

明 細 書

発明の名称： ファイルの秘匿分散システム及び秘匿分散方法

技術分野

[0001] 本発明は、ファイルの秘匿分散システム及び秘匿分散方法に関するものであり、より詳細には、記録媒体に記録されているファイルを暗号化し、安全に管理、監視、有効化・無効化するためのファイルの秘匿分散システム及び秘匿分散方法に関するものである。

背景技術

[0002] 従来から、インターネット等の公衆網（以下単に「インターネット」とする。）を通じてファイルなどのデータを送信する場合、データを暗号化し、Eメールに添付して送信したり、VPN（Virtual Private Network）を使ってデータを送信したりすることが行われている。しかし、それらの方法の場合は通信経路上でデータが盗聴され、また、鍵情報やパスワードが解読された場合には、データが復号されて漏洩してしまう。

[0003] このようなセキュリティの弱点に対処する方法として、秘密分散法が知られている。秘密分散法は、秘密にすべきデータを複数の断片データに分割し、これらの断片データを全て又は一定数以上集めない限り、元データを復元できないようにする技術である。

[0004] 秘密分散法に関するものとして、特開2008-139996号公報（特許文献1）に、情報端末が秘密分散技術を用いて複数のシェアファイルを作成し、シェアファイルの1つを携帯通信端末又は管理サーバに保存するシステムが開示されている。

[0005] 例えば、秘密分散法を適用したアプリケーションを用いれば、送信者は、送信ファイルを複数の断片データに分割することができる。また、送信者は、各断片ファイルをそれぞれ別のEメールに添付して送信することができる。受信者は、複数のEメールに添付された断片ファイルを同じフォルダに集めて、いずれかの実行ファイル形式の断片ファイルを実行することで、元の

送信ファイルを得ることができる。

[0006] しかしながら、上記のようなファイル送信の仕方は、ユーザの手間が増えるだけでなく、同じメールサーバに断片ファイルが置かれるために安全性が低下してしまう。ユーザは、各断片ファイルを添付するEメールの宛先を異ならせたり、各断片ファイルをそれぞれ別の送信方法で送信したりすることはできるが、このような作業は非常に手間がかかり、利便性を損なう。また、送信者と受信者の間で、ファイルの復元方法に関する連絡のミスが発生し易くなり、受信者がファイルの復元に失敗するおそれもある。

[0007] かかる事情に鑑み、特許第6322763号公報（特許文献2）に記載の発明は、安全性及び利便性を向上させたデータ転送システムにおけるデータ転送方法を提唱している。それは、送信者システムと、受信者システムと、前記送信者システムと前記受信者システムとの間のネットワークを介したデータ転送を管理する管理システムとを備えるものである。

[0008] この方法は、以下のステップからなるものである。

- ・送信者システムが、秘密分散法を利用して元データを複数の断片データに分割し、各断片データにつきそれぞれ送信経路を選択し、各断片データを、選択したそれぞれの送信経路に送信し、各送信経路に関する情報を管理システムに送信する。

- ・管理システムが、送信者システムから各送信経路に関する情報を受信し、受信した各送信経路に関する情報を受信者システムに送信する。

- ・受信者システムが、各送信経路に関する情報を管理システムから受信し、受信した各送信経路に関する情報に基づいて各送信経路から各断片データを受信し、秘密分散法を利用して受信した各断片データを元データに復元する。

先行技術文献

特許文献

[0009] 特許文献1：特開2008-139996号公報

特許文献2：特許第6322763号公報

発明の概要

発明が解決しようとする課題

[0010] 上記構成の特許文献2に記載の発明によれば、安全性及び利便性を向上したデータ転送の仕組みを提供することができるとされている。しかし、その発明に係る方法は、端末（送信者システム）にダウンロードしたアプリケーションにより、インターネット等に情報伝達して端末内のファイルを削除するというものであるため、ネットワークに接続されていない環境やバックアップ等によってファイルが不定の場所に移動されたりしたような場合に、削除データの復元を有効に行うことができないという問題が生ずる。

