許可があるか否かをアクセス制御情報（図１９）をもとに判定する。そして、判定結果を情報処理装置へ送信する。

【０１３３】

鍵情報の送信許可がある場合（ステップＳ７１２：ＹＥＳ）は、処理をステップＳ７１３へ移行する。

【０１３４】

鍵情報の送信許可がない場合（ステップＳ７１２：ＮＯ）は、本フローチャートに示す処理を終了する。

【０１３５】

ステップＳ７１３では、鍵管理サーバ１０３のＣＰＵ２０１は、鍵情報を情報処理装置に送信する。

【０１３６】

ステップＳ７１４では、情報処理装置のＣＰＵ２０１は、ステップＳ７１２で鍵管理サーバ１０３から送信された鍵情報の送信可否の判定結果を受信し、鍵情報の取得の可否を判断する。

【０１３７】

鍵情報の取得が可能であると判断された場合（ステップＳ７１４：ＹＥＳ）は、処理を

ステップＳ７１５へ移行する。
【０１３８】
鍵情報の取得が不可能である場合、またはステップＳ７０５で鍵情報の取得要求をしていない場合（ステップＳ７１４：ＮＯ）は、処理をステップＳ７１６へ移行する。
【０１３９】
ステップＳ７１５では、情報処理装置のＣＰＵ２０１は、ステップＳ７１３で送信された鍵情報を取得し、保存する。なお、受信した鍵情報を保存する場合に、別途情報処理装置の使用者にパスワード等の入力を求めて暗号化することでセキュリティを高めるような構成としても良い。
【０１４０】
ステップＳ７１６では、情報処理装置のＣＰＵ２０１は、保持情報ファイル（図８）をステップＳ７１５で取得した鍵情報に更新する。そして、本フローチャートに示す処理を終了する。
【０１４１】
以上の処理により、サーバから取得するファイルについても暗号化されるため、当該ファイルについても本発明におけるアクセス制御システムの対象とすることができる。
【０１４２】
次に、図８を用いて、本発明の実施形態において情報処理装置（１０４、１０５、１０６）が鍵管理サーバ１０３に対してファイルをアップロードする場合の処理、およびファイルを削除する場合の処理について説明する。
【０１４３】
なお、図８のフローチャートで示す処理については、情報処理装置のＣＰＵ２０１が所定の制御プログラムを読み出して実行する処理である。
【０１４４】
ステップＳ８０１では、情報処理装置のＣＰＵ２０１は、ユーザによるファイルに対する操作がファイルの削除であるか、鍵管理サーバ１０３へのアップロードであるかを判断する。
【０１４５】
ファイルの削除である場合（ステップＳ８０１：削除）は、処理をステップＳ８０５に移行する。
【０１４６】
ファイルのアップロードである場合（ステップＳ８０１：アップロード）は、処理をステップＳ８０２に移行する。
【０１４７】
ステップＳ８０２では、情報処理装置のＣＰＵ２０１は、当該アップロードされるファイルと、鍵管理サーバ１０３にログインするために資格情報とを鍵管理サーバ１０３へ送信する。
【０１４８】
ステップＳ８０３では、情報処理装置のＣＰＵ２０１は、ステップＳ８０２において送信された送信処理の結果（送信に成功したか否か）を鍵管理サーバ１０３から受信する。
【０１４９】
ステップＳ８０４では、情報処理装置のＣＰＵ２０１は、ステップＳ８０３で受信した送信処理の結果を判断する。
【０１５０】
送信に失敗した場合（ステップＳ８０４：ＮＯ）は、本フローチャートに示す処理を終了する。
【０１５１】
送信に成功した場合（ステップＳ８０４：ＹＥＳ）は、処理をステップＳ８０５に移行する。
【０１５２】

ステップＳ８０５では、情報処理装置のＣＰＵ２０１は、当該送信した、またはユーザから削除操作が行われたファイルを情報処理装置の記憶領域から削除する。

【０１５３】

ステップＳ８０６では、情報処理装置のＣＰＵ２０１は、ステップＳ８０５で記憶領域から削除されたファイルに関する情報が保持ファイル情報３１９にあるか否かを判断する。

【０１５４】

あると判断された場合（ステップＳ８０６：ＹＥＳ）は、処理をステップＳ８０７に移行する。

【０１５５】

ないと判断された場合（ステップＳ８０６：ＮＯ）は、本フローチャートに示す処理を終了する。

【０１５６】

ステップＳ８０７では、情報処理装置のＣＰＵ２０１は、保持ファイル情報３１９からステップＳ８０５で記憶領域から削除されたファイルに関する情報を削除する。

【０１５７】

ステップＳ８０８では、情報処理装置のＣＰＵ２０１は、鍵管理サーバ１０３へ、当該ファイルの鍵発行情報の削除要求を送信する。そして本フローチャートに示す処理を終了する。

【０１５８】

なお、鍵管理サーバ１０３は、情報処理装置からの要求通りに鍵発行情報を削除しても構わないし、鍵の発行履歴を保存するために有効期限のみを書き換えるようにしてもかまわない。

【０１５９】

次に、図９を用いて、本発明の実施形態において鍵管理サーバ１０３におけるファイルのアップロード時の処理について説明する。

【０１６０】

なお、図９のフローチャートで示す処理については、鍵管理サーバ１０３のＣＰＵ２０１が所定の制御プログラムを読み出して実行する処理である。

【０１６１】

ステップＳ９０１では、鍵管理サーバ１０３のＣＰＵ２０１は、鍵管理サーバ１０３のＣＰＵ２０１は、ステップＳ８０２で情報処理装置から送信されたファイルおよび資格情報を受信する。

