

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6324794号
(P6324794)

(45) 発行日 平成30年5月16日 (2018. 5. 16)

(24) 登録日 平成30年4月20日 (2018. 4. 20)

(51) Int. Cl.		F I			
G 0 6 F	12/00	(2006. 01)	G 0 6 F	12/00	5 3 3 J
G 0 6 F	21/62	(2013. 01)	G 0 6 F	12/00	5 3 7 H
G 0 9 C	1/00	(2006. 01)	G 0 6 F	21/62	
			G 0 9 C	1/00	6 6 0 D

請求項の数 13 (全 22 頁)

(21) 出願番号	特願2014-86190 (P2014-86190)	(73) 特許権者	000233055
(22) 出願日	平成26年4月18日 (2014. 4. 18)		株式会社日立ソリューションズ
(65) 公開番号	特開2015-207081 (P2015-207081A)		東京都品川区東品川四丁目12番7号
(43) 公開日	平成27年11月19日 (2015. 11. 19)	(74) 代理人	110000279
審査請求日	平成29年1月4日 (2017. 1. 4)		特許業務法人ウィルフォート国際特許事務所
		(72) 発明者	久原 雄三
			東京都品川区東品川四丁目12番7号 株式会社日立ソリューションズ内
		審査官	甲斐 哲雄

最終頁に続く

(54) 【発明の名称】 クラウド・ストレージ・システム

(57) 【特許請求の範囲】

【請求項1】

端末装置の同期記録領域にファイルを記録すると、当該ファイルをサーバ装置に送信して管理することで、他の端末装置からも当該ファイル进行操作可能とするストレージ・システムであって、

前記端末装置は、

前記同期記録領域のファイル読み出し指令に対応して、当該ファイルを復号化して読み出し、一時的記憶領域に保持する復号化読出手段と、

前記ファイルに関連づけられたプログラムを起動し、前記復号化されたファイル进行操作できる状態とする関連プログラム起動手段と、

書込指令によって前記同期記録領域に記録されたファイルが、暗号化されているかどうかを判断する書込時判断手段と、

書込時判断手段によって、当該ファイルが暗号化されていないと判断された場合には、当該ファイルを暗号化する暗号化手段と、

一時的記憶領域の復号化ファイルの内容が変更されたかどうかを監視し、変更があれば当該復号化ファイルまたは当該復号化ファイルを暗号化した暗号化ファイルを、同期記録領域に書き込むための書込指令を出す書込指令手段と、

を備えたストレージ・システム。

【請求項2】

端末装置の同期記録領域にファイルを記録すると、当該ファイルをサーバ装置に送信し

10

20

て管理することで、他の端末装置からも当該ファイル进行操作可能とするストレージ・システムに用いる前記端末装置であって、

前記同期記録領域のファイル読み出し指令に対応して、当該ファイルを復号化して読み出し、一時的記憶領域に保持する復号化読出手段と、

前記ファイルに関連づけられたプログラムを起動し、前記復号化されたファイル进行操作できる状態とする関連プログラム起動手段と、

書込指令によって前記同期記録領域に記録されたファイルが、暗号化されているかどうかを判断する書込時判断手段と、

書込時判断手段によって、当該ファイルが暗号化されていないと判断された場合には、当該ファイルを暗号化する暗号化手段と、

一時的記憶領域の復号化ファイルの内容が変更されたかどうかを監視し、変更があれば当該復号化ファイルまたは当該復号化ファイルを暗号化した暗号化ファイルを、同期記録領域に書き込むための書込指令を出す書込指令手段と、

を備えた端末装置。

【請求項 3】

端末装置の同期記録領域にファイルを記録すると、当該ファイルをサーバ装置に送信して管理することで、他の端末装置からも当該ファイル进行操作可能とするストレージ・システムに用いる前記端末装置を、コンピュータによって実現するための端末プログラムであって、コンピュータを、

前記同期記録領域のファイル読み出し指令に対応して、当該ファイルを復号化して読み出し、一時的記憶領域に保持する復号化読出手段と、

前記ファイルに関連づけられたプログラムを起動し、前記復号化されたファイル进行操作できる状態とする関連プログラム起動手段と、

書込指令によって前記同期記録領域に記録されたファイルが、暗号化されているかどうかを判断する書込時判断手段と、

書込時判断手段によって、当該ファイルが暗号化されていないと判断された場合には、当該ファイルを暗号化する暗号化手段と、

一時的記憶領域の復号化ファイルの内容が変更されたかどうかを監視し、変更があれば当該復号化ファイルまたは当該復号化ファイルを暗号化した暗号化ファイルを、同期記録領域に書き込むための書込指令を出す書込指令手段として機能させるための端末プログラム。

【請求項 4】

請求項 3 の 端末 プログラムにおいて、

前記書込時判断手段は、前記書込指令によって同期記録領域に記録されたファイルについて、少なくとも前記ファイルに付された暗号化識別子または前記ファイルのファイル名の拡張子に基づいて、当該ファイルが暗号化されているか否かを判断することを特徴とする 端末 プログラム。

【請求項 5】

請求項 3 の 端末 プログラムにおいて、コンピュータを、さらに

前記同期記録領域にファイルが書き込まれようとする際に、当該ファイルを暗号化して書き込む暗号化書込手段として機能させるための 端末 プログラム。

【請求項 6】

請求項 3 または 5 の 端末 プログラムにおいて、

前記復号化読出手段は、前記同期記録領域からファイルが読み出されようとする際に、当該ファイルを復号化して読み出すことを特徴とする 端末 プログラム。

【請求項 7】

請求項 5 または 6 の 端末 プログラムにおいて、

前記復号化読出手段および暗号化書込手段は、読出指令または書込指令をオペレーティングシステムから受けて、処理を実行するものであることを特徴とする 端末 プログラム。

【請求項 8】

請求項 5 または 7 の 端末プログラムにおいて、

前記ストレージ・システムは、端末装置の同期記録領域にファイル実体は残さずに、当該ファイル実体に関連づけられたファイル仮体を残し、端末装置において当該ファイル仮体を開く操作をすると、サーバ装置からファイル実体を同期記録領域にダウンロードする実体取得処理を行うように構成されており、

前記暗号化書込手段は、前記実体取得処理による同期記録領域への書き込みについては、例外的に暗号化を行わずに書き込みを行い、

前記復号化読出手段は、読出指令を受けると、前記サーバ装置に対して実体取得処理を実行するように指令し、同期記録領域内にファイル実体がダウンロードされると、当該ファイル実体を復号化して読み出し、一時的記憶領域に保持することを特徴とする端末プログラム。

10

【請求項 9】

請求項 3 ～ 8 のいずれかの端末プログラムにおいて、コンピュータを、さらに

前記一時的記憶領域に保持されたファイルを、当該ファイルに対応付けられたプログラムが終了すれば、あるいは端末装置が終了すれば、削除する削除手段として機能させるための端末プログラム。

【請求項 10】

端末装置の同期記録領域にファイルを記録すると、当該ファイルをサーバ装置に送信して管理することで、他の端末装置からも当該ファイル进行操作可能とするストレージ・システムであって、

20

前記端末装置は、

前記同期記録領域にファイルが書き込まれようとする際に、当該ファイルを暗号化して書き込む暗号化書込手段と、

前記同期記録領域からファイルが読み出されようとする際に、当該ファイルを復号化して読み出し、一時的記憶領域に保持する復号化読出手段と、

書込指令によって前記同期記録領域に記録されたファイルが、暗号化されているかどうかを判断する書込時判断手段と、

書込時判断手段によって、当該ファイルが暗号化されていないと判断された場合には、当該ファイルを暗号化する暗号化手段と、

一時的記憶領域の復号化ファイルの内容が変更されたかどうかを監視し、変更があれば当該復号化ファイルまたは当該復号化ファイルを暗号化した暗号化ファイルを、同期記録領域に書き込むための書込指令を出す書込指令手段とを備え、

30

前記復号化読出手段および暗号化書込手段は、読出指令または書込指令をオペレーティングシステムから受けて、処理を実行するものであることを特徴とするストレージ・システム。

【請求項 11】

端末装置の同期記録領域にファイルを記録すると、当該ファイルをサーバ装置に送信して管理することで、他の端末装置からも当該ファイル进行操作可能とするストレージ・システムに用いる前記端末装置であって、

前記同期記録領域にファイルが書き込まれようとする際に、当該ファイルを暗号化して書き込む暗号化書込手段と、

40

前記同期記録領域からファイルが読み出されようとする際に、当該ファイルを復号化して読み出し、一時的記憶領域に保持する復号化読出手段と、

書込指令によって前記同期記録領域に記録されたファイルが、暗号化されているかどうかを判断する書込時判断手段と、

書込時判断手段によって、当該ファイルが暗号化されていないと判断された場合には、当該ファイルを暗号化する暗号化手段と、

一時的記憶領域の復号化ファイルの内容が変更されたかどうかを監視し、変更があれば当該復号化ファイルまたは当該復号化ファイルを暗号化した暗号化ファイルを、同期記録領域に書き込むための書込指令を出す書込指令手段とを備え、