[0011] 本発明はこのような問題がなく、ファイルの復元を複雑化することにより十分な秘匿性を保持でき、また、ハードウェア障害発生時や災害時等において一部のファイルが消失しても、残りのファイルを用いて原本ファイルの復元が可能で、事業継続性を確保し得るファイルの秘匿分散システム及び方法を提供することを課題とする。

課題を解決するための手段

[0012] 上記課題を解決するための請求項1に記載の発明は、

ネットワークを介して接続された発信ユーザ端末と受信ユーザ端末間における暗号化ファイルの送受信を、管理サーバを介して秘匿状態にて実行させるためのシステムであって、

前記発信ユーザ端末は、原本ファイルを暗号化した上で複数の分割ファイルに断片化すると共に、前記原本ファイルの復元に必要な分割ファイル数の閾値を設定する機能と、前記分割ファイルを複数結合して成る結合ファイルを複数作成し、前記結合ファイルを開封するために必要な復元情報を前記結合ファイルに付し、前記復元情報を付した結合ファイルを複数のオンラインストレージに分散して保存させる機能とを備え、

前記管理サーバは、前記発信ユーザ端末から送られる前記復元情報を保持・管理し、アクセス権を有する前記受信ユーザ端末から前記結合ファイルの前記復元情報の照会を受けることにより前記受信ユーザ端末に前記復元情報

を送信する機能を備え、

前記受信ユーザ端末は、前記管理サーバから受信した前記復元情報を用いて、前記オンラインストレージから取得した前記結合ファイルを開封でき、開封して得られる前記分割ファイルの数が前記復元情報に含まれる前記分割ファイルの閾値以上の場合に、前記原本ファイルの復元が可能となることを特徴とするファイルの秘匿分散システムである。

[0013] 一実施形態においては、前記発信ユーザ端末及び受信ユーザ端末は、通信部と、ファイルを暗号化・復号化するための暗号化・復号化部と、暗号化された原本ファイルを分割し、その分割ファイルを複数結合して成る結合ファイルを複数作成し、前記結合ファイルを前記複数のオンラインストレージに分散する際に各結合ファイルの配置情報を管理するファイル情報管理部と、前記結合ファイルを前記複数のオンラインストレージに分散させる分散ファイル入出力部とを含み、

前記管理サーバは、ユーザインターフェース部と、通信部と、自身の端末に本システムで使用する各種パラメータの保存、読み出し、管理を行うユーザ管理部と、前記発信ユーザ端末及び受信ユーザ端末の通信部を通してデータの送受信を行い、そのデータを基に前記結合ファイルの開封をコントロールする開封管理部と、前記結合ファイルの作成・開封時に前記開封管理部に前記結合ファイルの作成・開封情報を提供し、また、前記発信ユーザ端末及び受信ユーザ端末で設定された情報を管理するファイル情報管理部と、各種データを内部動作のデータから生成する機能を提供する管理パラメータ生成部と、動作のログを生成してデータベースに保存する機能を提供するログ生成部とを含むことを特徴とする。

[0014] 一実施形態においては、前記原本ファイルの復元に必要な前記分割ファイルの数の閾値が予め前記発信ユーザ端末のファイル情報管理部において設定され、前記管理サーバのファイル情報管理部において管理される。また、前記管理サーバは、インターネット未接続時に開封を行う場合に用いる、時間制限されているワンタイムパスワードを作成するワンタイムパスワード生成

部を含み、前記発信ユーザ端末及び受信ユーザ端末は、このワнтаイムパスワードを解析するためのワнтаイムパスワード解析部を含む。

[0015] 一実施形態においては、前記結合ファイルに付加される復元情報には、アクセス権と開封可能期限と前記分割ファイルの閾値が含まれる。また、前記結合ファイルを開封するためのアプリケーションは、自己解凍型、ディスク構成閲覧ソフト型、仮想ディスクマウント型のいずれかとされる。