【０１６２】

ステップＳ９０２では、鍵管理サーバ１０３のＣＰＵ２０１は、ステップＳ９０１で受信した資格情報を用いてＬＤＡＰサーバ１０１に正当なユーザであるか否かを問い合わせる。

【０１６３】

ステップＳ９０３では、鍵管理サーバ１０３のＣＰＵ２０１は、ステップＳ９０２で問い合わせた結果をもとに、当該ユーザが正当なユーザであるか否かを判断する。

【０１６４】

正当なユーザである場合（ステップＳ９０３：ＹＥＳ）は、処理をステップＳ９０５に移行する。

【０１６５】

正当ではないユーザの場合（ステップＳ９０３：ＮＯ）は、処理をステップＳ９０４に移行する。

【０１６６】

ステップＳ９０４では、鍵管理サーバ１０３のＣＰＵ２０１は、情報処理装置に対して、ファイルのアップロードに失敗した旨の通知を出して、本フローチャートに示す処理を終了する。

【０１６７】
ステップＳ９０５では、鍵管理サーバ１０３のＣＰＵ２０１は、ステップＳ９０３で正当なユーザであると判断されたユーザが、アップロードをするファイルの保存先に対する書き込み権限があるか否かを判断する。
【０１６８】
書き込み権限がある場合（ステップＳ９０５：ＹＥＳ）は、処理をステップＳ９０６に移行する。
【０１６９】
書き込み権限がない場合（ステップＳ９０５：ＮＯ）は、処理をステップＳ９０４に移行し、情報処理装置に対して、ファイルのアップロードに失敗した旨の通知を出して、本フローチャートに示す処理を終了する。
【０１７０】
ステップＳ９０６では、鍵管理サーバ１０３のＣＰＵ２０１は、書き込み先に当該ファイルがあるか否かを判断する。すなわち、既存のファイルがアップロードされたか、それとも新規ファイルがアップロードされたかを判断する。
【０１７１】
書き込み先にファイルがあると判断された場合（すなわち既存のファイルがアップロードされた場合）（ステップＳ９０６：ＮＯ）は、処理をステップＳ９０７に移行する。
【０１７２】
書き込み先のファイルがないと判断された場合（すなわち新規ファイルがアップロードされた場合）（ステップＳ９０６：ＹＥＳ）は、処理をステップＳ９１０に移行する。
【０１７３】
ステップＳ９０７では、鍵管理サーバ１０３のＣＰＵ２０１は、当該ユーザと当該既存のファイルに対する鍵情報を鍵発行情報３０９から取得する。
【０１７４】
ステップＳ９０８では、鍵管理サーバ１０３のＣＰＵ２０１は、ステップＳ９０７で鍵発行情報を取得できたか否かを判断する。
【０１７５】
鍵発行情報を取得出来た場合（ステップＳ９０８：ＹＥＳ）は、処理をステップＳ９０９に移行する。
【０１７６】
鍵発行情報を取得出来なかった場合（ステップＳ９０８：ＮＯ）は、処理をステップＳ９０４に移行し、情報処理装置に対して、ファイルのアップロードに失敗した旨の通知を出して、本フローチャートに示す処理を終了する。
【０１７７】
ステップＳ９０９では、鍵管理サーバ１０３のＣＰＵ２０１は、該当する鍵でファイルを復号する。
【０１７８】
ステップＳ９１０では、鍵管理サーバ１０３のＣＰＵ２０１は、アップロードされたファイルの書き込み先がアクセスルールに該当するか否かを判断する。
【０１７９】
アクセスルールに該当すると判断された場合（ステップＳ９１０：ＹＥＳ）は、処理をステップＳ９１１に移行する。
【０１８０】
アクセスルールに該当しないと判断された場合（ステップＳ９１０：ＮＯ）は、処理をステップＳ９１２に移行する。
【０１８１】
ステップＳ９１１では、鍵管理サーバ１０３のＣＰＵ２０１は、アップロードされるファイルに対する新規アクセス制限情報を作成し、アクセス制限情報（図１９）に追加登録する。

【０１８２】
ステップＳ９１２では、鍵管理サーバ１０３のＣＰＵ２０１は、書き込み先のファイルサーバ１０２にファイルを保存する。
【０１８３】
ステップＳ９１３では、鍵管理サーバ１０３のＣＰＵ２０１は、ファイルのアップロードに成功した旨を情報処理装置に対して通知する。そして本フローチャートに示す処理を終了する。
【０１８４】
次に、図１０を用いて、本発明の実施形態において鍵管理サーバ１０３におけるアクセスルールの変更処理について説明する。
【０１８５】
なお、図１０のフローチャートで示す処理については、鍵管理サーバ１０３のＣＰＵ２０１が所定の制御プログラムを読み出して実行する処理である。
【０１８６】
ステップＳ１００１では、鍵管理サーバ１０３のＣＰＵ２０１は、情報処理装置からアクセスルールの変更要求を受け付ける。
【０１８７】
ステップＳ１００２では、鍵管理サーバ１０３のＣＰＵ２０１は、ステップＳ１００２で受け付けたアクセスルールの変更をアクセスルール情報３０７（図１８）へ反映させる。
【０１８８】
ステップＳ１００３では、鍵管理サーバ１０３のＣＰＵ２０１は、ステップＳ１００２で追加および変更されたアクセスルールをアクセスルール情報３０７（図１８）から取得し、当該ルールで指定されるファイルおよびディレクトリ内のファイルの情報を取得する。
【０１８９】
そして、ステップＳ１００５～Ｓ１００８までの処理を繰り返す（ステップＳ１００４）。
【０１９０】
ステップＳ１００５では、鍵管理サーバ１０３のＣＰＵ２０１は、ステップＳ１００５～Ｓ１００８の処理の対象となっているファイルに対するアクセス制御情報が存在するか否かを判断する。
【０１９１】
アクセス制御情報が存在すると判断された場合（ステップＳ１００５：ＹＥＳ）は、処理をステップＳ１００７に移行する。
【０１９２】
アクセス制御情報が存在しないと判断された場合（ステップＳ１００５：ＮＯ）は、処理をステップＳ１００６に移行する。
【０１９３】
ステップＳ１００６では、鍵管理サーバ１０３のＣＰＵ２０１は、処理対象のファイルに対する新しいアクセス制御情報を作成し、次のファイルに対する繰り返し処理へ移行する。
【０１９４】
ステップＳ１００７では、鍵管理サーバ１０３のＣＰＵ２０１は、ステップＳ１００５で確認されたアクセス制御情報のアクセスルールＩＤに、ステップＳ１００２で変更されたアクセスルールのＩＤが含まれるか否かを判断する。
【０１９５】
含まれると判断された場合（ステップＳ１００７：ＹＥＳ）は、次のファイルに対する繰り返し処理へ移行する。
【０１９６】