50

前記復号化読出手段および暗号化書込手段は、読出指令または書込指令をオペレーティングシステムから受けて、処理を実行するものであることを特徴とする端末装置。

【請求項 1 2】

端末装置の同期記録領域にファイルを記録すると、当該ファイルをサーバ装置に送信して管理することで、他の端末装置からも当該ファイル进行操作可能とするストレージ・システムに用いる前記端末装置を、コンピュータによって実現するための端末プログラムであって、コンピュータを、

前記同期記録領域にファイルが書き込まれようとする際に、当該ファイルを暗号化して書き込む暗号化書込手段と、

前記同期記録領域からファイルが読み出されようとする際に、当該ファイルを復号化して読み出し、一時的記憶領域に保持する復号化読出手段と、

書込指令によって前記同期記録領域に記録されたファイルが、暗号化されているかどうかを判断する書込時判断手段と、

書込時判断手段によって、当該ファイルが暗号化されていないと判断された場合には、当該ファイルを暗号化する暗号化手段と、

一時的記憶領域の復号化ファイルの内容が変更されたかどうかを監視し、変更があれば当該復号化ファイルまたは当該復号化ファイルを暗号化した暗号化ファイルを、同期記録領域に書き込むための書込指令を出す書込指令手段として機能させ、

前記復号化読出手段および暗号化書込手段は、読出指令または書込指令をオペレーティングシステムから受けて、処理を実行するものであることを特徴とする端末プログラム。

【請求項 1 3】

請求項 1 2 の端末プログラムにおいて、

前記ストレージ・システムは、端末装置の同期記録領域にファイル実体は残さずに、当該ファイル実体に関連づけられたファイル仮体を残し、端末装置において当該ファイル仮体を開く操作をすると、サーバ装置からファイル実体を同期記録領域にダウンロードする実体取得処理を行うように構成されており、

前記暗号化書込手段は、前記実体取得処理による同期記録領域への書き込みについては、例外的に暗号化を行わずに書き込みを行い、

前記復号化読出手段は、読出指令を受けると、前記サーバ装置に対して実体取得処理を実行するように指令し、同期記録領域内にファイル実体がダウンロードされると、当該ファイル実体を復号化して読み出し、一時的記憶領域に保持することを特徴とする端末プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

この発明は、サーバ装置にファイルなどを共有するクラウド・ストレージ・システムに関するものである。

【背景技術】

【0002】

端末装置の記録領域の内容を、サーバ装置の記録領域の内容と同期させることで、サーバ装置に最新の記録状況を複製し、他の端末装置からも記録領域の内容を操作できるようにするクラウド・ストレージ・システムが実用化されている。たとえば、Dropbox社（商標）などが用いられている。Dropbox（商標）では、端末装置に同期フォルダを作成し、このフォルダ中のファイルについては、サーバ装置にも複製を生成し、同期をとるようにしている。

【0003】

常に、最新の状況がサーバ装置に保持されているので、端末装置を持ち歩かなくとも、移動先にサーバ装置に接続できる端末装置があれば、作業を継続的に進めることができる。

【0004】

しかしながら、上記のような従来技術においては、インターネットでアクセス可能なサーバ装置上にファイルなどが記録されることになり、セキュリティ上好ましいとはいえなかった。

【0005】

この問題を解決するために、同期フォルダにファイルを保存する前に、暗号化プログラムを起動して暗号化してから保存し、同期フォルダから読み出したファイルについては、復号化プログラムによって復号化して使用することも行われている。

【先行技術文献】

【特許文献】

【0006】

10

【特許文献1】特開2002-99456

【非特許文献】

【0007】

【非特許文献1】Dropbox（商標）説明(<https://www.dropbox.com/business>)

【発明の概要】

【発明が解決しようとする課題】

【0008】

上記のように暗号化する方法では、ユーザにとって操作が煩雑であり、煩わしいという問題があった。

【0009】

20

特許文献1には、指定のフォルダにファイルを保存すると、当該ファイルが暗号化されていないことを検出して、自動的に暗号化して保存することのできるシステムが開示されている。この特許文献1の技術は、クラウド・ストレージ・システムを対象とするものではないが、仮に、これをクラウド・ストレージ・システムに用いたとすると、暗号化という面においては、煩雑さが解消されるというメリットがある。

【0010】

しかしながら、上記特許文献1においても、復号化の際には、復号化プログラムを立ち上げて、フォルダ内のファイルを復号化した上、展開用フォルダを指定して復号化ファイルを保存するという操作が必要であり、煩雑であった。しかも、アプリケーションソフトウェアにて編集したファイルを、展開用フォルダにて更新し、その後、暗号化のためのフォルダに記録するという操作が必要であった。つまり、多くのファイルを扱わなければならないが、ユーザが意識しなければならないフォルダ、ファイルの数が増え、混乱を招く可能性があった。

30

【0011】

また、特許文献1では、フォルダに保存されたファイルが暗号化されているかいないかを判断して、暗号化されていなければ自動的に暗号化するようにしている。このため、端末装置の同期フォルダにはファイル実体を置かず、ファイル仮体のみを保存するようなクラウド・ストレージ・システムに、特許文献1の自動暗号化を組み合わせたと仮定すると、適切な動作がなされない可能性があった。すなわち、上記のようなクラウド・ストレージ・システムでは、同期フォルダ中に仮体ファイルしか記録されない。このため、これを暗号化したとしても、サーバ装置側には暗号化されていない実体ファイルが記録されることになり、セキュリティ上の問題が解決されなかった。

40

【0012】

この発明は上記のいずれかの問題を解決して、セキュリティを担保しつつ、ユーザの操作性のよい、クラウド・ストレージ・システム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】

【0013】

(1)(2)(3)この発明に係るストレージ・システムは、端末装置の同期記録領域にファイルを記録すると、当該ファイルをサーバ装置に送信して管理することで、他の端末装置からも当該ファイルを操作可能とするストレージ・システムであって、前記端末装置は、前記

50

同期記録領域のファイル読み出し指令に対応して、当該ファイルを復号化して読み出し、一時的記憶領域に保持する復号化読出手段と、前記ファイルに関連づけられたプログラムを起動し、前記復号化されたファイル进行操作できる状態とする関連プログラム起動手段とを備えている。

【0014】

したがって、ユーザは復号化のための操作を行わなくとも、暗号化されてサーバ装置に保存されている暗号化ファイルを復号化して編集することができる。

【0015】

(4)この発明に係る端末プログラムは、コンピュータを、書込指令によって前記同期記録領域に記録されたファイルが、暗号化されているかどうかを判断する書込時判断手段と、書込時判断手段によって、当該ファイルが暗号化されていないと判断された場合には、当該ファイルを暗号化する暗号化手段として機能させるものである。

10

【0016】

したがって、ユーザは暗号化のための操作を行わなくとも、ファイルを暗号化して保存することができる。

【0017】

(5)この発明に係る端末プログラムは、コンピュータを、一時的記憶領域の復号化ファイルの内容が変更されたかどうかを監視し、変更があれば当該復号化ファイルまたは暗号化ファイルを同期記録領域に書き込むための書込指令を出す書込指令手段として機能させるものである。

20

【0018】

したがって、一時記憶領域に保持したファイルを編集して上書きすれば、同期記録領域のファイルも変更される。

【0019】

(6)この発明に係る端末プログラムは、書込時判断手段は、前記書込指令によって同期記録領域に記録されたファイルについて、少なくとも前記ファイルに付された暗号化識別子または前記ファイルのファイル名の拡張子に基づいて、当該ファイルが暗号化されているか否かを判断する。

【0020】

したがって、確実に暗号化ファイルであるか否かを判断することができる。

30

【0021】

(7)この発明に係る端末プログラムは、コンピュータを、同期記録領域にファイルが書き込まれようとする際に、当該ファイルを暗号化して書き込む暗号化書込手段として機能させるものである。

【0022】

したがって、ユーザが暗号化の操作を行うことなく、ファイルを暗号化して同期処理を行うことができる。

【0023】

(8)この発明に係る端末プログラムは、復号化読出手段が、前記同期記録領域からファイルが読み出されようとする際に、当該ファイルを復号化して読み出すことを特徴としている。

40

【0024】

したがって、ユーザが復号化の操作を行うことなく、同期記録領域のファイルを復号化する処理を行うことができる。

【0025】

(9)この発明に係る端末プログラムは、復号化読出手段および暗号化書込手段が、読出指令または書込指令をオペレーティングシステムから受けて、処理を実行するものであることを特徴としている。