[0016] 上記課題を解決するための請求項 7 に記載の発明は、

ネットワークを介して接続された発信ユーザ端末と受信ユーザ端末間における暗号化ファイルの送受信を、管理サーバを介して秘匿状態にて実行させるための方法であって、

前記発信ユーザ端末に、原本ファイルを暗号化した上で複数の分割ファイルに断片化すると共に、前記原本ファイルの復元に必要な分割ファイル数の閾値を設定する機能と、前記分割ファイルを複数結合して成る結合ファイルを複数作成し、前記結合ファイルを開封するための復元情報を前記結合ファイルに付し、前記復元情報を付した結合ファイルを複数のオンラインストレージに分散して保存させる機能を具備させ、

前記管理サーバに、前記発信ユーザ端末から送られる前記復元情報を保持・管理し、アクセス権を有する前記受信ユーザ端末から前記結合ファイルの前記復元情報の照会を受けた場合に前記受信ユーザ端末に前記復元情報を送信する機能を具備させ、

前記受信ユーザ端末が、前記管理サーバから受信した前記復元情報を用いて、前記オンラインストレージから取得した前記結合ファイルを開封してそれに含まれる前記分割ファイルを取り出し、前記閾値以上の数の前記分割ファイルから前記原本ファイルを復元することを可能にしたことを特徴とするファイルの秘匿分散方法である。

[0017] また、上記課題を解決するための請求項 8 に記載の発明は、

ネットワークを介して接続された発信ユーザ端末と受信ユーザ端末間における暗号化ファイルの送受信を、管理サーバを介して秘匿状態にて実行させ

るための方法であって、

前記発信ユーザ端末において、原本ファイルを暗号化した上で複数の分割ファイルに断片化すると共に、前記原本ファイルの復元に必要な分割ファイル数の閾値を設定する原本ファイル暗号化・分割ステップと、

前記発信ユーザ端末において、前記分割ファイルを複数結合して成る結合ファイルを複数作成する結合ファイル作成ステップと、

前記発信ユーザ端末において、前記結合ファイルの開封に必要な復元情報を作成して前記結合ファイルに付する復元情報作成ステップと、

前記発信ユーザ端末において、前記復元情報を付した前記複数の結合ファイルをそれぞれ異なるオンラインストレージに分散して保存するオンラインストレージ分散・保存ステップと、

前記管理サーバにおいて、前記発信ユーザ端末から送られる前記復元情報を保持・管理する復元情報保存ステップとを含み、

アクセス権を有する前記受信ユーザ端末から前記管理サーバに対して前記結合ファイルの前記復元情報の照会があった場合に、前記管理サーバから前記受信ユーザ端末に前記復元情報が送信され、前記受信ユーザ端末において前記復元情報を用い、前記オンラインストレージから取得した前記結合ファイルを開封して前記分割ファイルを取り出し、前記閾値以上の数の前記分割ファイルから原本ファイルを復元することを可能にしたことを特徴とするファイルの秘匿分散方法である。

[0018] 上記ファイルの秘匿分散方法における一実施形態においては、前記結合ファイルに付加される復元情報としてアクセス権と開封可能期限と分割ファイルの閾値が含まれ、また、前記結合ファイルを開封するためのアプリケーションは、自己解凍型、ディスク構成閲覧ソフト型、仮想ディスクマウント型のいずれかとされる。そして、前記結合ファイルと前記開封用アプリケーションとの間に可変長のギャップが埋め込まれる。

発明の効果

[0019] 本発明に係るファイルの秘匿分散システム及び方法は上記のとおりである

ので、ファイルの復元が複雑化されているために十分な秘匿性を保持でき、また、結合ファイルが秘匿状態にてオンラインストレージに分散保存されているため、ハードウェア障害発生時や災害時等において一部のファイルが消失しても、残りのファイルを用いて原本ファイルの復元が可能であるので、事業継続性を確保できるという効果がある。

図面の簡単な説明

[0020] [図1]本発明に係るファイルの秘匿分散システムの概略構成図である。

[図2]本発明に係るファイルの秘匿分散システムの概略ブロック図である。

[図3]本発明に係るファイルの秘匿分散方法における処理の流れを示すフロー図である。

[図4]本発明に係るファイルの秘匿分散方法における、原本ファイル暗号化・分割ステップからオンラインストレージ分散・保存ステップまでの処理を説明するための図である。