含まれないと判断された場合（ステップＳ１００７：ＮＯ）は、処理をステップＳ１００８に移行する。

【０１９７】

ステップＳ１００８では、鍵管理サーバ１０３のＣＰＵ２０１は、ステップＳ１００２で変更されたアクセスルールのＩＤを、ステップＳ１００５で確認されたアクセス制御情報に追加する。そして、次のファイルに対する繰り返し処理へ移行する。

【０１９８】

以上の処理により、アクセス制限ルールが変更や追加された場合にも、変更・追加された新たなルールをファイルに適用することが可能となる。

次に、図１１～図１６に示す各画面について説明する。

【０１９９】

図１１は、情報処理装置で実行されるファイル管理プログラムの画面の一例である。

【０２００】

画面１１００は、サーバ側の管理ファイルシステムを表示する領域（１１０１）、１１０１において選択されたディレクトリ内のファイル一覧を表示する領域（１１０２）、ローカルのファイルシステムを表示する領域（１１０３）、１１０３において選択されたディレクトリ内のファイル一覧を表示する領域（１１０４）、サーバからのダウンロード指示を受け付けるボタン（１１０５）、サーバへのアップロード指示を受け付けるボタン（１１０６）、鍵を受信するか否かの選択を受け付けるチェックボックス（１１０７）で構成される。

【０２０１】

ユーザによりディレクトリ内のファイル一覧を表示する領域１１０２からファイルが選択され、必要に応じてチェックボックス１１０７がチェックされ、ダウンロード指示ボタン１１０５が押下されることで、図７に示すフローチャートの処理が実行される。

【０２０２】

ユーザによりディレクトリ内のファイル一覧を表示する領域１１０４からファイルが選択され、アップロード指示ボタン１１０６が押下されることで、図９に示すフローチャートの処理が実行される。

【０２０３】

ユーザによりディレクトリ内のファイル一覧を表示する領域１１０４からファイルが選択され、削除指示が行われることで、図８に示すフローチャートの処理が実行される。

【０２０４】

ユーザによりディレクトリ内のファイル一覧を表示する領域１１０４からファイルが選択され、ファイルオープン指示が行われることで、図４に示すフローチャートの処理が実行される。

【０２０５】

図１２は、鍵管理サーバ１０３で実行されるサーバ管理プログラムの画面例である。

【０２０６】

画面１２００は、鍵管理サーバ１０３が管理するファイルサーバのファイルシステムを表示する領域（１２０１）、領域１２０１でユーザにより選択されたディレクトリ内のファイル一覧を表示する領域（１２０２）、ネットワーク定義一覧画面を表示するためのメニュー項目（１２０３）、アクセスルール一覧画面を表示するためのメニュー項目（１２０４）で構成される。

図１３は、ネットワーク定義一覧画面の一例である。

【０２０７】

この画面は、図１２に示すメニュー項目１２０３に対するユーザの操作に応じて表示される。

【０２０８】

画面１３００は、現在のネットワーク定義一覧を表示する領域（１３０１）、新しいネットワーク定義の追加指示を受け付けるボタン（１３０２）、既存のネットワーク定義の

編集を受け付けるボタン（１３０３）、既存のネットワーク定義の削除指示を受け付けるボタン（１３０４）、変更された内容をネットワーク定義情報３０６に反映させる指示を受け付けるボタン（１３０５）、変更された内容を破棄する指示を受け付けるボタン（１３０６）で構成される。

【０２０９】

管理者により、ネットワーク定義追加ボタン１３０２が押下されることで、ネットワーク定義一覧表示領域１３０１に新しい行が追加され、これを編集することで新しいネットワーク定義が追加される。

【０２１０】

管理者により、ネットワーク定義一覧表示領域１３０１のネットワーク定義が選択された状態で編集ボタン１３０３が押下されることで、選択されたネットワーク定義が変更状態となり、これを編集することで、既存のネットワーク定義が編集される。

【０２１１】

管理者により、ネットワーク定義一覧表示領域１３０１のネットワーク定義が選択された状態で削除ボタン１３０４が押下されることで、選択したネットワーク定義が削除される。

図１４はアクセスルール一覧画面の一例である。

【０２１２】

図１４に示すアクセスルール一覧画面は、図１２のメニュー項目１２０４が操作されることで表示される。

【０２１３】

画面１４００は現在のアクセスルール一覧を表示する領域（１４０１）、新しいアクセスルールの追加を受け付けるボタン（１４０２）、既存のアクセスルールの編集を受け付けるボタン（１４０３）、既存のアクセスルールの削除を受け付けるボタン（１４０４）、変更された内容をアクセスルール情報３０７に反映指示を受け付けるボタン（１４０５）、変更された内容を破棄する指示を受け付けるボタン（１４０６）で構成される。