【0026】

(10)この発明に係る端末プログラムは、ストレージ・システムは、端末装置の同期記録領

50

域にファイル実体は残さずに、当該ファイル実体に関連づけられたファイル仮体を残し、端末装置において当該ファイル仮体を開く操作をすると、サーバ装置からファイル実体を同期記録領域にダウンロードする実体取得処理を行うように構成されており、前記暗号化書込手段は、前記実体取得処理による同期記録領域への書き込みについては、例外的に暗号化を行わずに書き込みを行い、前記復号化読出手段は、読出指令を受けると、前記サーバ装置に対して実体取得処理を実行するように指令し、同期記録領域内にファイル実体がダウンロードされると、当該ファイル実体を復号化して読み出し、一時的記憶領域に保持することを特徴としている。

【0027】

したがって、ファイルの実体を端末装置側に保存しないシステムにおいても、ユーザによる暗号化・復号化操作なく、暗号化したストレージシステムを提供できる。

10

【0028】

(11)この発明に係る端末プログラムは、コンピュータを、一時的記憶領域に保持されたファイルを、当該ファイルに対応付けられたプログラムが終了すれば、あるいは端末装置が終了すれば、削除する削除手段として機能させるためのものである。

【0029】

したがって、余分なファイルを残さないようにすることができる。

【0030】

(12)(13)(14)この発明に係るストレージ・システムは、端末装置の同期記録領域にファイルを記録すると、当該ファイルをサーバ装置に送信して管理することで、他の端末装置からも当該ファイルを操作可能とするストレージ・システムであって、前記端末装置は、前記同期記録領域にファイルが書き込まれようとする際に、当該ファイルを暗号化して書き込む暗号化書込手段と、前記同期記録領域からファイルが読み出されようとする際に、当該ファイルを復号化して読み出す復号化読出手段とを備え、前記復号化読出手段および暗号化書込手段は、読出指令または書込指令をオペレーティングシステムから受けて、処理を実行するものであることを特徴としている。

20

【0031】

したがって、ユーザは暗号化・復号化のための操作を行う必要のない、暗号化されたストレージ・システムを実現することができる。

【0032】

30

(15)この発明に係る端末プログラムは、ストレージ・システムは、端末装置の同期記録領域にファイル実体は残さずに、当該ファイル実体に関連づけられたファイル仮体を残し、端末装置において当該ファイル仮体を開く操作をすると、サーバ装置からファイル実体を同期記録領域にダウンロードする実体取得処理を行うように構成されており、暗号化書込手段は、前記実体取得処理による同期記録領域への書き込みについては、例外的に暗号化を行わずに書き込みを行い、復号化読出手段は、読出指令を受けると、前記サーバ装置に対して実体取得処理を実行するように指令し、同期記録領域内にファイル実体がダウンロードされると、当該ファイル実体を復号化して読み出し、一時的記憶領域に保持することを特徴としている。

【0033】

40

したがって、ファイルの実体を端末装置側に保存しないシステムにおいても、ユーザによる暗号化・復号化操作なく、暗号化したストレージシステムを提供できる。

【0034】

「復号化読出手段」は、実施形態においては、ステップS7、S8がこれに対応する。

【0035】

「復号化して読み出す」とは、読み出す際に復号化するという意味であり、複合化してから読み出す場合だけでなく、読み出してから復号化する場合も含む概念である。

【0036】

「関連プログラム起動手段」は、実施形態においては、ステップS9がこれに対応する。

50

【0037】

「書込時判断手段」は、実施形態においては、ステップS2がこれに対応する。

【0038】

「暗号化手段」は、実施形態においては、ステップS3がこれに対応する。

【0039】

「書込指令手段」は、実施形態においては、ステップS10、S12がこれに対応する。

【0040】

「暗号化書込手段」は、実施形態においては、ステップS3、S4がこれに対応する。

【0041】

「暗号化して書き込む」とは、書き込み際に暗号化するという意味であり、暗号化してから書き込み場合だけでなく、書き込んでから暗号化する場合も含む概念である。

【0042】

「プログラム」とは、CPUにより直接実行可能なプログラムだけでなく、ソース形式のプログラム、圧縮処理がされたプログラム、暗号化されたプログラム等を含む概念である。

【図面の簡単な説明】

【0043】

【図1】この発明の第1の実施形態によるクラウド・ストレージ・システムの機能ブロック図である。

【図2】端末装置T1のハードウェア構成である。

【図3】ファイル書き込みの際のフローチャートである。

【図4】暗号化ファイルのデータ構造である。

【図5】ファイルの読み出し・更新の際のフローチャートである。

【図6】ファイルの読み出し・更新の際のフローチャートである。

【図7】第2の実施形態によるクラウド・ストレージ・システムの機能ブロック図である。

。

【図8】ファイル書き込みの際のフローチャートである。

【図9】ファイルの読み出し・更新の際のフローチャートである。

【図10】第3の実施形態によるクラウド・ストレージ・システムの機能ブロック図である。

【図11】ファイル書き込みの際のフローチャートである。

【図12】ファイルの読み出し・更新の際のフローチャートである。

【図13】ファイルの読み出し・更新の際のフローチャートである。

【図14】ファイルの読み出し・更新の際のフローチャートである。

【発明を実施するための形態】

【0044】

1. 第1の実施形態

1.1全体構成

一般に、クラウド・ストレージ・システムにおいては、端末装置とサーバ装置との間の同期の取り方において2つの方法がある。一つは、端末装置に記録されたファイルはそのまま残しつつ、サーバ装置にそのファイルを複製する方法である。もう一つは、端末装置のファイルをサーバ装置に転送し、端末装置にはファイルの実体は残さず、ファイルがあることを示すデータ（ファイル仮体）を残す方法である。

【0045】

前者の方法であれば、端末装置にファイル実体があるので、サーバ装置に接続できない状態であっても、ファイルの操作を行うことが可能である。一方、後者の方法であれば、端末装置にファイル実体がないので、サーバ装置に接続できる環境でないとファイルの操作ができないものの、端末装置の記憶容量が小さくてすむという利点がある。

【0046】

10

20

30

40

50

この実施形態では、前者の方法によるクラウド・ストレージ・システムを前提として説明を行う。図 1 に、この発明の一実施形態によるクラウド・ストレージ・システムの全体構成を示す。

【0047】

端末装置 T1、T2・・・は、それぞれ、インターネットなどを介して、サーバ装置 S に接続可能である。各端末装置 T1、T2・・・には、同期記録領域 10 が設けられている。各端末装置 T1、T2・・・の同期記録領域 10 とサーバ装置 S の同期記録領域 20 は、互いに同期をとるように構成されている。したがって、いずれかの端末装置 T にて、同期記録領域 10 のファイル 12 が変更されると、サーバ装置 S のファイル 22 も同期して変更される。その結果、他の端末装置 T2・・・のファイル 12 も同じように変更されることになる。

10

【0048】

端末装置 T1 において、同期記録領域 10 に新たなファイル 12 が記録されると（あるいは、ファイル 12 が更新されると）、書込時判断手段 8 は、書き込まれたファイル 12 が暗号化されているかどうかを判断する。暗号化されていない（平文である）と判断されると、暗号化書込手段 6 は、平文ファイル 12 を暗号化して暗号化ファイル 13 とする。したがって、暗号化されたファイル 13 が、暗号化ファイル 22 としてサーバ装置 S の同期記録領域 20 に記録されることになる。ユーザは、暗号化のための操作を別途行うことなく、同期記録領域 10 に暗号化したファイル 13 を記録することができる。

20

【0049】

端末装置 T1 において、暗号化ファイル 13 に対する読み出し指令があると、復号化読出手段 2 は、暗号化ファイル 13 を復号化して読み出す。復号化したファイルは、平文ファイル 15 として一時的記憶領域 14 に保持される。関連プログラム起動手段 4 は、一時的記憶領域 14 の平文ファイル 15 に関連づけられたプログラムを起動する。したがって、ユーザは、復号化のための操作を別途行うことなく、同期記録領域 10 の暗号化ファイル 13 を復号化し、関連するプログラムを起動することができる。

【0050】

上記のようにして、ユーザ操作の煩わしさをもたらすことなく、暗号化によるセキュリティを維持したクラウド・ストレージ・システムを実現できる。

30

【0051】

1.2 ハードウェア構成

図 2 に、端末装置 T1 のハードウェア構成を示す。なお、他の端末装置 T2・・・も同様の構成である。CPU 30 には、メモリ 32、ディスプレイ 34、ハードディスク 36、DVD-ROM ドライブ 38、マウス／キーボード 40、通信回路 42 が接続されている。

