

請求の範囲

[請求項1] 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、開封して収集した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である場合に、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。

[請求項2] 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、請求項 1 に記載のファイルの秘匿分散システム。

[請求項3] 前記原本ファイルの復元に必要な前記分割ファイル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、請求項 2 に記載のファイルの秘匿分散システム。

[請求項4] 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を含む、請求項 1 乃至 3 のいずれかに記載のファイルの秘匿分散システム。

[請求項5] 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、請求項 1 に記載のファイルの秘匿分散システム。

[請求項6] 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である、請求項 1 に記載のファイルの秘匿分散システム。

[請求項7]

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。

[請求項8]

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、予め設定された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。

[請求項9] 前記結合ファイルに付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、請求項7又は8に記載のファイルの秘匿分散方法。

[請求項10] 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である、請求項7又は8に記載のファイルの秘匿分散方法。

[請求項11] 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、請求項10に記載のファイルの秘匿分散方法。