[図5]本発明に係るファイルの秘匿分散方法における、原本ファイルの復元方法を説明するための図である。

発明を実施するための形態

[0021] 本発明を実施するための形態について、図面を参照しつつより詳細に説明する。図1に示されるように、本発明に係るファイルの秘匿分散システムは、ネットワーク1を介して、暗号化されたファイルの送受信を行う発信ユーザ端末2及び受信ユーザ端末3と、送受信される暗号化ファイルを保存する複数のオンラインストレージ4と、管理サーバ5によって構成される。管理サーバ5は、前記暗号化ファイルの復元情報を保持すると共に、前記暗号化ファイルに対するアクセス権及び開封可能期限を設定・編集するためのユーザインターフェースを提供し、設定された前記暗号化ファイルの復元情報を保持・管理する。

[0022] 受信ユーザ端末3は、発信ユーザ端末2の管理者によって指定され、アクセス権を付与される1又は複数のユーザ（以下「公開ユーザ」とする）が扱う端末である。公開ユーザは、個人の場合とグループの場合とがある。

- [0023] 発信ユーザ端末2及び受信ユーザ端末3は、図2に示されるように、後述する管理サーバ5との間で通信を行うための通信部11と、ファイルを暗号化するためのエンコード部12と、ファイルを復号化するためのデコード部13と、ファイル情報管理部14と、分散ファイル入出力部15の各モジュールを構成させるための、実行形式のクライアントアプリケーションをインストールしたものである。ファイル情報管理部14は、暗号化された原本ファイルを分割して断片化した分割ファイルを複数結合して成る結合ファイルを複数生成し、また、結合ファイルを分散する際に各結合ファイルの配置情報やチェック・サム等を管理する。分散ファイル入出力部15は、ファイル情報管理部14から供給された結合ファイルを複数のオンラインストレージ4に分散させる。
- [0024] このクライアントアプリケーションは更に、各アプリケーションで使用するモジュールの正否のチェックを行うモジュール管理部18と、各アプリケーションにおいて必要とされる形式のデータを分散ファイル入出力部15から取得するファイル集配信部19と、ファイル集配信部19で取得したデータの整合性を検証するファイル検証部20とから成るライブラリ17を構成する。このライブラリ17は、クライアントアプリケーションを構成する各モジュールで各アプリケーションが呼び出す機能の集合として作成されるものである。
- [0025] 管理サーバ5は、クライアントアプリケーション（発信ユーザ端末2）から送られてくるファイル情報を登録し、指定された公開ユーザにのみ登録情報を公開するユーザ認証機能を果たすものである。管理サーバ5は、ユーザがアクセス権や開封可能期限等の設定・変更を行うための設定変更用画面や、開封記録等の閲覧をするための表示画面を提供するユーザインターフェース部21と、発信ユーザ端末2及び受信ユーザ端末3の通信部11との間で通信を行うための通信部22と、自身の端末に本システムで使用する各種パラメータを保存し、読み出し、また、管理を行うユーザ管理部23を有する。ここにおけるパラメータには、管理サーバ5にアクセスするID、端末の

MACアドレス、公開ユーザ情報、グループ化したユーザの情報等が含まれる。

[0026] 管理サーバ5はまた、発信ユーザ端末2及び受信ユーザ端末3の通信部11を通してデータの送受信を行い、そのデータを基にファイルの開封をコントロールする開封管理部24と、ファイルの作成・開封時に開封管理部24にファイルの作成・開封情報を提供し、また、発信ユーザ端末2及び受信ユーザ端末3で設定された情報を管理するファイル情報管理部25を含む。そして更に、各種データを生成するジェネレータである管理パラメータ生成部26と、動作のログを生成してデータベース29に保存する機能を提供するログ生成部27とを含んで構成される。