【0052】

通信回路 42 は、インターネットに接続するためのものである。ハードディスク 36 には、オペレーティングシステム 44、同期プログラム 46、端末プログラム 48 が記録されている。同期プログラム 46、端末プログラム 48 は、オペレーティングシステム 44 と協働して、その機能を発揮するものである。また、これらプログラムは、DVD-ROM 52 に記録されていたものを、DVD-ROM ドライブ 38 を介して、ハードディスク 36 にインストールしたものである。

40

【0053】

同期プログラム 46 は、クラウド・ストレージによる同期処理を実現するためのプログラムであり、たとえば、Dropbox（商標）などを用いることができる。端末プログラム 48 は、暗号・復号化処理を行うためのプログラムである。この実施形態では、同期プログラム 46 と端末プログラム 48 に分離しているが、一体のプログラムとして構成してもよい。

【0054】

50

サーバ装置 S のハードウェア構成も、端末装置 T1 と同様である。ただし、ハードディスク 36 には、同期プログラム 46 が記録されているが、端末プログラム 48 は記録されていない。

【0055】

1.3 処理内容

図 3 に、このシステムによるファイル書き込みのフローチャートを示す。端末プログラム 48、同期プログラム 46 は、ハードディスク 36 の同期フォルダ 50 に変化があったかどうか（新しいファイルが記録されたか、ファイル内容に変更があったか）を監視しており、変化があれば処理を開始する。

10

【0056】

したがって、今、同期フォルダ 50 に、書き込み指令があつて（同期フォルダ 50 にファイルアイコンがドロップされた、同期フォルダ 50 を指定した保存命令があつたなど）ファイルが新たに記録されたとすると、端末プログラム 48、同期プログラム 46 が処理を開始する。まず、端末プログラム 48 にしたがって、端末装置 T1 の CPU 30（以下端末装置 T1 と省略することがある）は、記録されたファイルを読み出す（ステップ S1）。端末装置 T1 は、当該ファイルが暗号化されているかどうかを判断する（ステップ S2）。この実施形態では、端末装置 T1 は、ファイルの内容をみて、暗号化されているかどうかを判断する。

【0057】

図 4 に、端末プログラム 48 によって暗号化された場合のファイルのデータ構造を示す。先頭に暗号化識別子が記録されている、この実施形態では、予め定められた 128 バイトの数字列を暗号化識別子としている。したがって、ファイルの先頭に、暗号化識別子があるかどうかによって、当該ファイルが端末プログラム 48 による暗号化ファイルであるか、暗号化されていないファイルであるかを判断することができる。

20

【0058】

暗号化ファイルでなければ、端末装置 T1 は、当該ファイルを暗号化する（ステップ S3）。この処理は、メモリ 32 上にファイルを展開して行われる。暗号化がなされると、ファイルのデータ構造は、図 4 に示すようになる。端末装置 T1 は、同期フォルダ 50 の当該ファイルを、暗号化したファイルで置き換える（ステップ S4）。この際、端末装置 T1 は、ファイル名の拡張子のみを変更して新たなファイル名とする。たとえば、元のファイルのファイル名が Patent.jtd であれば、Patent.zdc を新たなファイル名とする。つまり、拡張子を zdc に変更したうえで、暗号化ファイルを記録する。

30

【0059】

なお、すでに端末プログラム 48 によって暗号化されたファイルであれば、暗号化は行わない。

【0060】

この処理と並行して、同期プログラム 46 により、端末装置 T1 は、同期フォルダ 50 内の上記暗号化されたファイルを、サーバ装置 S にアップロードする（ステップ S41）。サーバプログラムにより、サーバ装置 S の CPU（以下、サーバ装置と省略することがある）は、暗号化ファイルを受信する（ステップ S61）。さらに、受信した暗号化ファイルを、ハードディスクに記録する（ステップ S62）。

40

【0061】

以上のようにして、ユーザは同期フォルダ 50 にファイルを記録する（あるいはファイルをドロップする）だけで、暗号化が行われ、サーバ装置 S との同期がとられる。

【0062】

なお、同期プログラム 46 の動作タイミングによっては、同期フォルダ 50 に記録された直後の平文ファイルが、サーバ装置 S に記録される可能性がある。しかし、その後、当該平文ファイルが暗号化されると、ファイルの内容が変化するので、再び同期プログラム 46 が動作し、サーバ装置 S に暗号化ファイルが記録される。したがって、最終的には、

50

サーバ装置 S に暗号化ファイルが記録されることになる。

【0063】

なお、同期プログラム 46 の側において、暗号化されていないファイルは同期をとらない（サーバ装置 S に記録しない）ようにしてもよい。

【0064】

図 5、図 6 に、ファイル読み出し・更新のフローチャートを示す。端末プログラム 48 は、同期フォルダ 50 内のファイルに対して、読出指令（ファイルアイコンがダブルクリックされる、プログラムからファイルオープンへの指示があるなど）があったかどうかを監視している。読出指令があると、端末装置 T1 は、同期フォルダ 50 の当該ファイルを読み出す（ステップ S6）。 10

【0065】

このファイルは暗号化されているので、端末装置 T1 は、当該ファイルを復号化する（ステップ S7）。この処理は、メモリ 32 にファイルを展開して行う。次に、端末装置 T1 は、復号化したファイルを、ハードディスク 36 の一時的記憶領域に格納する（ステップ S8）。この際、暗号化ファイルのファイル名を、元のファイルのファイル名に変更して格納する。たとえば、暗号化ファイルのファイル名が Patent.zdc であれば、元のファイル名 Patent.jtd に戻して格納する。なお、元のファイル名は、図 4 に示すように、暗号化ファイルの先頭部分に記載されているのでこれを用いる。

【0066】

次に、端末装置 T1 は、復号化したファイルに対応するプログラムを起動し、当該ファイルを開く（ステップ S9）。なお、ファイルに対応するプログラムは、当該ファイルの拡張子に基づいて判断する。たとえば、拡張子が docx であればマイクロソフト社の Word（商標）、jtd であればジャストシステム社の一太郎（商標）というように判断することができる。 20

【0067】

なお、既に対応するプログラムが起動している場合には、プログラムは新たに起動しなくてもよい。

【0068】

したがって、ユーザは、同期フォルダ 50 内のファイルをダブルクリックするだけで、復号化されたファイルが、対応するプログラムによって開かれ、編集を行うことができる。 30

【0069】

端末プログラム 48 は、ハードディスク一時的記憶領域のファイル内容が変更されたかどうかを監視している（ステップ S10）。つまり、ユーザが一時的記憶領域のファイルを編集し、編集後のファイルを上書きしたかどうかを監視している。

【0070】

一時的記憶領域のファイル内容が変化したことを検出すると、端末装置 T1 は、一時的記憶領域に保存された編集後ファイルを読み出して暗号化する（ステップ S11）。続いて、端末装置 T1 は、この暗号化された編集後ファイルを、同期フォルダ 50 内の元の暗号化ファイルに上書きする（ステップ S12）。すなわち、元の暗号化ファイルを、暗号化された元の編集後ファイルで置き換える。 40

【0071】

これにより、同期フォルダ 50 内の暗号化ファイルの内容が変更されることになる。したがって、同期フォルダ 50 内の変更に基づいて処理が開始される図 3 のファイル書き込み処理が実行される。図 3 において、端末プログラム 48 により、端末装置 T1 は、当該暗号化ファイルを読み出す（ステップ S1）。このファイルは暗号化されているので、さらなる暗号化は行われない（ステップ S2）。

【0072】

また、同期プログラム 46 により、端末装置 T1 は、当該暗号化ファイルをサーバ装置 S にアップロードする（ステップ S41）。サーバ装置 S は、これを受信して（ステップ 50

S 6 1)、記録する(ステップS 6 2)。すなわち、同期処理が行われる。図 6 においては、図 3 の処理のうち、ステップS 4 1、S 6 1、S 6 2のみを示している。

【0073】

したがって、ユーザは、ファイルを編集した後、上書き保存の操作を行うだけで、同期フォルダ50の暗号ファイルの更新、サーバ装置Sとの同期処理を行うことができる。

【0074】

図 6 に戻って、ステップS 1 3において、端末装置T1は、ユーザによる編集作業が終了したかどうかを判断する(ステップS 1 3)。一時的記憶領域に編集後ファイルが上書き保存されたとしても、依然として、ユーザが編集を継続している可能性もあるので、この判断が必要である。

10

【0075】

ここでは、端末装置T1は、当該ファイルに関連づけられたプログラムが終了(起動していない状態)した場合には、ユーザによる編集が終了したと判断する。なお、関連づけられたプログラムが複数起動している場合には、全てのプログラムが終了したときに、ユーザによる編集が終了したと判断してもよいし、当該ファイルに対応付けて起動したプログラムが終了すれば、ユーザによる編集が終了したと判断してもよい。