【０２１４】

管理者により、アクセスルール追加ボタン１４０２が押下される又は領域１４０１のアクセスルールが選択された状態で編集受付ボタン１４０３が押下されることで、後述するアクセスルール設定画面１５００（図１５）が表示される。

【０２１５】

管理者により、領域１４０１のアクセスルールが選択された状態で、削除ボタン１４０４が押下されることで、選択されたアクセスルールが削除される。

【０２１６】

管理者が、アクセスルールの編集後に１４０５を押下することで、図１４のフローチャートの処理が実行される。

図１５は、アクセスルール設定画面の一例を図である。

【０２１７】

画面１５００は、接続形態の選択を受け付けるコンボボックス（１５０１）、アクセス制限の内容の選択を受け付ける領域（１５０２）、アクセス対象のユーザの選択を受け付けるコンボボックス（１５０３）、対象となるファイル・ディレクトリを表示する領域（１５０４）、対象となるファイル・ディレクトリの追加を受け付けるためのボタン（１５０５）、既存の対象ファイル・ディレクトリの削除を受け付けるためのボタン（１５０６）、内容を確定させるためのボタン（１５０７）、内容を破棄する指示を受け付けるためのボタン（１５０８）で構成される。

【０２１８】

なお、１５０１の内容は、ネットワーク定義情報３０６から作成される。

図１６は、鍵送信設定画面の一例を示す図である。

【０２１９】

図１６に示す鍵送信設定画面は、図１２のファイル一覧表示領域１２０２からファイル

が選択され、鍵送信設定の操作が行われることで表示される。

【０２２０】

画面１６００は、送信許可の可否の選択を受け付けるチェックボックス（１６０１）、許可対象のユーザ・部署等の一覧を表示する領域（１６０２）、許可対象の追加を受け付けるためのボタン（１６０３）、選択された許可対象を削除する指示を受け付けるためのボタン（１６０４）、設定を反映させる指示を受け付けるためのボタン（１６０５）、設定を破棄する指示を受け付けるためのボタン（１６０６）で構成される。

【０２２１】

許可対象はＬＤＡＰサーバ１０１から情報を取得し、選択する。管理者により内容の編集がなされ、反映ボタン１６０５が押下されることで、アクセス制御情報３０８の鍵送信可否及び許可対象が変更される。

【０２２２】

以上の構成により、情報処理装置の利用場所を限定することなく、管理者が指定した信頼できるネットワーク接続のみにおいて、ファイルに適切なアクセス権を付与することができる。

【０２２３】

また、管理者が特別に許可したファイルにおいては、情報処理装置への鍵の保存が可能となるので、サービスが障害で利用できない場合やネットワークがサービスへ到達不能な場合であっても、ファイルの利用が可能になる。

【０２２４】

また、ユーザごとに鍵を管理しているので、特定のユーザの資格情報が漏洩した場合であっても、対策を講じるまでの間、該ユーザの鍵情報を無効にし、該ユーザに対する鍵の発行を停止することで、他のユーザに影響を与えることなく、許可ネットワークからのなりすましによる機密ファイルの取得・閲覧及びファイルサーバ内のファイルの改竄を防止することができる。

【０２２５】

なお、上述した各種データの構成及びその内容はこれに限定されるものではなく、用途や目的に応じて、様々な構成や内容で構成されることは言うまでもない。

【０２２６】

また、本発明におけるプログラムは、図４～図１０の処理方法をコンピュータが実行可能なプログラムである。なお、本発明におけるプログラムは図４～図１０の各装置の処理方法ごとのプログラムであってもよい。

【０２２７】

以上のように、前述した実施形態の機能を実現するプログラムを記録した記録媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記録媒体に格納されたプログラムを読み出し、実行することによっても本発明の目的が達成されることは言うまでもない。

【０２２８】

この場合、記録媒体から読み出されたプログラム自体が本発明の新規な機能を実現することになり、そのプログラムを記録した記録媒体は本発明を構成することになる。

【０２２９】

プログラムを供給するための記録媒体としては、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、ＣＤ－Ｒ、ＤＶＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ、ＥＥＰＲＯＭ、シリコンディスク等を用いることが出来る。

【０２３０】

また、コンピュータが読み出したプログラム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、そのプログラムの指示に基づき、コンピュータ上で稼働しているＯＳ（オペレーティングシステム）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形態の機能が実現される場合も含まれることは言うまでもな

い。

【０２３１】

さらに、記録媒体から読み出されたプログラムが、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形態の機能が実現される場合も含まれることは言うまでもない。

【０２３２】

また、本発明は、複数の機器から構成されるシステムに適用しても、ひとつの機器から成る装置に適用しても良い。また、本発明は、システムあるいは装置にプログラムを供給することによって達成される場合にも適応できることは言うまでもない。この場合、本発明を達成するためのプログラムを格納した記録媒体を該システムあるいは装置に読み出すことによって、そのシステムあるいは装置が、本発明の効果を享受することが可能となる。

