

(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2012-123788

(P2012-123788A)

(43) 公開日 平成24年6月28日(2012.6.28)

| (51) Int.Cl. | F 1 | テーマコード (参考) |
|-----------------------------|------------|-------------|
| G06F 12/00 (2006.01) | GO6F 12/00 | 545M |
| | GO6F 12/00 | 520H |
| | GO6F 12/00 | 545F |
| | GO6F 12/00 | 520E |

審査請求 有 請求項の数 4 O L (全 14 頁)

| | | | |
|--------------|------------------------------|----------|---|
| (21) 出願番号 | 特願2011-243026 (P2011-243026) | (71) 出願人 | 509246150 イーストソフト コーポレーション 大韓民国 137-070 ソウル セオ チヨーニング セオチヨーニドン 1464 -30 イーストビルディング 8階 |
| (22) 出願日 | 平成23年11月7日 (2011.11.7) | (74) 代理人 | 100094248 弁理士 楠本 高義 |
| (31) 優先権主張番号 | 10-2010-0124046 | (72) 発明者 | サン ミン チョ 大韓民国 133-758 ソウル セオ ンドン-グ オクス-ドン サムスン ア パートメント 107-1602 |
| (32) 優先日 | 平成22年12月7日 (2010.12.7) | (72) 発明者 | ヒョン ウー ソン 大韓民国 137-797 ソウル セオ チヨーニング ジャムウォン-ドン 71-1 1 バンポ ハンシン タワー アパート メント 102-1007 |
| (33) 優先権主張国 | 韓国 (KR) | | |

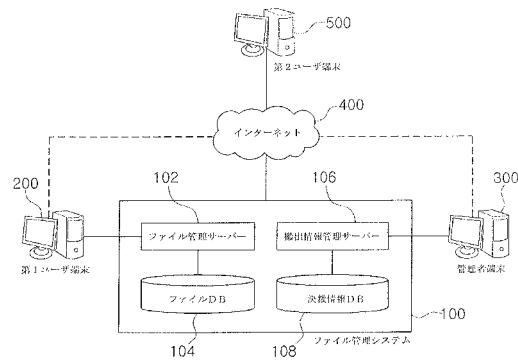
(54) 【発明の名称】ウェブストレージシステムにおけるファイル管理方法

(57) 【要約】

【課題】ファイルに関するデータを流出させることなく、ウェブストレージシステムを利用したファイルの生成及び保存を行ことが可能なウェブストレージシステムにおけるファイル管理方法を提供する。

【解決手段】ファイル管理サーバー、ファイルDB、搬出情報管理サーバー、決裁情報DBを備えたファイル管理システムを用いることにより、ウェブストレージシステムに接続してファイルを生成、変更、保存する場合に、ローカルPCから特定の種類のファイルをすべて削除し、ファイル管理システムにのみ保存させ、ローカルPCには何らの資料を保存させないようにした。

【選択図】図2



【特許請求の範囲】**【請求項 1】**

ネットワークに連結された第1ユーザ端末(200)が生成したファイルを保存するウェブストレージサービスを提供するファイル管理システム(100)が前記第1ユーザ端末(200)に特定の種類のファイルを保存しないように管理する方法であって、

前記第1ユーザ端末(200)がLANまたはインターネット(400)を介して前記ファイル管理システム(100)に接続すれば、前記ファイル管理システム(100)に備えられたファイル管理サーバー(102)が前記第1ユーザ端末(200)にファイル管理クライアントプログラムを転送してインストールするステップと、

前記クライアントプログラムが前記第1ユーザ端末(200)で行われるファイル管理政策を設定して保存した後、前記第1ユーザ端末(200)に対するファイル監視を開始するステップと、

前記クライアントプログラムが前記第1ユーザ端末(200)を監視しつつ、前記ファイル管理政策で監視対象として設定された拡張子を有するファイルを発見すれば、前記クライアントプログラムが前記ファイルを前記ファイル管理システム(100)に転送した後、前記ファイルを前記第1ユーザ端末(200)から削除するステップと、

前記ファイル管理サーバー(102)は、転送された前記ファイルをファイルDB(104)に保存し、前記ファイルを検索することができる情報をDBMSに記録するステップと、

前記第1ユーザ端末(200)が前記ファイル管理システム(100)に接続して、保存された特定のファイルを要請すれば、前記ファイル管理サーバー(102)は、前記第1ユーザ端末(200)がネットワークファイルシステムドライバーを介して前記ファイルDB(104)に接続して、前記特定のファイルを開くように許容するステップと、

前記第1ユーザ端末(200)が前記ファイルの内容または属性を変更して保存を要請すれば、前記ファイル管理サーバー(102)は、前記ファイルの修正及び保存を一つのトランザクションで処理して、前記修正された事項を前記ファイルDB(104)に保存するステップと、

を含むウェブストレージシステムにおけるファイル管理方法。

【請求項 2】

前記クライアントプログラムがインストールされた第1ユーザ端末(200)から特定のファイルに対するUSBメモリ搬出申し込みが前記ファイル管理システム(100)に受け付けられれば、搬出情報管理サーバー(106)が決裁申し込み情報を決裁情報DB(108)に保存するステップと、