【0076】

ユーザによるファイルの編集が終了したと判断すると、端末装置T1は、一時的記憶領域の編集後ファイルを削除する(ステップS 1 4)。これにより、余分なファイルを残さないようにすることができる。

20

【0077】

なお、ユーザによる編集が終了していないと判断した場合には、端末装置T1は、ステップS 1 0に戻って処理を繰り返す。

【0078】

1.4その他の実施形態

(1)上記実施形態では、ステップSにおける、暗号化されたファイルであるかどうかの判断を、暗号化ファイルの内容の先頭に記述されている暗号化識別子に基づいて行っている。しかし、ファイルに付された拡張子、ファイルのインデックス情報などに基づいて判断するようにしてもよい。さらに、これらの要素を組み合わせで判断してもよい。

30

【0079】

(2)上記実施形態では、ステップS 1 3における、ユーザによる編集が終了したかどうかの判断を、関連するプログラムが終了したかどうかによって行っている。しかし、上記判断に加えて、あるいは上記判断に代えて、オペレーティングシステムに対するシャットダウンの指令が出た場合には、ユーザによる編集が終了したと判断するようにしてもよい。

【0080】

また、オペレーティングシステムに対するシャットダウンの指令が出た場合に、一時的記憶領域の全ての内容を削除するようにしてもよい。この場合、個々のファイルについて、ユーザによる編集が終了したかどうかを判断して削除する必要がない。

【0081】

40

(3)上記実施形態では、一次記憶領域のファイルが編集されて上書きされた場合、編集後のファイルを暗号化した後、同期フォルダ50の暗号化ファイルを更新するようにしている(図6のステップS 1 0～S 1 2)。しかし、編集後のファイルを暗号化せずに、一次記憶領域の元の暗号化ファイルに上書きするようにしてもよい。この場合には、図3において、ステップS 3にて暗号化が行われ、編集後の暗号化ファイルが同期フォルダ50に記録されることになる。

【0082】

(4)上記実施形態では、ステップS 2において、端末プログラム48によって暗号化されたファイルであるかどうかを判断している。したがって、他のプログラムによって暗号化されたファイルは、重ねて暗号化されることになる。二重に暗号化をしたくない場合には

50

、端末プログラム４８に限らずいずれかの暗号化プログラムによって暗号化されているかどうかを判断するようにしてもよい。この場合、内容やヘッダによって判断してもよいし、拡張子によって判断するようにしてもよい。

【００８３】

(5)上記変形例は、その本質に反しない限り、第２、第３の実施形態にも適用可能である。

【００８４】

２．第２の実施形態

2.1全体構成

10

図７に、第２の実施形態によるクラウド・ストレージ・システムの全体構成を示す。この実施形態においても、第１の実施形態と同じように、端末装置Ｔ１、Ｔ２・・・の同期記録領域１０にファイル実体を残す方法を前提として説明を進める。

【００８５】

端末装置Ｔ１において、ハードディスクなどの記録部に対するファイルの書込指令（新たなファイル記録やファイル更新）があると、暗号化書込手段６はこれを受領する。この実施形態では、暗号化書込手段６は、ハードディスク３６に対するドライバと同等のレイヤーにて動作するよう構成される。したがって、ファイル処理するアプリケーションは、特段の意識をすることなく、ハードディスク３６に対する書込を行っているとの認識で指令を出している。

20

【００８６】

暗号化書込手段６は、上記書込指令が、同期記録領域１０に対するものであるか否かを判断する。同期記録領域１０に対する書込指令であれば、ファイルを暗号化して、書き込みを行う。ユーザは、暗号化のための操作を別途行うことなく、同期記録領域１０に暗号化したファイル１３を記録することができる。

【００８７】

端末装置Ｔ１において、ハードディスクなどの記録部に対するファイルの読出指令があると、復号化読出手段２はこれを受領する。この実施形態では、復号化読出手段２は、ハードディスク３６に対するドライバと同等のレイヤーにて動作するよう構成される。

【００８８】

30

復号化読出手段２は、上記読出指令が、同期記録領域１０に対するものであるか否かを判断する。同期記録領域１０からの読み出しを行うための読出指令であれば、暗号化ファイル１３を読み出し、復号化を行う。

【００８９】

復号化したファイルは、平文ファイル１５として一時的記憶領域１４に保持される。関連プログラム起動手段４は、一時的記憶領域１４の平文ファイル１５に関連づけられたプログラムを起動する。したがって、ユーザは、復号化のための操作を別途行うことなく、同期記録領域１０の暗号化ファイル１３を復号化し、関連するプログラムを起動することができる。

【００９０】

40

上記のようにして、ユーザ操作の煩わしさをもたらすことなく、暗号化によるセキュリティを維持したクラウド・ストレージ・システムを実現できる。

【００９１】

2.2ハードウェア構成

端末装置Ｔ１、Ｔ２・・・、サーバ装置Ｓのハードウェア構成は、第１の実施形態と同様である。ただし、端末プログラム４８が、アプリケーションのレベルではなく、ドライバのレベルにて実装されている点が異なっている。

【００９２】

50

2.3処理内容

図8に、ファイル書き込みの際の処理を示す。たとえば、ユーザがファイルのアイコンを、同期フォルダ50にドロップしたとする。これを受けて、オペレーティングシステム44は、書込指令を発する。端末プログラム48は、オペレーティングシステム44から、ハードディスク36に対するファイルの書込指令を受け取ると（ステップS15）、その書込指令が同期フォルダ50に対するものであるかを判断する（ステップS16）。

【0093】

同期フォルダ50に対する書き込みであるか否かは、オペレーティングシステム44からの書込指令の内容をみれば判断できる。すなわち、書込指令には、書込先のフォルダ名が含まれているからである。

【0094】

書込指令が同期フォルダ50に対するものでなければ、当該ファイルをハードディスク36に記録する（ステップS3）。書込指令が同期フォルダ50に対するものであれば、当該ファイルを暗号化した後（ステップS3）、ハードディスク36に記録する（ステップS3）。

【0095】

同期フォルダ50に対して暗号化ファイルが書き込まれると、同期プログラム46が処理を開始する。端末装置T1は、当該暗号化ファイルをサーバ装置Sにアップロードする（ステップS41）。サーバ装置Sは、これを受信して（ステップS61）、記録する（ステップS62）。すなわち、同期処理が行われる。

【0096】

したがって、ユーザは、暗号化処理を意識しなくとも、同期フォルダ50に対する書き込みにおいては、自動的に暗号化処理が行われる。

【0097】

図9、図6に、ファイル読み出し・更新のフローチャートを示す。たとえば、ユーザが同期フォルダ50内のファイルのアイコンを、ダブルクリックしたとする。これを受けて、オペレーティングシステム44は、読出指令を発する。端末プログラム48は、オペレーティングシステム44から、ハードディスク36に対するファイルの読出指令を受け取ると（ステップS17）、当該ファイルを読み出す（ステップS6）。

【0098】

次に、端末装置T1は、読出指令が同期フォルダ50に対するものであるかを判断する（ステップS18）。同期フォルダ50に対する読み出しであるか否かは、オペレーティングシステム44からの読出指令の内容をみれば判断できる。すなわち、読出指令には、読出先のフォルダ名が含まれているからである。

【0099】

読出指令が同期フォルダ50に対するものでなければ、当該ファイルに対応するプログラムを起動する（ステップS9）。読出指令が同期フォルダ50に対するものであれば、当該ファイルを復号化した後（ステップS7）、ハードディスク36の一時的記憶領域に格納する（ステップS8）。この際、暗号化ファイルのファイル名を、元のファイルのファイル名に変更して格納する。たとえば、暗号化ファイルのファイル名がPatent.zdcであれば、元のファイル名Patent.jtdに戻して格納する。

【0100】

次に、端末装置T1は、復号化したファイルに対応するプログラムを起動し、当該ファイルを開く（ステップS9）。なお、既に対応するプログラムが起動している場合には、プログラムは新たに起動しなくてもよい。

【0101】

したがって、ユーザは、同期フォルダ50内のファイルをダブルクリックするだけで、復号化されたファイルが、対応するプログラムによって開かれ、編集を行うことができる。

【0102】

10

20

30

40

50

ファイルが開かれ編集された後の処理は、第1の実施形態における処理（図6参照）と同様である。すなわち、ファイルが編集されて上書きされるごとに、サーバ装置Sとの同期処理が実行される。

【0103】

3. 第3の実施形態

3.1全体構成

図10に、第3の実施によるクラウド・ストレージ・システムの全体構成を示す。この実施形態においては、端末装置T1、T2・・・の同期記録領域10にファイル実体を残さず、同期をとったときにサーバ装置Sの側にのみファイル実体を残す方法を前提としたシステムについて説明する。この方法のシステムの場合、端末装置T1、T2・・・の同期記録領域10には、サーバ装置のファイル実体に関連づけられた仮体ファイルが記録される。