【０２３３】

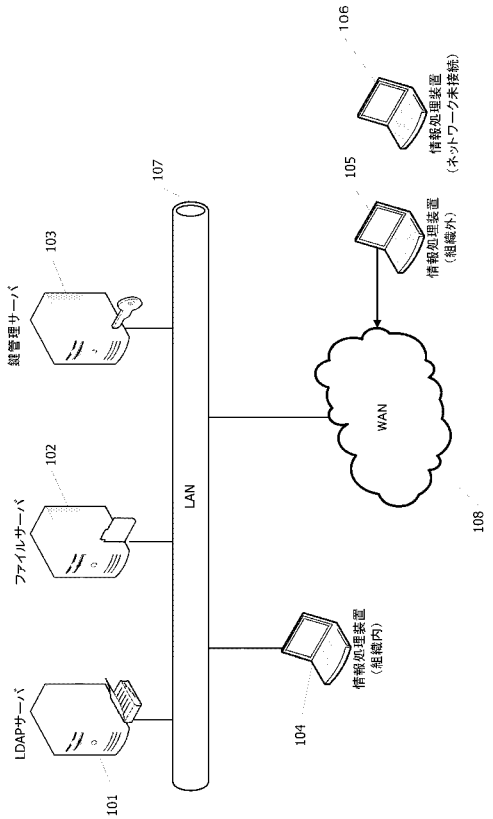
さらに、本発明を達成するためのプログラムをネットワーク上のサーバ、データベース等から通信プログラムによりダウンロードして読み出すことによって、そのシステムあるいは装置が、本発明の効果を享受することが可能となる。なお、上述した各実施形態およびその変形例を組み合わせた構成も全て本発明に含まれるものである。

【符号の説明】

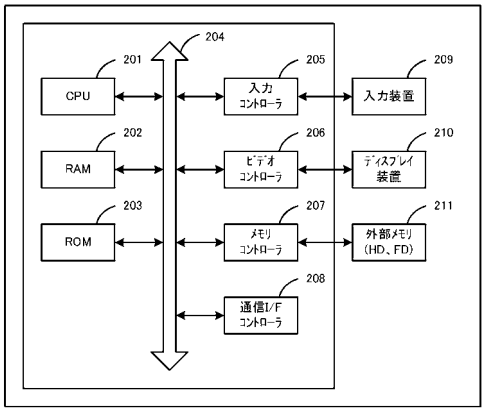
【０２３４】

１０１　ＬＤＡＰサーバ
１０２　ファイルサーバ
１０３　鍵管理サーバ
１０４　情報処理装置（組織内）
１０５　情報処理装置（組織外）
１０６　情報処理装置（ネットワーク未接続）
１０７　ＬＡＮ
１０８　ＷＡＮ

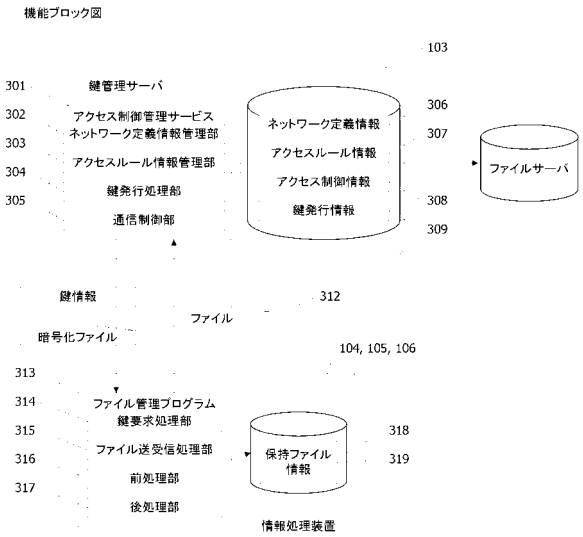
【図１】


106
情報処理装置
（ネットワーク未接続）
107
105
情報処理装置
（組織外）
103
鍵管理サーバ
WAN
102
ファイルサーバ
LAN
108
情報処理装置
（組織内）
LDAPサーバ
104
101

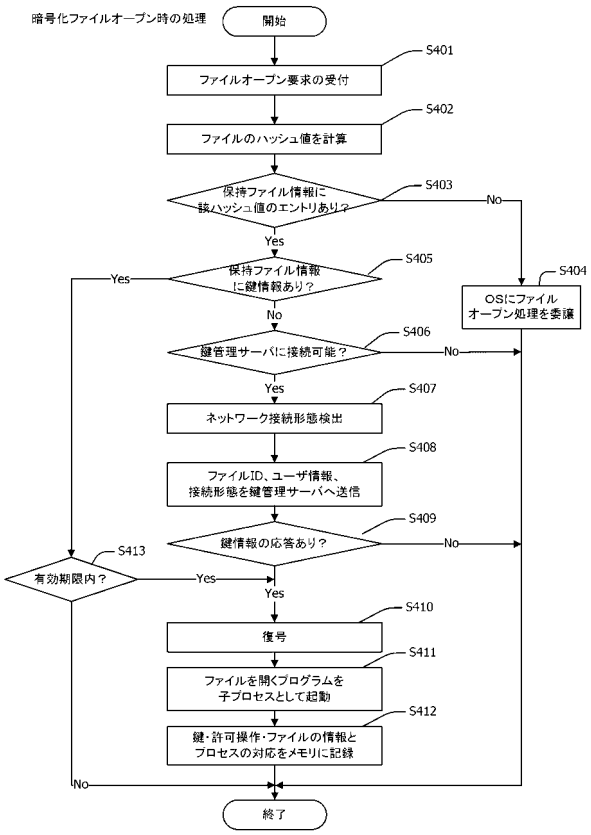
【図２】


204
201
CPU
205
入力
コントローラ
209
入力装置
202
RAM
206
ビデオ
コントローラ
210
ディスプレイ
装置
203
ROM
207
メモリ
コントローラ
211
外部メモリ
(HD、FD)
208
通信I/F
コントローラ

