

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B1)

(11) 特許番号

特許第4385111号
(P4385111)

(45) 発行日 平成21年12月16日(2009.12.16)

(24) 登録日 平成21年10月9日(2009.10.9)

(51) Int.Cl.		F I
G06F 21/24	(2006.01)	G06F 12/14 510F
G06F 12/00	(2006.01)	G06F 12/00 531M
G06F 13/00	(2006.01)	G06F 12/00 531D
		G06F 13/00 520B
		G06F 12/00 545A

請求項の数 2 (全 15 頁)

(21) 出願番号	特願2008-262704 (P2008-262704)	(73) 特許権者	800000068
(22) 出願日	平成20年10月9日(2008.10.9)		学校法人東京電機大学
審査請求日	平成21年1月23日(2009.1.23)		東京都千代田区神田錦町2-2
早期審査対象出願		(74) 代理人	100119677
			弁理士 岡田 賢治
		(74) 代理人	100115794
			弁理士 今下 勝博
		(72) 発明者	官保 憲治
			東京都千代田区神田錦町2-2 学校法人
			東京電機大学内
		(72) 発明者	上野 洋一郎
			東京都千代田区神田錦町2-2 学校法人
			東京電機大学内

最終頁に続く

(54) 【発明の名称】 セキュリティレベル制御ネットワークシステム

(57) 【特許請求の範囲】

【請求項1】

通信ネットワークで接続されたデータファイル保有サーバ、データ配信サーバ及び監視サーバと、前記データ配信サーバと通信ネットワークで接続された複数のクライアント端末と、を備えるセキュリティレベル制御ネットワークシステムであって、

前記データファイル保有サーバは、

保有しているデータファイルの分割数及び複製数が定められたセキュリティレベルを前記データ配信サーバに通知するセキュリティレベル通知手段と、

前記データファイルを前記データ配信サーバに送信するデータファイル送信手段と、を備え、

前記データ配信サーバは、

前記データファイル送信手段からのデータファイルを受信するデータ配信サーバ受信手段と、

前記データ配信サーバ受信手段の受信するデータファイルを格納するデータ配信サーバ格納手段と、

前記セキュリティレベル通知手段からセキュリティレベルを取得すると、取得したセキュリティレベルで定められた前記データファイルの分割数及び複製数を決定するとともに前記分割数及び前記複製数によって生成されるデータピースの総数を決定するセキュリティレベル決定手段と、

前記データ配信サーバ格納手段からデータファイルを取得し、取得したデータファイル

を暗号化する暗号化手段と、

前記暗号化手段の暗号化したデータファイルを複数のデータピースに分割してデータピース同士を可逆演算することで一体化処理を行なう一体化手段と、

前記一体化手段の一体化処理を行なったデータファイルを取得し、取得した当該データファイルを前記セキュリティレベル決定手段の決定する分割数に分割する分割手段と、

前記分割手段から前記データピースを取得し、取得した前記データピースのそれぞれを前記セキュリティレベル決定手段の決定する複製数に複製する複製手段と、

前記複製手段の複製したデータピースを、前記複数のクライアント端末に分散して送信するデータピース送信手段と、を備え、

前記複数のクライアント端末は、

前記データ配信サーバからのデータピースを格納可能であるか否かの判定を指示する応答要求を前記監視サーバから受けると、前記データ配信サーバからのデータピースを格納可能であるか否かを判定し、当該判定結果を前記監視サーバに返信する応答手段と、

前記データピース送信手段からのデータピースを受信するクライアント端末受信手段と

、
前記クライアント端末受信手段の受信するデータピースを格納するクライアント端末格納手段と、を備え、

前記監視サーバは、

前記複数のクライアント端末に、前記応答要求を送信し、前記応答手段からの判定結果を収集して、前記クライアント端末のそれぞれがデータピースを受信可能な状態であるか否かをリスト化するクライアント端末リスト作成手段と、