[0027] 開封管理部24は、ファイル情報管理部25のデータを使用して結合ファイルを分割することが可能な場合には当該結合ファイルを分割し、閾値を満たした結合ファイルであるかどうかの確認を行う。また、管理パラメータ生成部26は、データを分割するために割り当てられるギャップのバイト数（後述するように、結合ファイルと復元用プログラムの間に可変長のギャップが埋め込まれる。）や閾値等、ファイルを復元するための内部情報を生成する。更に、ファイル情報管理部25は、分割された個々のファイルとそれを集約した結合ファイルの情報で、分割ファイル数、結合ファイル数、保存するストレージの情報、その他生成されるファイルのすべての情報を開封管理部24に送信する。

[0028] 本システムは、インターネット接続を前提としているが、インターネット未接続時においても開封可能にすることが好ましい。そのために、管理サーバ5は、インターネット未接続時に開封を行う場合に用いる、時間制限されているワンタイムパスワードを作成するワンタイムパスワード生成部28を含む。そして、発信ユーザ端末2及び受信ユーザ端末3は、このワンタイムパスワードを解析するためのワンタイムパスワード解析部16を含む。かくして、インターネット未接続時において、このワンタイムパスワードをワンタイムパスワード解析部16で読み込んで解析することにより、データを復

元することが可能となる。

[0029] ファイル情報管理部 14 において生成される各結合ファイルには、少なくともアクセス権（公開ユーザ）と開封可能期限を含む復元情報が付される。公開ユーザは複数の場合もあり、また、公開ユーザは 1 個人の場合とグループの場合とがある。この復元情報は、後述するように、管理サーバ 5 において保存管理され、アクセス権を付与された公開ユーザが管理サーバ 5 に照会し、ユーザ認証を経て管理サーバ 5 から供給される。この復元情報を取得した公開ユーザは、その復元情報を用いて、オンラインストレージ 4 から取得した結合ファイルに含まれる分割ファイルを閾値以上収集することにより、原本ファイルを復元することができる。

[0030] 結合ファイルを開封するためのアプリケーションは、自己解凍型、ディスク構成閲覧ソフト型、仮想ディスクマウント型のいずれかとされ、各結合ファイルに付される。自己解凍型の場合、結合ファイルは単一の形式にまとめられ、開封時に単独で自己解凍により自動的に開封される。この場合管理サーバ 5 に問い合わせを行い、アクセス権や開封期日の確認が行われ、開封可能な場合は元の分割ファイルに戻され、管理サーバ 5 から受信した復元情報を元に、デコード部 13 においてデコードされる。なお、この自己解凍型の場合、ファイルは実行形式の形態をとるためにメール添付などできない場合があるが、社内共有や USB メモリ等の媒体を経由してやり取りするのには好適である。

[0031] ディスク構成閲覧ソフト型の場合は、OS 上でのエクスプローラ形式のアプリケーションでファイルの暗号化が行われ、また、復号化が行われる。この場合、ファイル閲覧アプリケーション形式でファイルの属性、その他が表示可能となる。分割ファイルは復元時に収集され、原本ファイルが復元される。

[0032] 仮想ディスクマウント型の場合は、仮想ディスクファイル形式の VHD 形式及び拡張形式のファイルをマウントして、OS 上のディスクへの書き込み時や読み込み時に自動でデータの変換が行われる。この場合、仮想ディスク

をマウントするのと同様に、システムにはドライブとして提供される。

[0033] このように、結合ファイルを開封するためのアプリケーションとして、自己解凍型、ディスク構成閲覧ソフト型、仮想ディスクマウント型のいずれかが用いられ、そのプログラムが結合ファイルに付されるが、その際、結合ファイルと自己解凍等の復元プログラムとの間に、可変長のギャップが埋め込まれ、所謂ゴミデータが挿入される。そのようにすることにより、複数の結合ファイルからデータ部を想定することが一層困難となる。