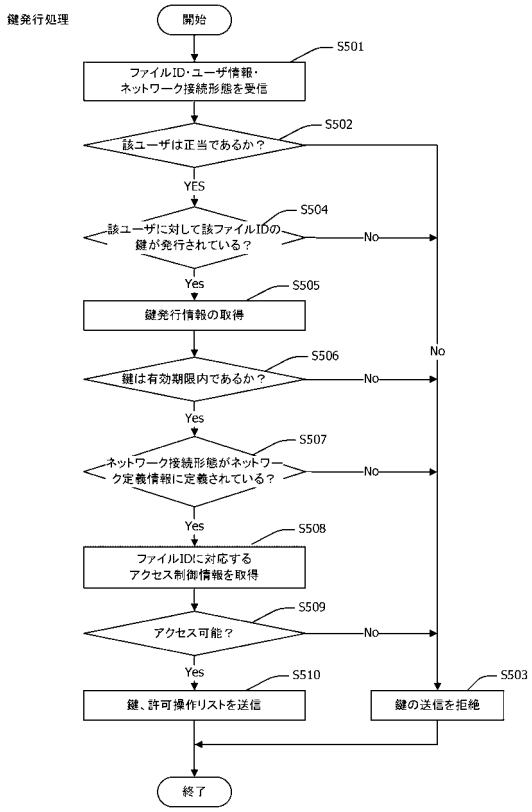
【図３】


機能ブロック図
103
301
鍵管理サーバ
302
アクセス制御管理サービス
ネットワーク定義情報管理部
303
アクセスルール情報管理部
304
鍵発行処理部
305
通信制御部
ネットワーク定義情報
アクセスルール情報
アクセス制御情報
鍵発行情報
306
307
308
309
ファイルサーバ
鍵情報
312
ファイル
暗号化ファイル
104, 105, 106
313
314
ファイル管理プログラム
鍵要求処理部
315
ファイル送受信処理部
316
前処理部
317
後処理部
保持ファイル
情報
318
319
情報処理装置

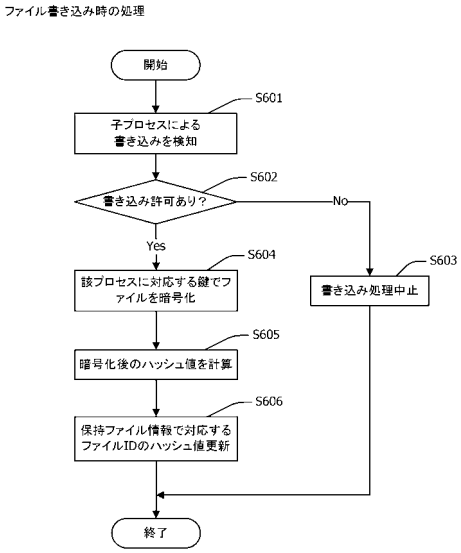
【図４】


暗号化ファイルオープン時の処理
開始
S401
ファイルオープン要求の受付
S402
ファイルのハッシュ値を計算
S403
保持ファイル情報に
該ハッシュ値のエントリあり？
No
Yes
S405
保持ファイル情報
に鍵情報あり？
Yes
S404
OSにファイル
オープン処理を委譲
No
S406
鍵管理サーバに接続可能？
No
Yes
S407
ネットワーク接続形態検出
S408
ファイルID、ユーザ情報、
接続形態を鍵管理サーバへ送信
S409
鍵情報の応答あり？
No
S413
有効期限内？
Yes
Yes
S410
復号
S411
ファイルを開くプログラムを
子プロセスとして起動
S412
鍵・許可操作・ファイルの情報と
プロセスの対応をメモリに記録
No
終了

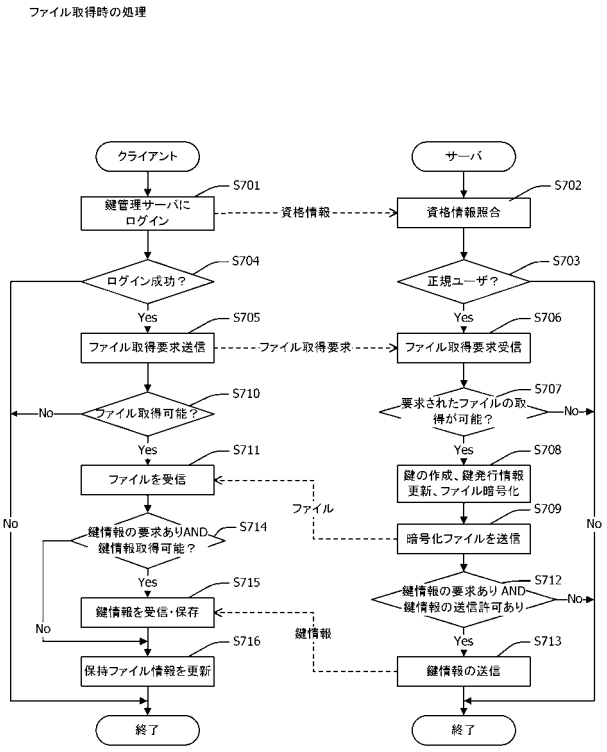
【図５】


鍵発行処理
開始
S501
ファイルID・ユーザ情報・
ネットワーク接続形態を受信
S502
該ユーザは正当であるか？
YES
S504
該ユーザに対して該ファイルIDの
鍵が発行されている？
No
Yes
S505
鍵発行情報の取得
S506
鍵は有効期限内であるか？
No
Yes
S507
ネットワーク接続形態がネットワー
ク定義情報に定義されている？
No
Yes
S508
ファイルIDに対応する
アクセス制御情報を取得
S509
アクセス可能？
No
Yes
S510
鍵、許可操作リストを送信
S503
鍵の送信を拒絶
No
終了