前記クライアント端末リスト作成手段の作成するクライアント端末リストを、前記データ配信サーバから参照可能な状態で格納するクライアント端末リスト格納手段と、を備え

、
前記データ配信サーバにおける前記セキュリティレベル決定手段は、

前記クライアント端末リスト格納手段の格納するクライアント端末リストからデータピースを受信可能な状態の前記クライアント端末の数を取得し、

取得したデータピースを受信可能な状態の前記クライアント端末の数が自己の決定したデータピースの総数以上であるか否かを判定し、

取得したデータピースを受信可能な状態の前記クライアント端末の数が自己の決定した前記データピースの総数以上である場合は、前記分割手段に前記分割数を出力するとともに前記複製手段に前記複製数を出力し、

取得したデータピースを受信可能な状態の前記クライアント端末の数が自己の決定した前記データピースの総数未満である場合は、前記データファイル保有サーバに、通知のあったセキュリティレベルが実施不可能である旨を通知することを特徴とするセキュリティレベル制御ネットワークシステム。

【請求項2】

前記データファイル保有サーバ及び前記データ配信サーバと通信ネットワークで接続されたウェブサーバをさらに備え、

前記データファイル保有サーバは、前記データファイル保有サーバ固有の情報及び予め定められたセキュリティレベルを格納するデータファイル保有サーバ認証手段をさらに備え、

前記セキュリティレベル通知手段は、前記データファイル保有サーバ認証手段に格納されている前記データファイル保有サーバ固有の情報及び前記セキュリティレベルを前記ウェブサーバに通知し、

前記ウェブサーバは、

前記データファイル保有サーバ固有の情報を予め格納する固有情報格納手段と、

前記セキュリティレベル通知手段からの前記データファイル保有サーバ固有の情報を受信すると、受信した前記固有の情報が前記固有情報格納手段に格納されているか否かを判定するウェブサーバ認証手段と、

10

20

30

40

50

前記セキュリティレベル通知手段からの前記データファイル保有サーバ固有の情報が前記固有情報格納手段に格納されていると前記ウェブサーバ認証手段が判定すると、前記セキュリティレベル通知手段からの前記セキュリティレベルを、前記データ配信サーバに通知するセキュリティレベル転送手段と、を備え、

前記セキュリティレベル決定手段は、前記セキュリティレベル転送手段からセキュリティレベルを取得することを特徴とする請求項1に記載のセキュリティレベル制御ネットワークシステム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、データファイルをバックアップするネットワークシステムに関し、特に、ディザスタリカバリ技術を用いて暗号レベル及びデータファイルの復元確率を管理ユーザが随意に変更できるネットワーク技術に関する。

【背景技術】

【0002】

現在、使用される社会インフラを構成するための各種システム構築に係る情報や各種の個人情報等のデータベース化が進んでいる。地方自治体や病院などの公共施設においても例外ではなく、住民の個人情報や医療情報といった各種のデータファイルを格納するデータベースを、災害時に迅速に復旧するためのバックアップが求められ、システムの障害がもたらす損失を減らすために、種々のバックアップシステムが提案されている。

【0003】

例えば、主及び副の2つのサイトを用意し、通信ネットワークを介して副サイトへデータファイルをバックアップするためのシステムや、GRID技術を用いて大規模データファイルをバックアップするためのシステムが提案されている(例えば、特許文献1参照)。また、データファイルを分割し、当該分割されたデータピースを暗号化した後に、非常に多くのクライアント端末に分散転送するバックアップ技術が提案されている。

【特許文献1】特開2006-67412号公報

【発明の開示】

【発明が解決しようとする課題】

【0004】

従来方式では、有限なネットワークリソースを対象としており、ネットワークリソースが時々刻々と変動することまでは考慮されていなかった。このため、データファイルを保有する管理ユーザのサービス要求に見合うセキュリティレベルが保証できてない状況が起こりえた。

【0005】

特に災害発生の予報や警報が通知された場合には、データファイルのバックアップを要求する管理ユーザ数が急激に増えることが予想される。この場合にはバックアップを行うためのデータファイル容量が急激に増えるので、すべてのデータファイルに対して最高度のセキュリティレベルを保証することは困難である。

【0006】

一方、データファイルを分割し、当該分割されたデータピースを暗号化した後に、非常に多くのクライアント端末に分散転送するバックアップ技術では、事実上、データファイルの分割数に応じてセキュリティレベルが決定されることになる。