管理者が管理者端末(300)を通じてファイル搬出を承認すれば、前記決裁情報DBを更新するステップと、

第1ユーザ端末(200)にUSBメモリを連結し、作業者がファイルダウンロードボタンをクリックすれば、前記クライアントプログラムは前記ファイル管理システム(100)に接続して、決裁情報とコピーの対象になるファイルについての情報を転送するステップと、

前記搬出情報管理サーバー(106)は、前記決裁が正常に行われたか否かを確認し、前記ファイルが保存された位置についての情報を前記クライアントプログラムに伝達するステップと、

前記ファイル管理サーバー(102)が前記ファイルに対する保安(ロック)を解除すれば、前記クライアントプログラムが前記ファイルをダウンロードして前記USBメモリに保存するステップと、

ファイル搬出が完了すれば、前記ファイル管理サーバー(102)は該当ファイルに対する保安(ロック)を再設定するステップと、

をさらに含むことを特徴とする請求項1に記載のウェブストレージシステムにおけるファイル管理方法。

【請求項 3】

10

20

30

40

50

前記クライアントプログラムがインストールされた第1ユーザ端末(200)から特定のファイルに対する電子メール搬出申し込みが前記ファイル管理システム(100)に受け付けられれば、搬出情報管理サーバー(106)が決裁申し込み情報を決裁情報DB(108)に保存するステップと、

管理者が管理者端末(300)を介してファイル搬出を承認すれば、前記搬出情報管理サーバー(106)が前記決裁情報DBを更新するステップと、

ファイル搬出が承認されれば、前記搬出情報管理サーバー(106)が前記第1ユーザ端末(200)に搬出対象になるファイルが保存された位置のURL情報をあるファイルリンク情報を伝達するステップと、

前記第1ユーザ端末(200)が前記ファイルリンク情報を添付した電子メールを作成して受信者に転送するステップと、

前記受信者が第2ユーザ端末(500)を利用してメールを受け付けた後、添付された前記ファイルリンク情報をクリックしてインターネット(400)を介して前記ファイル管理システム(100)に接続すれば、前記ファイル管理サーバー(102)は前記ファイルリンク情報に対応するファイルを、インターネット(400)を介して前記第2ユーザ端末(500)に転送するステップと、

をさらに含むことを特徴とする請求項1に記載のウェブストレージシステムにおけるファイル管理方法。

【請求項4】

前記ファイル管理政策で監視対象として設定される拡張子を有するファイルは、ワープロファイル、プレゼンテーションファイル、スプレッドシートファイル、ポストスクリプトファイル、圧縮ファイル、CADファイル、動画イメージファイル、静止画イメージファイル、オーディオファイルのうち何れか一つ以上であることを特徴とする、請求項1ないし請求項3のうち何れか1項に記載のウェブストレージシステムにおけるファイル管理方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ウェブストレージシステムにおけるファイル管理方法に関し、さらに詳細には、ウェブストレージシステムに接続してファイルを生成、変更、保存する場合に、ローカルPC(Personal Computer)から特定の種類のファイルをすべて削除し、ファイル管理システムにのみ保存させることによって、ローカルPCにはファイルに関するデータを保存させないウェブストレージシステムにおけるファイル管理方法に関する。

【背景技術】

【0002】

企業において大部分の業務がコンピュータによって行われているが、一般的に企業のコンピュータ環境は、サーバーに複数のクライアント端末が連結されて構成される。そして、クライアント端末で生成される電子ファイルはクライアント端末またはサーバーに保存される。

【0003】

近年、会社内のクライアント端末に保存された電子ファイルの流出事故が急増している。したがって、クライアント端末で生成及び編集される電子ファイルに対するファイル管理装置、方法及びシステムが必要である。

【0004】

図1は、従来技術によるファイル管理装置及びサーバーの全体的な構成を示す概念図である。

【0005】

図1に示すように、従来技術によるファイル管理方法は、サーバー110と連結された一つ以上の第1ないし第Nのファイル管理装置121、122、123で構成されるファ

10

20

30

40

50

イル管理装置 120 によって行われる。ファイル管理装置 120 は、ファイル管理方法を行なうために第 1 ないし第 N のクライアント端末 121-1, 122-1, 123-1 に設けられたクライアントファイル管理プログラムモジュール、あるいは、クライアントファイル管理プログラムモジュールを備えるクライアント端末を用いることができる。

【0006】

それぞれのファイル管理装置 120 には管理政策部が備えられ、管理政策部はサーバー 110 から所定の管理政策を受信する。管理政策は、所定の電子ファイルの拡張子情報（例えば、doc、hwp、xlsなど）と所定のキーワード情報を含む。

【0007】

クライアント端末は、サーバー 110 からクライアント端末のユーザによるサーバー 110 の保存スペースである管理スペースを提供される。

【0008】

クライアント端末では、ユーザの業務結果物である電子ファイルに対する保存イベントが発生し得るが、例えば、クライアント端末のユーザがワードを利用して文書を生成した後、C ドライブのマイドキュメント（my document）フォルダに保存する保存イベントを発生させることができる。