10

【0104】

端末装置T1において、ハードディスクなどの記録部に対するファイルの書込指令（新たなファイル記録やファイル更新）があると、暗号化書込手段6はこれを受領する。この実施形態では、暗号化書込手段6は、ハードディスク36に対するドライバと同等のレイヤーにて動作するよう構成される。したがって、ファイル処理するアプリケーションは、特段の意識をすることなく、ハードディスク36に対する書込を行っているとの認識で指令を出している。

20

【0105】

暗号化書込手段6は、上記書込指令が、同期記録領域10に対するものであるか否かを判断する。同期記録領域10に対する書込指令であれば、ファイルを暗号化して、書き込みを行う。ユーザは、暗号化のための操作を別途行うことなく、同期記録領域10に暗号化したファイル13を記録することができる。

【0106】

同期記録領域10に暗号化ファイル13が記録されると、同期手段（図示せず）により、サーバ装置Sの同期記録領域20との間で同期処理が実行される。この同期処理において、暗号化ファイル13は、サーバ装置Sの同期記録領域20にアップロードされ、暗号化実体ファイル22として記録される。その際、端末装置T1の同期記録領域10の暗号化ファイル13は削除され、仮体ファイル17に置き換えられる。仮体ファイル17は、暗号化実体ファイル22に関連づけられており、暗号化実体ファイル22を呼び出すためのものである。

30

【0107】

端末装置T1において、ハードディスクなどの記録部に対するファイルの読出指令があると、復号化読出手段2はこれを受領する。この実施形態では、復号化読出手段2は、ハードディスク36に対するドライバと同等のレイヤーにて動作するよう構成される。

【0108】

復号化読出手段2は、上記読出指令が、同期記録領域10に対するものであるか否かを判断する。同期記録領域10からの読み出しを行うための読出指令であれば、以下のような処理がなされる。

40

【0109】

同期記録領域10の仮体ファイル17を読に出す指令である場合、同期手段（図示せず）は、読み出された仮体ファイル17に基づいて、関連づけられている暗号化実体ファイル22をサーバ装置Sからダウンロードし、同期記録領域10に記録する。この暗号化実体ファイル22の書き込みは、同期記録領域10に対する書込指令であるから、暗号化書込手段6によって処理されることになる。

【0110】

前述のように、暗号化書込手段6は、同期記録領域10に対する書き込みの際には、ファイルを暗号化して書き込むものである。しかし、同期処理によるサーバ装置Sからのダ

50

ウンロードにおいては、既に暗号化されたファイルを、同期記録領域 10 に戻すものであるから、重ねて暗号化を行うべきではない。そこで、この実施形態では、同期手段からの書込指令の場合には、当該ファイルを暗号化せず、同期記録領域 10 に書き込むようにしている。したがって、同期記録領域 10 には、暗号化実体ファイル 22 が暗号化ファイル 13 として復元されることになる。

【0111】

複合化読出手段 2 は、この暗号化ファイル 13 を読み出し、復号化を行う。復号化したファイルは、平文ファイル 15 として一時的記憶領域 14 に保持される。関連プログラム起動手段 4 は、一時的記憶領域 14 の平文ファイル 15 に関連づけられたプログラムを起動する。したがって、ユーザは、復号化のための操作を別途行うことなく、同期記録領域 10 の暗号化ファイル 13 を復号化し、関連するプログラムを起動することができる。

10

【0112】

上記のようにして、ユーザ操作の煩わしさをもたらすことなく、暗号化によるセキュリティを維持したクラウド・ストレージ・システムを実現できる。

【0113】

2.2 ハードウェア構成

端末装置 T1、T2・・・、サーバ装置 S のハードウェア構成は、第 1 の実施形態と同様である。ただし、端末プログラム 48 が、アプリケーションのレベルではなく、ドライバのレベルにて実装されている点が異なっている。

20

【0114】

3.3 処理内容

図 11 に、ファイル書き込みの際の処理を示す。たとえば、ユーザがファイルのアイコンを、同期フォルダ 50 にドロップしたとする。これを受けて、端末プログラム 48 が、当該ファイルを暗号化し、ハードディスク 36 の同期フォルダ 50 に記録する処理は、第 2 の実施形態と同様である（ステップ S15、S16、S3、S4）。

【0115】

ただし、同期フォルダ 50 への書き込みが、実体取得処理によるものである場合には、ファイルの暗号化（ステップ S3）は行わずに書き込みを行う。ここでは、実体取得処理ではないので、ファイルを暗号化して書き込むことになる。

30

【0116】

同期フォルダ 50 に対して暗号化ファイルが書き込まれると、同期プログラム 46 が処理を開始する。端末装置 T1 は、当該暗号化ファイルをサーバ装置 S にアップロードする（ステップ S41）。サーバ装置 S は、これを受信して（ステップ S61）、記録する（ステップ S62）。

【0117】

さらに、端末装置 T1 は、同期フォルダ 50 の暗号化ファイルを仮体ファイルに置き換える（ステップ S42）。つまり、ファイルの実体は、サーバ装置 S に置かれ、端末装置 T1 には、これに関連づけられた仮体ファイルが記録される。このようにして、同期処理が行われる。

40

【0118】

したがって、ユーザは、暗号化処理を意識しなくとも、同期フォルダ 50 に対する書き込みにおいては、自動的に暗号化処理が行われる。

【0119】

図 12、図 13、図 14 に、ファイル読み出し・更新のフローチャートを示す。たとえば、ユーザが同期フォルダ 50 内の仮体ファイルのアイコンを、ダブルクリックしたとする。これを受けて、オペレーティングシステム 44 は、読出指令を発する。端末プログラム 48 は、オペレーティングシステム 44 から、ハードディスク 36 に対するファイルの読出指令を受け取ると（ステップ S17）、これを同期プログラム 46 に伝える。つまり

50

、同期プログラム 4 6 に対し、仮体ファイルに対応する実体取得指令を与える（ステップ S 2 0）。

【0 1 2 0】

同期プログラム 4 6 により、端末装置 T1 は、この指令を受けて、サーバ装置 S に対して、暗号化実体ファイルのダウンロードを要求する（ステップ S 4 5）。サーバ装置 S は、これを受けて、仮体ファイルに対応する暗号化実体ファイルを送信する（ステップ S 1 8）。

【0 1 2 1】

同期プログラム 4 6 によって、端末装置 T1 は、ダウンロードした暗号化実体ファイルを、同期フォルダ 5 0 に書き込む指令をオペレーティングシステムに与える（ステップ S 4 6）。この書込指令は、オペレーティングシステムから端末プログラム 4 8 に与えられる。したがって、前記の図 1 1 の書き込み処理が実行されることになる。この際、暗号化実体ファイルの同期フォルダ 5 0 への書き込みは、実体取得処理によるものであるから、暗号化は行わずに書き込みが行われる（図 1 1 のステップ S 1 9 参照）。

【0 1 2 2】

暗号化実体ファイルが同期フォルダ 5 0 に書き込まれると、端末プログラム 4 8 によって、端末装置 T1 は、当該ファイルを読み出す（図 1 3 のステップ S 6）。

【0 1 2 3】

次に、端末装置 T1 は、ステップ S 1 7 における読出指令が同期フォルダ 5 0 に対するものであるかを判断する（ステップ S 1 8）。

【0 1 2 4】

読出指令が同期フォルダ 5 0 に対するものでなければ、当該ファイルに対応するプログラムを起動する（ステップ S 9）。読出指令が同期フォルダ 5 0 に対するものであれば、当該ファイルを復号化した後（ステップ S 7）、ハードディスク 3 6 の一時的記憶領域に格納する（ステップ S 8）。この際、暗号化ファイルのファイル名を、元のファイルのファイル名に変更して格納する。

【0 1 2 5】

次に、端末装置 T1 は、復号化したファイルに対応するプログラムを起動し、当該ファイルを開く（ステップ S 9）。

【0 1 2 6】

したがって、ユーザは、同期フォルダ 5 0 内のファイルをダブルクリックするだけで、復号化されたファイルが、対応するプログラムによって開かれ、編集を行うことができる。

【0 1 2 7】

端末プログラム 4 8 は、ハードディスク一時的記憶領域のファイル内容が変更されたかどうかを監視している（ステップ S 1 0）。つまり、ユーザが一時的記憶領域のファイルを編集し、編集後のファイルを上書きしたかどうかを監視している。

【0 1 2 8】

一時的記憶領域のファイル内容が変化したことを検出すると、端末装置 T1 は、一時的記憶領域に保存された編集後ファイルを読み出して暗号化する（ステップ S 1 1）。続いて、端末装置 T1 は、この暗号化された編集後ファイルを、同期フォルダ 5 0 に書き込む（ステップ S 1 2）。