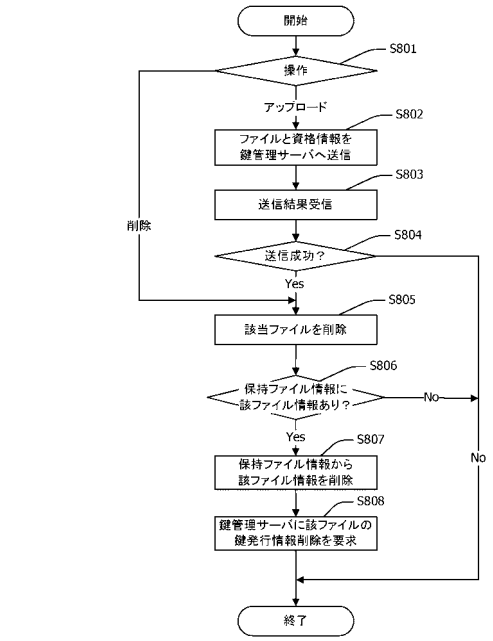
【図６】


ファイル書き込み時の処理
開始
S601
子プロセスによる
書き込みを検知
S602
書き込み許可あり？
No
Yes
S604
該プロセスに対応する鍵でフ
ァイルを暗号化
S603
書き込み処理中止
S605
暗号化後のハッシュ値を計算
S606
保持ファイル情報で対応する
ファイルIDのハッシュ値更新
終了

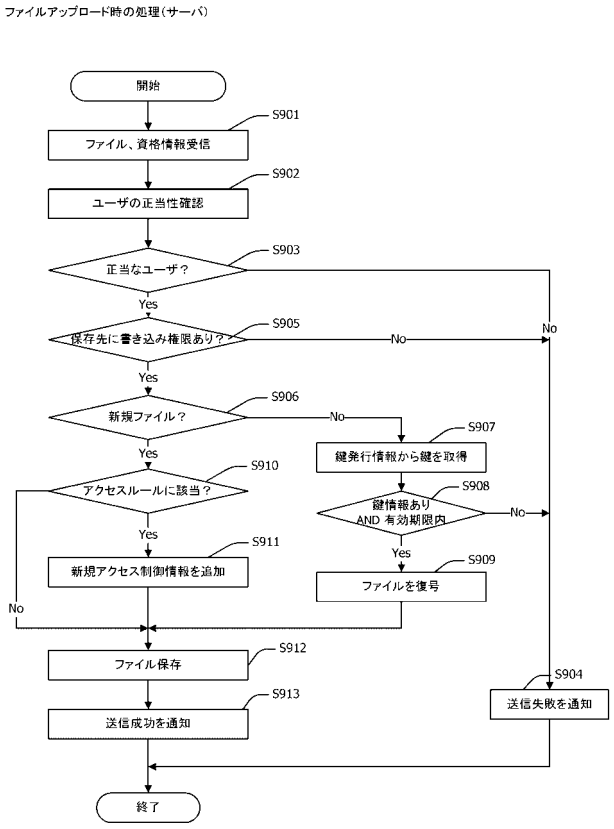
【図７】


ファイル取得時の処理
クライアント
サーバ
S701
鍵管理サーバに
ログイン
資格情報
S702
資格情報照合
S704
ログイン成功？
S703
正規ユーザ？
Yes
S705
ファイル取得要求送信
ファイル取得要求
S706
ファイル取得要求受信
No
S710
ファイル取得可能？
S707
要求されたファイルの取
得が可能？
No
Yes
S711
ファイルを受信
S708
鍵の作成、鍵発行情報
更新、ファイル暗号化
ファイル
S709
暗号化ファイルを送信
No
S714
鍵情報の要求ありAND
鍵情報取得可能？
S712
鍵情報の要求あり AND
鍵情報の送信許可あり
No
S715
鍵情報を受信・保存
鍵情報
S716
保持ファイル情報を更新
S713
鍵情報の送信
終了
終了

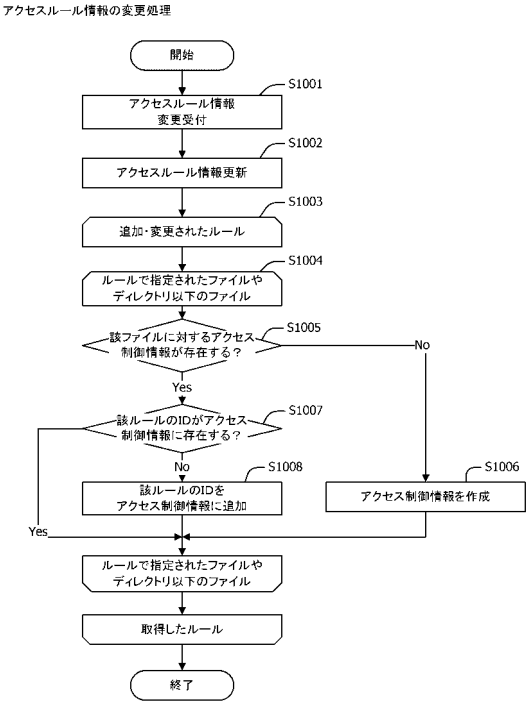
【図８】


ファイルアップロード・削除時の処理（クライアント）
開始
S801
操作
アップロード
削除
S802
ファイルと資格情報を
鍵管理サーバへ送信
S803
送信結果受信
S804
送信成功？
No
Yes
S805
該当ファイルを削除
S806
保持ファイル情報に
該ファイル情報あり？
No
Yes
S807
保持ファイル情報から
該ファイル情報を削除
S808
鍵管理サーバに該ファイルの
鍵発行情報削除を要求
終了