【0009】

ファイル管理装置 120 に備えられた判断部は、クライアント端末で生成または編集されて保存されるはずの作業ファイルが管理の対象である管理対象ファイルであるか否かを、管理政策を参照して判断する。

10

20

30

30

40

【0010】

例えば、管理政策が所定の拡張子情報として“doc、hwp、xls”情報を含む場合、保存イベントが発生した作業ファイルがワードファイル（すなわち、doc を拡張子として有するファイル）であるか否かから、作業ファイルが管理対象ファイルであるか否かを判断する。

【0011】

また、管理政策が所定のキーワード情報をとして“対外秘、会計、財務”情報を含む場合、保存イベントが発生した作業ファイルの内容に“対外秘、会計、財務”が含まれるか否かのフィルタリングを行い、そのフィルタリングの結果から該当作業ファイルが管理対象ファイルであるか否かを判断する。

【0012】

判断部の判断結果、クライアント端末で保存イベントが発生した作業ファイルが管理対象ファイルではない場合、クライアント端末のユーザが指定した保存スペースに作業ファイルが保存される。しかし、管理対象ファイルである場合には、管理対象ファイルがクライアント端末の保存スペースに保存されないように制御する。

【0013】

従来技術では、ローカル PC（クライアント端末）に特定の種類のファイルが保存されることを防止することによって、ファイルの流出、コピー、または盗用を防止することができたが、基本的にローカル PC で文書の生成及び変更作業が行われるときに発生する臨時的な保存過程は防止することはできなかったため、根本的にローカル PC にこれらのファイルに関するデータを一切残さないということはできなかった。

【0014】

また、ローカル PC で作業した資料を USB メモリにコピーして搬出しようとしたり、電子メールに添付して他のユーザに送信しようとしたりする場合に、どのような承認過程を経るかについての説明がないため、ファイルの伝達及び共有が難しいという問題点があった。

【先行技術文献】

【特許文献】

【0015】

【特許文献 1】韓国特許公開第 2009-0028005 号公報（ファイルの管理装置及

50

び方法)

【発明の概要】

【発明が解決しようとする課題】

【0016】

前述の問題点を解決するための本発明は、ウェブストレージサービスを提供するファイル管理システムに接続した状態で、ファイルの生成及び保存作業を行うユーザのユーザ端末に特定の種類のファイルが全く保存されないように、ファイルの保存スペースを監視し、ファイルを削除するウェブストレージシステムにおけるファイル管理方法を提供することを目的とする。

【0017】

また、本発明は、特定の種類のファイルは、ユーザ端末ではない、ファイル管理システムにのみ保存されるようにし、ファイル名、保存位置、属性についての情報を別途のデータとして生成して、DBMS (Database Management System) によって管理させるウェブストレージシステムにおけるファイル管理方法を提供することを目的とする。

【0018】

また、本発明は、ユーザがユーザ端末で特定のファイルを検索して開き、ファイルの内容を変更する作業を行う場合に、ファイル管理システムがファイルの開閉、変更に対するすべての権限を保有した状態で、作業の開始から終了(保存)までの過程を一つのトランザクションで処理することによって、ユーザ端末にはファイルに関するデータを一切残さないウェブストレージシステムにおけるファイル管理方法を提供することを目的とする。

【0019】

また、本発明は、ユーザがファイル管理システムに保存されたファイルをUSBメモリにコピーまたは電子メールに添付して他のユーザに送信しようとするとき、管理者の決裁を得て初めてファイルのコピーやファイルの添付を可能にするウェブストレージシステムにおけるファイル管理方法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】

【0020】

前述の課題を解決するためになされた本発明は、ネットワークに連結された第1ユーザ端末200が生成したファイルを保存するウェブストレージサービスを提供するファイル管理システム100が前記第1ユーザ端末200に特定の種類のファイルを保存しないように管理する方法であって、前記第1ユーザ端末200がLANまたはインターネット400を介して前記ファイル管理システム100に接続すれば、前記ファイル管理システム100に備えられたファイル管理サーバー102が前記第1ユーザ端末200にファイル管理クライアントプログラムを転送してインストールするステップと、前記クライアントプログラムが前記第1ユーザ端末200で行われるファイル管理政策を設定して保存した後、前記第1ユーザ端末200に対するファイル監視を開始するステップと、前記クライアントプログラムが前記第1ユーザ端末200を監視しつつ、前記ファイル管理政策で監視対象として設定された拡張子を有するファイルを発見すれば、前記クライアントプログラムが前記ファイルを前記ファイル管理システム100に転送した後、前記ファイルを前記第1ユーザ端末200から削除するステップと、前記ファイル管理サーバー102は、転送された前記ファイルをファイルDB104に保存し、前記ファイルを検索することができる情報をDBMSに記録するステップと、前記第1ユーザ端末200が前記ファイル管理システム100に接続して、保存された特定のファイルを要請すれば、前記ファイル管理サーバー102は、前記第1ユーザ端末200がネットワークファイルシステムドライバーを介して前記ファイルDB104に接続して、前記特定のファイルを開くように許容するステップと、前記第1ユーザ端末200が前記ファイルの内容または属性を変更して保存を要請すれば、前記ファイル管理サーバー102は、前記ファイルの修正及び保存を一つのトランザクションで処理して、前記修正された事項を前記ファイルDB104に保存するステップと、を含む。