【0 1 2 9】

これにより、同期フォルダ 5 0 内の暗号化ファイルの内容が変更されることになる。同期プログラム 4 6 は、この変更によって処理を開始する。同期プログラム 4 6 により、端末装置 T1 は、当該暗号化ファイルをサーバ装置 S にアップロードする（ステップ S 4 1）。サーバ装置 S は、これを受信して（ステップ S 6 1）、記録する（ステップ S 6 2）。すなわち、同期処理が行われる。

【0 1 3 0】

また、同期プログラム 4 6 の処理により、端末装置 T1 は、同期フォルダ 5 0 の暗号化

10

20

30

40

50

ファイルを仮体ファイルに置き換える（ステップS 4 2）。

【0131】

したがって、ユーザは、ファイルを編集した後、上書き保存の操作を行うだけで、同期フォルダ50の暗号ファイルの更新、サーバ装置Sとの同期処理を行うことができる。

【0132】

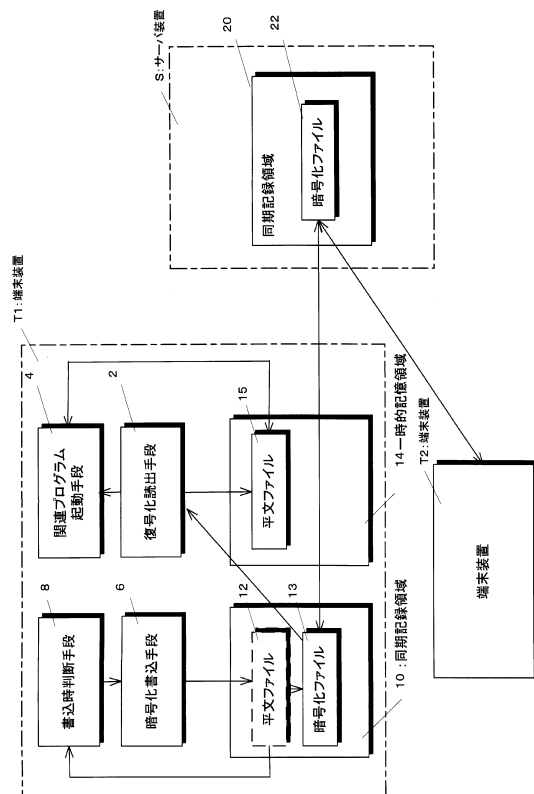
ステップS 1 3において、端末装置T1は、ユーザによる編集作業が終了したかどうかを判断する（ステップS 1 3）。ユーザによるファイルの編集が終了したと判断すると、端末装置T1は、一時的記憶領域の編集後ファイルを削除する（ステップS 1 4）。これにより、余分なファイルを残さないようにすることができる。