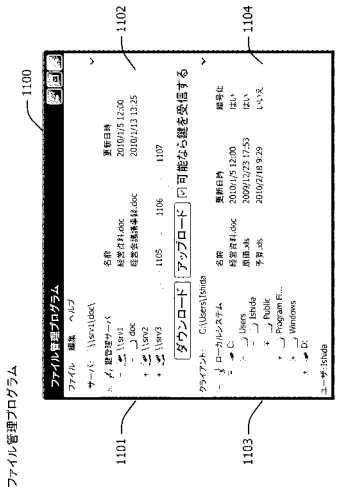
【図９】



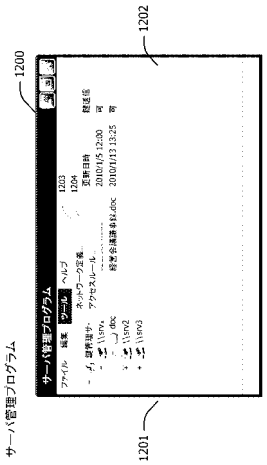
【図１０】



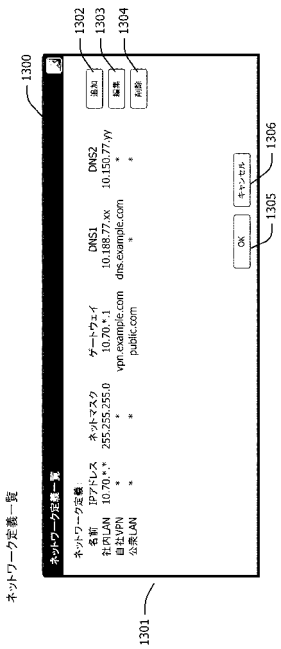
【図１１】



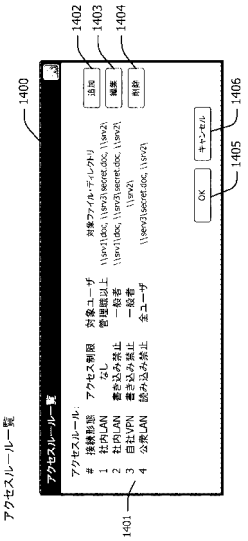
【図１２】



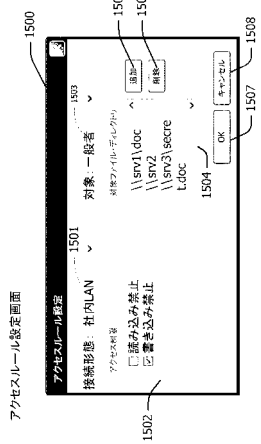
【図１３】



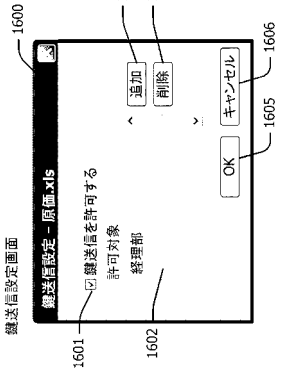
【図１４】



【図１５】



【図１６】



【図１７】

ネットワーク定義情報

接続形態名	IPアドレス	ネットマスク	ゲートウェイ	DNS1	DNS2	…
社内LAN	10.70.*.*	255.255.255.0	10.70.*.1	10.188.77.xx	10.150.77.yy	…
自社VPN			vpn.example.com	dns.example.com		…
公衆LAN			public.com			…
:	:	:	:	:	:	:

【図１８】

アクセスルール情報

アクセスルールID	接続形態	アクセス制限	対象ユーザ	対象ファイル・ディレクトリ
1	社内LAN	なし	管理職以上	¥¥srv1¥doc, ¥¥srv3¥secret.doc, ¥¥srv2¥
2	社内LAN	書き込み禁止	一般者	¥¥srv1¥doc, ¥¥srv3¥secret.doc, ¥¥srv2¥
3	自社VPN	書き込み禁止	一般者	¥¥srv2¥
4	公衆LAN	読み込み禁止	全ユーザ	¥¥srv3¥secret.doc, ¥¥srv2¥
:	:	:	:	:

【図１９】

アクセス制御情報

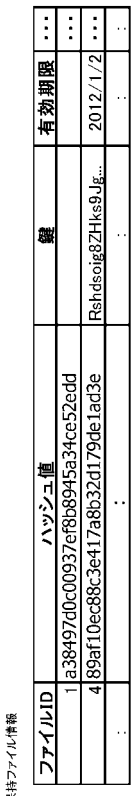
ファイルID	ファイルパス	アクセスルールID	鍵送信可否	許可対象	…
1	¥¥srv1¥doc¥経営資料.doc	1, 2	Yes	経営幹部	…
2	¥¥srv1¥doc¥経営会議議事録.doc	1, 2	Yes	経営幹部	…
3	¥¥srv3¥secret.doc	1, 2, 4	No	–	…
4	¥¥srv2¥経理¥原価.xls	1, 2, 3, 4	Yes	経理部	…
:	:	:	:	:	:

【図２０】

鍵発行情報

ファイルID	ユーザ	鍵	有効期限	…
1	akagi	MSHishaeHaod3hg...	2010/1/1	…
1	ishida	jshOhsor8h80sh32...	2012/3/31	…
2	ueno	pldnuZYdaba332fj...	2011/12/15	…
4	ishida	Rshdsoig8ZHks9Jg...	2012/1/2	…
:	:	:	:	:

【図２１】


保持ファイル情報
ファイルID
ハッシュ値
鍵
有効期限
1
a38497d0c00937ef8b8945a34ce52edd
4
89af10ec88c3e417a8b32d179de1ad3e
Rshdsoig8ZHks9Jg...
2012/1/2

フロントページの続き

(51)Int.Cl.	F I	テーマコード（参考）
	Ｇ０６Ｆ 12/14 ５６０Ａ	

Ｆターム(参考) 5B017 AA03 BA07 BB10 CA16
5B285 AA01 AA04 AA05 BA07 CA02 CA06 CA12 CA16 CA17 CA32
CA41 CA42 CA45 CB02 CB50 CB62 CB72 CB85 DA01 DA04
DA06
5J104 AA16 EA01 EA04 EA15 JA03 NA02 NA27 NA37 PA14