10

20

30

40

50

【0021】

また、本発明は、前記クライアントプログラムがインストールされた第1ユーザ端末200から特定のファイルに対するUSBメモリ搬出申し込みが前記ファイル管理システム100に受け付けられれば、搬出情報管理サーバー106が決裁申し込み情報を決裁情報DB108に保存するステップと、管理者が管理者端末300を通じてファイル搬出を承認すれば、前記決裁情報DBを更新するステップと、第1ユーザ端末200にUSBメモリを連結し、作業者がファイルダウンロードボタンをクリックすれば、前記クライアントプログラムは前記ファイル管理システム100に接続して、決裁情報とコピーの対象になるファイルについての情報を転送するステップと、前記搬出情報管理サーバー106は、前記決裁が正常に行われたか否かを確認し、前記ファイルが保存された位置についての情報を前記クライアントプログラムに伝達するステップと、前記ファイル管理サーバー102が前記ファイルに対する保安を解除すれば、前記クライアントプログラムが前記ファイルをダウンロードして前記USBメモリに保存するステップと、ファイル搬出が完了すれば、前記ファイル管理サーバー102は該当ファイルに対する保安を再設定するステップと、をさらに含んでいてもよい。

10

【0022】

あるいは、本発明は、前記クライアントプログラムがインストールされた第1ユーザ端末200から特定のファイルに対する電子メール搬出申し込みが前記ファイル管理システム100に受け付けられれば、搬出情報管理サーバー106が決裁申し込み情報を決裁情報DB108に保存するステップと、管理者が管理者端末300を介してファイル搬出を承認すれば、前記搬出情報管理サーバー106が前記決裁情報DBを更新するステップと、ファイル搬出が承認されれば、前記搬出情報管理サーバー106が前記第1ユーザ端末200に搬出対象になるファイルが保存された位置のURL情報を前記ファイルリンク情報を伝達するステップと、前記第1ユーザ端末200が前記ファイルリンク情報を添付した電子メールを作成して受信者に転送するステップと、前記受信者が第2ユーザ端末500を利用してメールを受け付けた後、添付された前記ファイルリンク情報をクリックしてインターネット400を介して前記ファイル管理システム100に接続すれば、前記ファイル管理サーバー102は前記ファイルリンク情報に対応するファイルを、インターネット400を介して前記第2ユーザ端末500に転送するステップと、をさらに含むように構成してもよい。

20

【0023】

さらに、本発明において、前記ファイル管理政策で監視対象として設定される拡張子を有するファイルは、ワープロファイル、プレゼンテーションファイル、スプレッドシートファイル、ポストスクリプトファイル、圧縮ファイル、CADファイル、動画イメージファイル、静止画イメージファイル、オーディオファイルのうち何れか一つ以上であることを特徴とする。

30

【発明の効果】**【0024】**

本発明によれば、ウェブストレージシステムを利用してファイルの生成及び保存を行うとき、遠隔地のユーザ端末には保安上の問題になり得るファイルに関するデータが一切残っていないため、ファイルの流出問題を解消することができる。

40

【0025】

また、本発明によれば、ウェブストレージシステムに保存されたファイルを他のユーザに転送するとき、決裁権限を有する管理者の承認を得た後にファイルのコピーやファイルの添付を可能にすることによってコンピュータファイルの流出を防止することができ、保安事故が発生したとき、責任を明らかにすることができます。

【図面の簡単な説明】**【0026】**

【図1】従来技術によるファイル管理装置及びサーバーの全体的な構成を示す概念図である。

50

【図2】本発明の実施形態によるファイル管理システムの連結状態を示すブロック図である。

【図3】ユーザ端末でのファイル管理方法の動作過程を示すフローチャートである。

【図4】USBメモリによるファイルのコピー過程を示すフローチャートである。

【図5】電子メールによるファイルの添付過程を示すフローチャートである。

【発明を実施するための形態】

【0027】

以下、図面を参照して本発明の実施形態によるウェブストレージシステムにおけるファイル管理方法（以下、ファイル管理方法と称す）を説明する。

【0028】

図2は、本発明の実施形態によるファイル管理システムの連結状態を示すブロック図である。

【0029】

本発明のファイル管理方法を具現化するためには、LANまたはインターネット400などで相互に連結されたファイル管理システム100、ユーザ端末200、500、及びファイル管理システム100と連結された管理者端末300が必要である。

【0030】

ファイル管理システム100は、ネットワークに連結された端末で生成されたファイルを保存し、保存されたファイルを正当なユーザに提供するウェブストレージサービスを提供する。ユーザは、ネットワークに連結さえすれば自身が生成したファイルをファイル管理システム100に保存することが可能であり、いつでも所望のファイルを検索して作業を行うことができる。