[0034] 本発明に係るファイルの秘匿分散方法は、原本ファイルを暗号化した上で複数の分割ファイルに断片化すると共に、前記原本ファイルの復元に必要な分割ファイル数の閾値を設定し、前記分割ファイルを複数結合して成る結合ファイルを複数作成し、前記結合ファイルを開封するための復元情報を前記結合ファイルに付加し、前記復元情報を付加した結合ファイルを複数のオンラインストレージに分散して保存させるものである。そして、アクセス権を有する者が前記復元情報を取得することにより、前記オンラインストレージから取得した前記結合ファイルを開封して取り出した閾値以上の数の分割ファイルから、原本ファイルの復元を可能にしたことを特徴としている。このファイルの秘匿分散方法は、上述した本発明に係るファイルの秘匿分散システムを利用して実施することができる。

[0035] 即ち、上記システムを利用したファイルの秘匿分散方法は、図3のフロー図に示されるように、以下のステップからなるものである。

- ・発信ユーザ端末2において、原本ファイルを暗号化した上で複数の分割ファイルに断片化すると共に、前記原本ファイルの復元に必要な分割ファイル数の閾値を設定する原本ファイル暗号化・分割ステップ（S1）

- ・発信ユーザ端末2において、分割ファイルを複数結合して成る結合ファイルを複数作成する結合ファイル作成ステップ（S2）

- ・発信ユーザ端末2において、結合ファイルの開封に必要な復元情報を作成して各結合ファイルに付する復元情報作成ステップ（S3）

- ・発信ユーザ端末2において、復元情報を付した複数の結合ファイルをそ

れぞれ異なるオンラインストレージ4に分散して保存するオンラインストレージ分散・保存ステップ(S4)

・管理サーバ5において、復元情報を保持・管理する復元情報保存ステップ(S5)

・受信ユーザ端末3において、管理サーバ5に対して結合ファイルの復元情報を照会するステップ(S6)

・ユーザ認証を経て管理サーバから取得した復元情報を用いて、オンラインストレージ4から取得した結合ファイルを開封し、収集した閾値以上の数の分割ファイルから原本ファイルを復元するステップ(S7)

[0036] 以下に、本発明に係るシステムを利用したファイルの秘匿分散方法につき、各ステップごとに詳細に説明する。

[0037] 原本ファイル暗号化・分割ステップ(S1)

このステップは、発信ユーザ端末2において、原本ファイルを暗号化した上で複数の分割ファイルに断片化するステップである。このようにファイルを暗号化した上で複数の分割ファイルに断片化すること自体は、一般に行われていることである。図4に示す例では、原本ファイルは9つの分割ファイルに断片化されている。この断片化に際し、原本ファイルの復元に必要な分割ファイルの数の閾値が設定される。後述するように、原本ファイルを復元するために、すべての分割ファイルを収集する必要はなく、所定数(閾値)以上の分割ファイルを集めれば足りる。

[0038] 結合ファイル作成ステップ(S2)

このステップは、発信ユーザ端末2のファイル情報管理部14において、分割ファイルを複数結合した結合ファイルを複数作成するステップである。この結合ファイルの形式は、ZIPファイル形式又は仮想ディスク形式とされる。結合ファイルは、分割ファイルを複数任意の組み合わせで結合したものであり、図4に示す例では、3つの結合ファイルが作成されている。そして、結合ファイル1は分割ファイル1, 2, 5の組み合わせとされ、結合ファイル2は分割ファイル3, 4, 8, 9の組み合わせとされ、結合ファイル

3は分割ファイル6, 7の組み合わせとされている。

[0039] 復元情報作成ステップ(S3)

このステップは、発信ユーザ端末2のファイル情報管理部14において、結合ファイルの復元に必要な復元情報を作成して各結合ファイルに付するステップである。ここにいう復元情報は、原本ファイルを復元するための情報ではなく、原本ファイルを復元する前処理である結合ファイルを開封するための情報であり、少なくともアクセス権、即ち、発信ユーザ端末2の管理者によって指定されるユーザ名(公開ユーザ名)と開封可能期限が含まれ、また、上述した原本ファイルの復元に必要な分割ファイルの閾値が含まれ、公開ユーザごとに設定される。この復元情報の作成は、管理サーバ5のユーザインターフェース部21によって提供されるユーザインターフェースを通して行う。なお、復元情報は固定されたものではなく、随時変更可能なものであり、変更がなされた場合は、後述する管理サーバ5のファイル情報管理部25における保存データが更新される。