【0133】

なお、ユーザによる編集が終了していないと判断した場合には、端末装置T1は、ステップS 1 0に戻って処理を繰り返す。

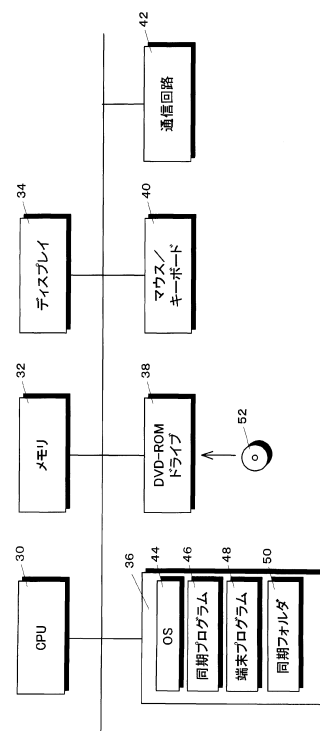
10

【図1】



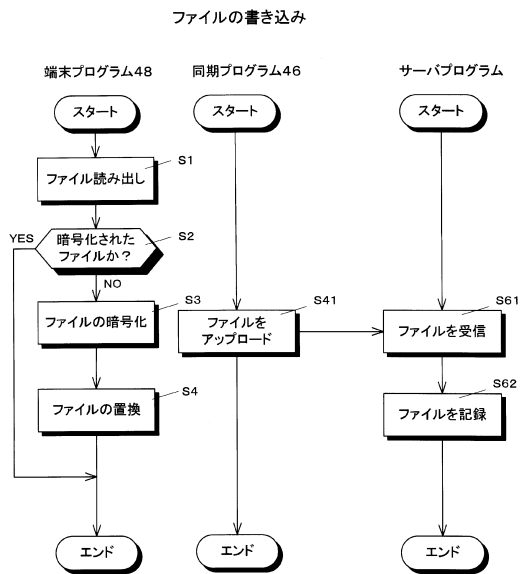
HS09201

【図2】



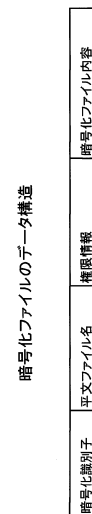
HS09202

【図 3】



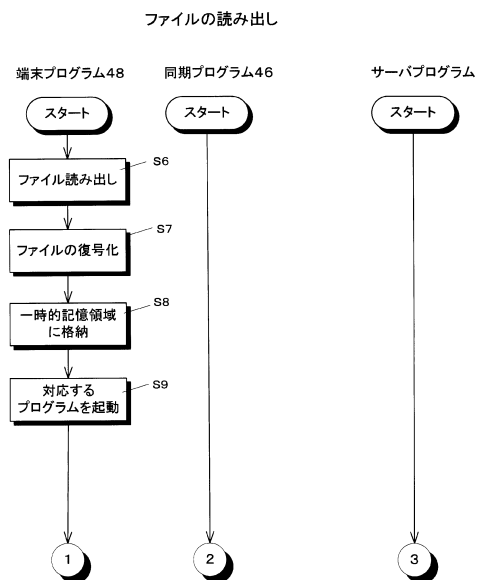
HSS09203

【図 4】



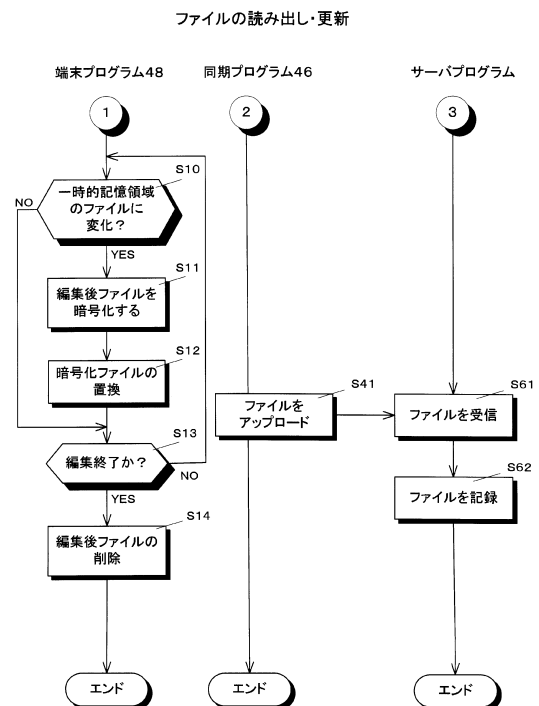
HSS09204

【図 5】



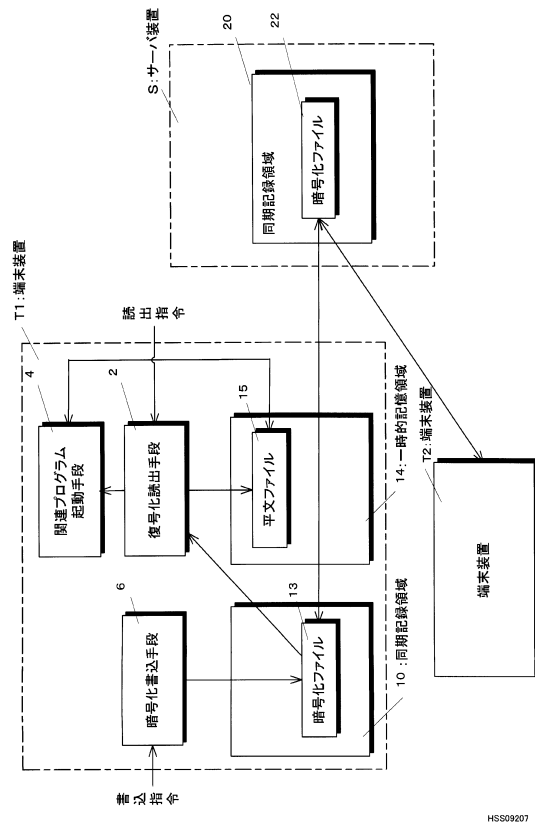
HSS09205

【図 6】

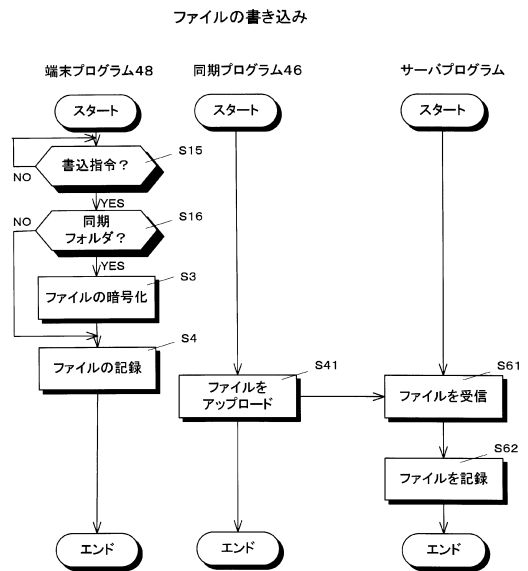


HSS09206

【図 7】

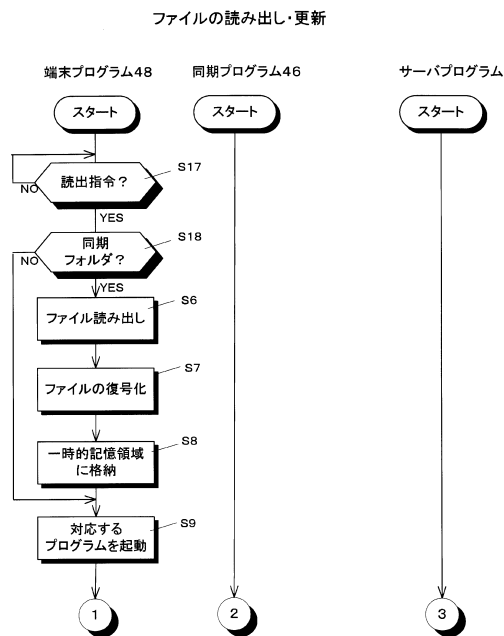


【図 8】



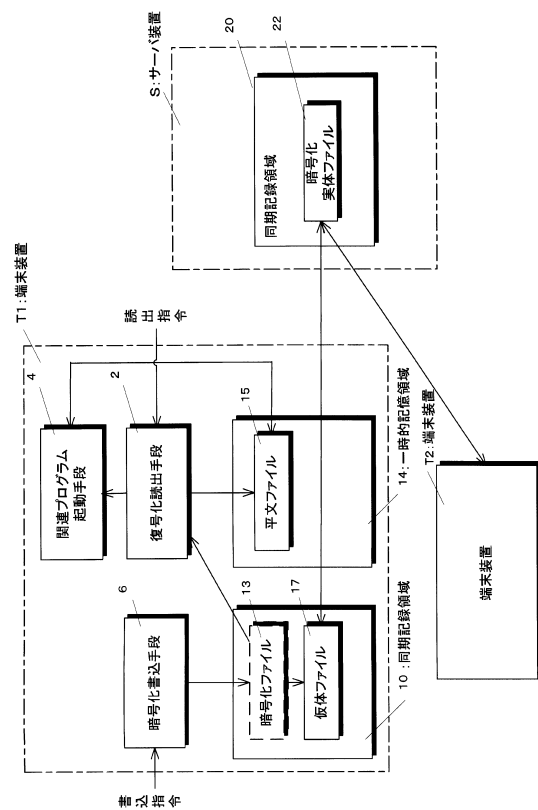
HSS09208

【図 9】



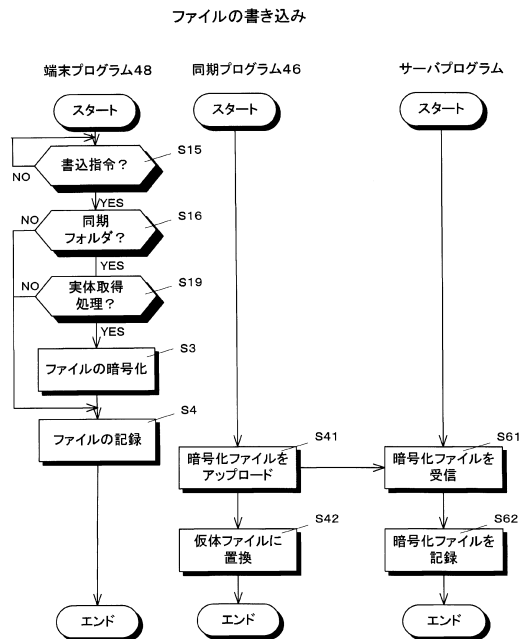
HSS09209

【図 10】



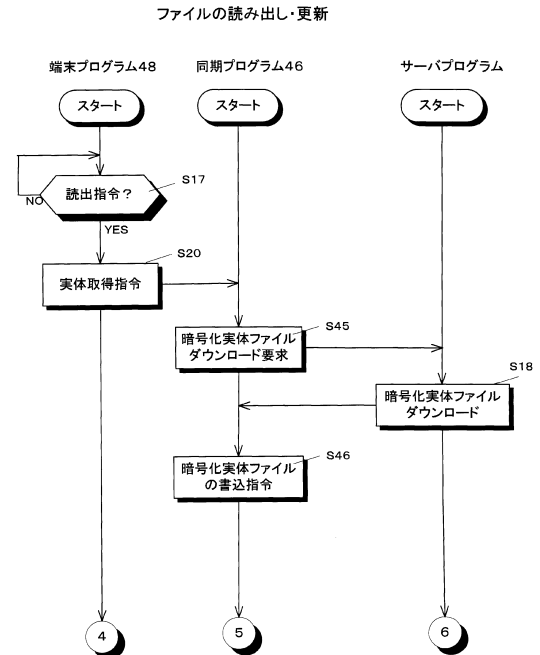
HSS092010

【図 1 1】



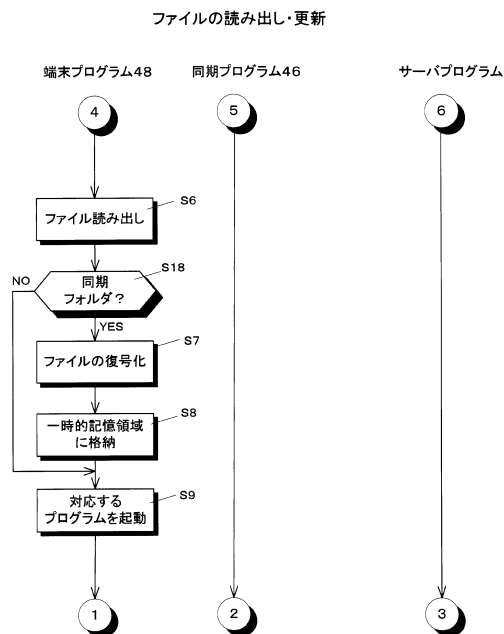
HSS09211

【図 1 2】



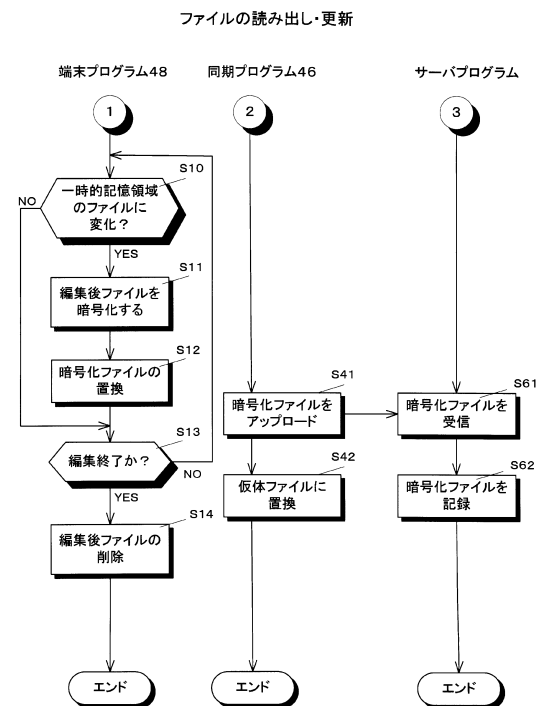
HSS09212

【図 1 3】



HSS09213

【図 1 4】



HSS092014

フロントページの続き

(56)参考文献 特開2010-266933 (JP, A)
特開2008-134821 (JP, A)
特開2008-123049 (JP, A)

(58)調査した分野(Int.Cl., DB名)
G06F 12/00
G06F 21/60-21/62
G09C 1/00