【0031】

ファイル管理システム100は、特定の種類のファイルをユーザ端末200、500に保存させずにファイル管理システム100にのみ残るように監視する。ファイル管理システム100は、ユーザがユーザ端末200、500で作業して生成したファイルを受けて保存する。ユーザがそのファイルを再要請する場合、ファイルを開いてユーザ端末200、500に転送することによってファイルの変更作業を可能にする。ユーザがファイル作業を終了すれば、ユーザ端末200、500にファイルに関するデータを一切残さず、変更されたファイルをファイル管理システム100に保存する。

【0032】

ファイル管理システム100には、ユーザ端末200、500で生成及び保存されるファイルを監視して制御するファイル管理サーバー102と、所定の種類のファイルを保存するファイルDB104とが備えられる。

【0033】

そして、ファイルDB104に保存されたファイルを他のユーザに送信するとき、決裁情報を確認してファイル搬出を承認する搬出情報管理サーバー106と、管理者が承認した内訳を保存する決裁情報DB108とをさらに備える。

【0034】

ファイル管理サーバー102は、ユーザ端末200、500にファイル管理クライアントプログラムをインストールし、ユーザ端末200、500との通信を通じて特定のファイルに対する保存作業を制御する。

【0035】

ファイル管理クライアントプログラムは、それぞれのユーザ端末200、500にインストールされ、端末上で行われるファイルの生成、変更、保存作業を監視しつつ、特定の種類のファイルが発見されれば、設定された内容によってファイルの転送、削除、保存作業を行う。

【0036】

本発明では、第1ユーザ端末200にファイル管理クライアントプログラムがインストールされ、このプログラムが第1ユーザ端末200で実行されつつ特定のファイルの監視

10

20

30

40

50

、転送、削除動作を行う。

【0037】

作業者は、第1ユーザ端末200を利用して各種の文書やワークシート、マルチメディアファイルを生成、変更、保存する。このとき、特定の種類のファイルは、保安上の理由により第1ユーザ端末200に保存しないことが好ましい。機密や対外秘として取り扱われるべきファイルが作業者の端末に残らないように、クライアントプログラムが監視及び管理を行う。

【0038】

第1ユーザ端末200に残さないファイルの種類は多様な基準によって設定可能であるが、本発明では、一例として、ファイル名の拡張子を基準にする。すなわち、マイクロソフト社のワード文書を示す‘*.doc’を拡張子として有するファイルをすべて削除するか、動画データを示す‘*.mpeg’を拡張子として有するファイルはすべてファイル管理システム100に転送する方法を選択することができる。

【0039】

本発明のクライアントプログラムが管理可能なファイルの拡張子は多様な種類の拡張子を含む。ワープロファイル(doc、hwpなど)、プレゼンテーションファイル(pptなど)、スプレッドシートファイル(xlsなど)、ポストスクリプトファイル(pdfなど)、圧縮ファイル(zip、alzなど)、CADファイル(cadなど)、動画イメージファイル(asf、avi、mpegなど)、静止画イメージファイル(bmp、jpeg、phg、pstなど)、オーディオファイル(mp3、wmvなど)が代表的である。

【0040】

管理対象になるファイルの拡張子は、管理者の選択によって多様に含めることができ、クライアントプログラムの設定変更を通じて削除や変更が可能である。

【0041】

以下、図3を参照して具体的なファイル管理方法を説明する。

【0042】

図3は、ユーザ端末でのファイル管理方法の動作過程を示すフローチャートである。

【0043】

まず、ユーザ(作業者)の第1ユーザ端末200がLANまたはインターネット400を介してファイル管理システム100に接続する(S102)。一般的には、会社内に設けられたPCなどをを利用して作業が行われ、会社内の保安のために本発明が適用される場合が多いと思われる。第1ユーザ端末200は、主にLANを介してファイル管理システム100に接続する。しかし、例えば、在宅勤務または外部出張中に行われる作業に対しても管理するためには、第1ユーザ端末200がインターネット400を利用して接続可能である必要がある。

【0044】

第1ユーザ端末200にファイル管理クライアントプログラムがインストールされている場合には、ファイル作業及び監視が直ちに行われるが、プログラムがインストールされていない場合には、プログラムを先にインストールしなければならない(S104)。ファイル管理サーバー102は、ファイル管理システム100に接続した端末にプログラムがインストールされているか否かを確認して、インストール過程が行われるように制御する。

【0045】

ファイル管理クライアントプログラムは、第1ユーザ端末200で行われるファイル管理政策を設定して保存する(S106)。クライアントプログラムは、第1ユーザ端末200から削除されるべきファイルの種類を、拡張子を基準にして設定する。監視対象ファイルの種類は、第1ユーザ端末200のユーザではない、ファイル管理システム100によって選択されることが好ましい。すなわち、削除対象になるファイルの拡張子は、ファイル管理サーバー102が定め、第1ユーザ端末200のユーザは、特定の種類のファイル