[0040] オンラインストレージ分散・保存ステップ(S4)

このステップは、復元情報が付された複数の結合ファイルが、発信ユーザ端末2のファイル情報管理部14から分散ファイル入出力部15を介して、それぞれ異なるオンラインストレージ4に分散されて保存されるステップである。図4に示す例では、結合ファイル1はオンラインストレージAに保存され、結合ファイル2はオンラインストレージBに保存され、結合ファイル3はオンラインストレージCに保存されている。その分散された結合ファイルがそれぞれどのオンラインストレージ4に配置されたかに関する配置情報やチェック・サム等は、ファイル情報管理部14において管理される。また、これらの情報は、同時に管理サーバ5のファイル情報管理部25に送信されて情報共有される。なお、各オンラインストレージ4に保存される結合ファイルは同一とは限らないが、容量や分散管理の運用等の関係で、すべて同一にされることもある。

[0041] 復元情報保存ステップ(S5)

このステップは、管理サーバ5のファイル情報管理部25において、発信ユーザ端末2のファイル情報管理部14から送信される復元情報を、後述の公開ユーザからの照会に対応するために保持・管理するステップである。

[0042] 復元情報照会ステップ(S6)

このステップは、原本ファイルの復元を希望する公開ユーザが、その受信ユーザ端末3から管理サーバ5に対して結合ファイルの復元情報を照会するステップである。公開ユーザから復元情報の照会があると、管理サーバ5の開封管理部24においてアクセス権等のチェックがなされ、アクセス権等を有する公開ユーザである場合には、当該公開ユーザの受信ユーザ端末3に復元情報が送信される。また、公開ユーザから復元情報の照会がある度に、ログ生成部27においてログが生成されてデータベース29に保存され、そのデータは、送信ユーザ端末1からの閲覧要求に応じて公開される。

[0043] 原本ファイル復元ステップ(S7)

このステップは、公開ユーザが、管理サーバ5から送信された復元情報を用いて、オンラインストレージ4から取得した結合ファイルを開封して収集した閾値以上の数の分割ファイルから、原本ファイルを復元するステップである。通例、原本ファイルへの復元には複数の結合ファイルが必要となるが、閾値以上の数の分割ファイルを含む結合ファイルの場合は、1つの結合ファイルでの復元が可能となる。図4に示す例では、結合ファイル1は3つの分割ファイルを含み、結合ファイル2は4つの分割ファイルを含み、結合ファイル3は2つの分割ファイルを含んでいるので、例えば、閾値数が4の場合は、分割ファイルを4つ含む結合ファイル2のみで足りることになり、閾値数が5の場合は、結合ファイルは少なくとも2つ必要となる(図5参照)。

[0044] 公開ユーザが結合ファイルを開封する度に、ログ生成部27においてログが生成されてデータベース29に登録され、ユーザがその開封記録を参照することが可能となる。なお、原本ファイルの復元に必要な分割ファイル数が閾値に満たない場合は、複数の結合ファイルが必要となるが、その場合は、

管理サーバ5 に対し、その他の分割ファイル及び結合ファイルを要求することによりデータが配信され、以て、復元プロセス（原本ファイル復元ステップ（S 7））が実行される。本発明においては、このように原本ファイルを復元するために、分割時に設定した閾値以上の数の分割ファイルを集めれば足り、これを、管理サーバ5 から送られてくる分割ファイルの復号化のための情報を用いてデコード部1 3 において復号化できる。

産業上の利用可能性

[0045] 本発明に係るファイルの秘匿分散システム及び方法は上記構成であって、ファイルの復元が複雑化されているために十分な秘匿性を保持することができる。また、結合ファイルが秘匿状態にてオンラインストレージに分散保存されるため、ハードウェア障害発生時や災害時等において一部のファイルが消失しても、残りのファイルを用いて原本ファイルを復元することが可能であるので、事業継続性を確保できるという効果があり、その産業上の利用可能性は大である。