10

20

30

40

50

ルに対して管理対象になるように追加する作業のみを可能にする。

【0046】

ファイルの監視及び削除は拡張子を基準にするため、実際は他の形式のファイルであるが、拡張子が同一である場合（例えば、ハングル文書のファイルに‘doc’拡張子を付けて保存した場合）にもファイルの削除は行われる。

【0047】

ファイル管理クライアントプログラムがインストールされ、監視政策の設定が完了すれば、第1ユーザ端末200に対するクライアントプログラムのファイル監視が開始される（S108）。

【0048】

ファイルの監視は、管理者の設定によって多様な方法によって行われる。すなわち、第1ユーザ端末200全体の保存スペースを検索して特定ファイルを検索する方法が一般的であるが、特定のフォルダのみを検索するように指定することも可能である。また、保存された既存のファイルすべてを対象として検索することも可能であるが、新たに生成または保存されるファイルに対してのみ監視を行うことも可能である。

【0049】

クライアントプログラムは、第1ユーザ端末200で行われるファイルの生成及び保存作業を監視しつつ、所定の種類の監視対象ファイル（特定の拡張子を有するファイル）が検索されれば、それをファイル管理システム100に転送する（S110、S112）。転送されたファイルはファイルDB104に保存され、ファイル管理サーバー102は該当ファイルを検索することができる情報（ファイルの位置、ファイル名、作成時間、ファイルのサイズなど）を別途のDBMSで管理する。

【0050】

もし、削除対象に相当するファイルが検索された場合、該当ファイルが他のプログラムによって使用中であれば、そのプログラムの作業が終了し、保存が終了した後にファイルを転送することが好ましい。

【0051】

最後に、クライアントプログラムは、第1ユーザ端末200から該当ファイルを永久的に削除する（S114）。ファイルの削除は、ファイル管理サーバー102への転送と同時にを行うことも可能である。

【0052】

ユーザがファイル管理システム100に転送されたファイル（監視政策の対象になる種類のファイル）を再検索して作業することを希望する場合には、ファイル管理システム100に接続してユーザの認証を受けた後、ファイルDB104に保存された該当ファイルを検索して作業を行う。従来技術では、ファイル作業が完了すれば、ローカル端末にファイルを一旦保存した後、中央サーバーに送るが、その過程でローカル端末に保存されたファイルが流出される恐れがある。

【0053】

本発明では、このような‘ファイルの開き・修正・閉じ’過程をネットワークファイルシステムと同様に、一つのトランザクションで処理して、第1ユーザ端末200にファイル関するデータが一切保存されないようにする。

【0054】

第1ユーザ端末200がファイル管理システム100に接続して特定のファイルを要請すれば、トランザクションが開始され、接続したユーザの権限を確認した後、ファイルが保存された位置についての情報を呼び出す。呼び出された情報に基づいてファイルを検索して第1ユーザ端末200に提供するが、第1ユーザ端末200のユーザはネットワークファイルシステムドライバーを介してファイルDB104に直接アクセスする。ユーザが作業を終えながらファイルの閉じを選択すれば、ファイル管理サーバー102のDBMSは修正された事項を直接ファイルDB104に記録しつつ保存する。ファイルを閉じると同時に、第1ユーザ端末200のメモリ上に臨時にアップロードされていたデータはすべ

10

20

30

40

50

て削除される。

【0055】

このようなすべての過程は、一つのトランザクションで処理され、ファイルの内容変更についての事項はDBMSに記録される。

【0056】

クライアントプログラムによってファイル管理システム100に保存されたファイルはユーザによって呼び出されて使用されるが、他人に伝達するためには伝達媒体を利用せねばならない。本発明ではUSBメモリを利用した保存と電子メールを利用した伝達方法を例示する。これらを以下に説明する。

【0057】

図4は、USBメモリによるファイルのコピー過程を示すフローチャートである。

【0058】

USBメモリにファイルをコピーして外部に搬出するためには、ユーザ端末にインストールされているファイル管理クライアントプログラムにより、搬出についての決裁情報を認識し、連結されたUSBメモリが認証された媒体であるか否かを確認せねばならない。本発明では、ファイル管理クライアントプログラムがインストールされた第1ユーザ端末200に基づいて説明する。

【0059】

まず、ファイルをコピーして搬出しようとする作業者がユーザ端末200でクライアントプログラムを利用してUSB搬出申し込みを行う(S202)。

【0060】

搬出申し込みがファイル管理システム100に受け付けられれば、搬出情報管理サーバー106は生成された承認インデックスをキー(key)として有する決裁情報テーブルにファイルのインデックスなどのその他の決裁申し込み情報を記録し、それを決裁情報DB108に保存する(S204)。

【0061】

ファイル搬出申し込み情報は、ファイル管理システム100によって管理者端末300に転送されて、決裁待機状態になる(S206)。

【0062】

管理者が管理者端末300を介してファイル搬出を承認すれば、決裁情報DBのテーブルに承認如何情報を更新する(S208)。

【0063】

ファイルの搬出が承認されれば、搬出情報管理サーバー106は、ユーザ端末200にファイル搬出申し込みに対する決裁が完了したことを通知する(S210)。このような通知は、クライアントプログラムを通じてユーザに告知することができる。

【0064】

作業者がファイルをコピーするUSBメモリをユーザ端末200に連結すれば、連結された媒体の識別番号と、保安プログラムがインストールされているか否かを確認する(S212)。USBメモリに対する識別番号と保安プログラムを確認することは、承認された媒体のみを使用可能にするためのことであり、状況によっては未確認媒体を使用するよう承認することも可能である。

【0065】

作業者は、ユーザ端末200でファイルのダウンロード及びUSBメモリ保存ボタンをクリックする(S214)。クライアントプログラムは、ファイルダウンロード確認ボタンを別途の入力ウィンドウに具現化することができる。

【0066】

クライアントプログラムは、ファイル管理システム100に接続して、承認が行われた決裁情報と、その他のコピーの対象になるファイルについての情報を転送する(S216)。搬出情報管理サーバー106は、転送された決裁情報を決裁情報DB108に保存された決裁情報テーブルと比較して、正常に決裁承認が行われたか否かを確認する。そして

10

20

30

40

50

、搬出情報管理サーバー106は、該当ファイルが保存されている位置についての情報(ファイルDBの位置など)をクライアントプログラムに伝達する。

【0067】

クライアントプログラムは、Active Xを通じてウェブから情報を受け、Active Xによって実行されたプローカープロセス(例えば、USB Downloader.exe)は、Active Xが有する情報を受ける。

【0068】

プローカープロセスは、作業者がダウンロード確認ボタンを押す瞬間、ファイル管理システム100とpipe通信を行い、ファイル管理サーバー102は、瞬時にプローカープロセスがダウンロードを行うことができるよう、該当ファイルに対する保安(ロック)を解除する(S218)。

10

【0069】

クライアントプログラムは、ファイルDB104で該当ファイルを検索してダウンロードした後、連結されたUSBメモリに保存する(S220)。

【0070】

ファイルの搬出が完了すれば、プローカープロセスは、ファイルの保存が完了したことをファイル管理サーバー102に通知し、ファイル管理サーバー102は、該当ファイルに対する保安(ロック)を再設定することによって、ファイルの搬出過程が完了する(S222)。

20

【0071】

一方、図5は、電子メールによるファイルの添付過程を示すフローチャートである。

【0072】

電子メールによるファイルの転送は、クライアントプログラムがインストールされた第1ユーザ端末200と、プログラムがインストールされていない第2ユーザ端末500との間で行われる。

【0073】

まず、作業者が第1ユーザ端末200でメールによるファイルの搬出を搬出情報管理サーバー106に申し込む(S302)。メールによる搬出申し込みもクライアントプログラムを通じて行われる。

30

【0074】

搬出情報管理サーバー106は、決裁情報DB108に搬出申し込み情報を記録し、申し込み内容を管理者端末300に転送して決裁を要請する(S304、S306)。

【0075】

管理者が管理者端末300を介して電子メールによるファイルの搬出を承認すれば、決裁情報DBのテーブルに承認如何情報を更新する(S308)。

【0076】

ファイル搬出の申し込みと決裁情報の記録、管理者の決裁及び決裁情報の更新などの過程は、USBメモリの搬出過程と同一である。

【0077】

電子メールによるファイルの搬出が承認されれば、搬出情報管理サーバー106は、第1ユーザ端末200にファイル搬出の申し込みに対する決裁が完了したことを通知しつつ、決裁情報とファイルリンク情報を伝達する(S310)。

40

【0078】

ファイルリンク情報は、ファイルが保存された位置のURL(Uniform Resource Locator)情報であって、メールを受信したユーザがインターネット400を介して該当位置のサーバーに接続して直接ファイルをダウンロード可能にするための情報である。電子メールに大容量またはマルチメディアファイルのリンク情報を添付して、受信者が直接接続してダウンロード可能にする技術は、出願人によって既に公開された技術であるため、その詳細な説明を省略する。

【0079】

50

第1ユーザ端末200の作業者は、電子メールを作成し、メールに決裁情報及びファイルリンク情報を添付した後、メールを受信者に転送する(S312、S314、S316)。

【0080】

第1ユーザ端末200の作業者が送ったメールは、受信者(第2ユーザ端末500のユーザ)に転送され、受信者は決裁情報またはリンク情報をクリックすることによってファイル管理システム100の搬出情報管理サーバー106に接続する(S318)。第2ユーザ端末500は、インターネット400を介して搬出情報管理サーバー106に接続する。

【0081】

搬出情報管理サーバー106は、第2ユーザ端末500から転送された決裁情報を分析して正当な決裁過程を経て、搬出承認が行われたファイルであるか否かを確認する(S320)。

【0082】

決裁情報が確認されれば、ファイル管理システム100は、第2ユーザ端末500がファイルDB104に接続するように許可し、ファイル管理サーバー102は、ファイルリンク情報に対応するファイルを、インターネット400を介して第2ユーザ端末500に転送する(S322)。転送されたファイルは、第2ユーザ端末500の保存スペースに永久的に保存される。

【0083】

以上、添付図面を参照して本発明の好ましい実施形態を説明したが、前述の本発明の技術的構成は、当業者が本発明のその技術的思想や必須の特徴を変更せずに他の具体的な形態に実施され得るということを理解できるであろう。したがって、前述の実施形態は、すべての面において例示的なものであり、限定的なものではないものとして理解されるべきであり、本発明の範囲は、前記詳細な説明よりは、後述する特許請求の範囲によって示され、特許請求の範囲の意味及び範囲、そしてその等価概念から導出されるすべての変更または変形された形態が本発明の範囲に含まれると解釈されなければならない。

【符号の説明】

【0084】

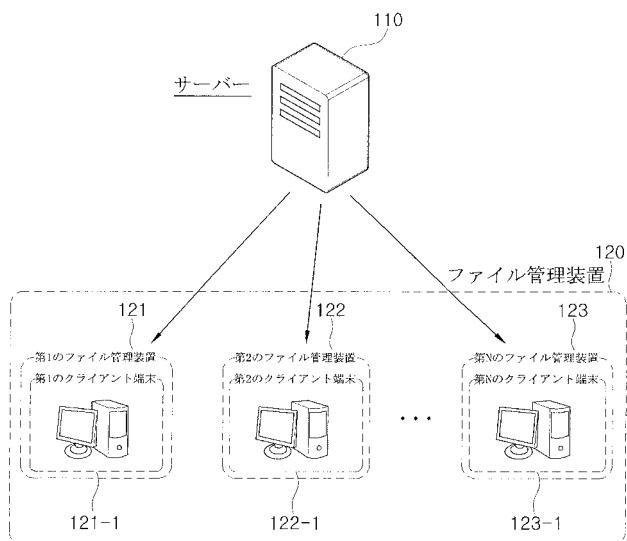
100 ファイル管理システム
102 ファイル管理サーバー
104 ファイルDB
106 搬出情報管理サーバー
108 決裁情報DB
200 第1ユーザ端末
300 管理者端末
400 インターネット
500 第2ユーザ端末

10

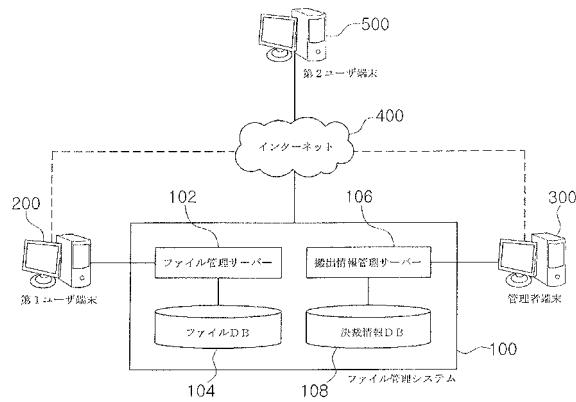
20

30

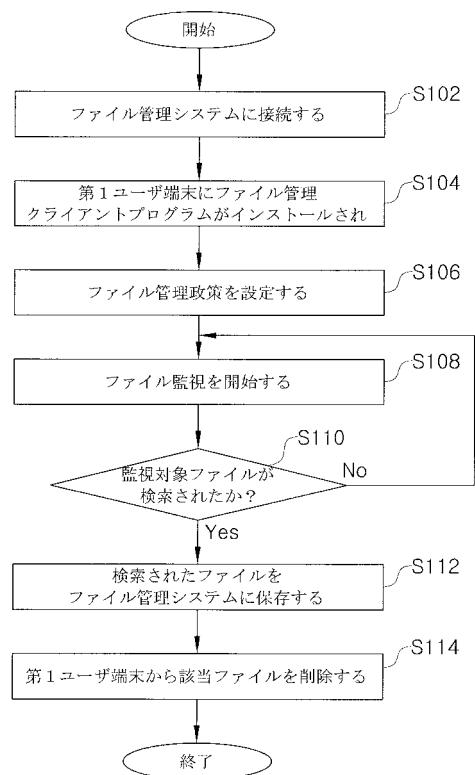
【図1】



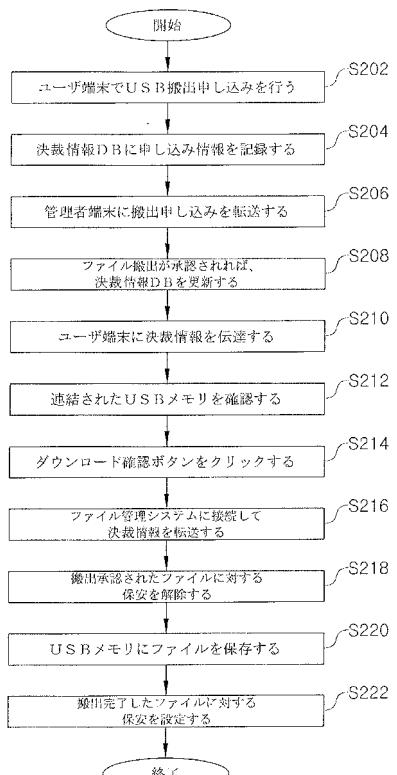
【図2】



【図3】



【図4】



【図5】