【0007】

そこで、本発明は、データファイルを分割し、当該分割されたデータピースを複数のクライアント端末に分散転送するバックアップ技術を用い、データファイルを保有する管理ユーザのサービス要求に見合ったセキュリティレベルでのバックアップを可能にすることを目的とする。

【課題を解決するための手段】

【0008】

10

20

30

40

50

上記課題を解決するために、本発明に係るセキュリティレベル制御ネットワークシステムは、データファイルを分割し、当該分割したデータピースを分散して送信するデータ配信サーバに、セキュリティレベルに応じてデータファイルの分割数を制御するセキュリティレベル決定手段を設けたことを特徴とする。これにより、管理ユーザがデータ配信サーバに対してセキュリティレベルを指示することで、管理ユーザの変動するサービス要求に見合ったセキュリティレベルでデータファイルのバックアップが可能となる。

【0009】

具体的には、本発明に係るセキュリティレベル制御ネットワークシステムは、通信ネットワークで接続されたデータファイル保有サーバ、データ配信サーバ及び監視サーバと、前記データ配信サーバと通信ネットワークで接続された複数のクライアント端末と、を備えるセキュリティレベル制御ネットワークシステムであって、

10

前記データファイル保有サーバは、保有しているデータファイルの分割数及び複製数が定められたセキュリティレベルを前記データ配信サーバに通知するセキュリティレベル通知手段と、前記データファイルを前記データ配信サーバに送信するデータファイル送信手段と、を備え、

前記データ配信サーバは、前記データファイル送信手段からのデータファイルを受信するデータ配信サーバ受信手段と、前記データ配信サーバ受信手段の受信するデータファイルを格納するデータ配信サーバ格納手段と、前記セキュリティレベル通知手段からセキュリティレベルを取得すると、取得したセキュリティレベルで定められた前記データファイルの分割数及び複製数を決定するとともに前記分割数及び前記複製数によって生成されるデータピースの総数を決定するセキュリティレベル決定手段と、前記データ配信サーバ格納手段からデータファイルを取得し、取得したデータファイルを暗号化する暗号化手段と、前記暗号化手段の暗号化したデータファイルを一体化する一体化手段と、前記一体化手段の一体化したデータファイルを取得し、取得した当該データファイルを前記セキュリティレベル決定手段の決定する分割数に分割する分割手段と、前記分割手段から前記データピースを取得し、取得した前記データピースのそれぞれを前記セキュリティレベル決定手段の決定する複製数に複製する複製手段と、

20

前記複製手段の複製したデータピースを、前記複数のクライアント端末に分散して送信するデータピース送信手段と、を備え、

前記複数のクライアント端末は、前記データ配信サーバからのデータピースを格納可能であるか否かの判定を指示する応答要求を前記監視サーバから受けると、前記データ配信サーバからのデータピースを格納可能であるか否かを判定し、当該判定結果を前記監視サーバに返信する応答手段と、前記データピース送信手段からのデータピースを受信するクライアント端末受信手段と、前記クライアント端末受信手段の受信するデータピースを格納するクライアント端末格納手段と、を備え、

30

前記監視サーバは、前記複数のクライアント端末に、前記応答要求を送信し、前記応答手段からの判定結果を収集して、前記クライアント端末のそれぞれがデータピースを受信可能な状態であるか否かをリスト化するクライアント端末リスト作成手段と、前記クライアント端末リスト作成手段の作成するクライアント端末リストを、前記データ配信サーバから参照可能な状態で格納するクライアント端末リスト格納手段と、を備え、

40

前記データ配信サーバにおける前記セキュリティレベル決定手段は、前記クライアント端末リスト格納手段の格納するクライアント端末リストからデータピースを受信可能な状態の前記クライアント端末の数を取得し、取得したデータピースを受信可能な状態の前記クライアント端末の数が自己の決定したデータピースの総数以上であるか否かを判定し、取得したデータピースを受信可能な状態の前記クライアント端末の数が自己の決定した前記データピースの総数以上である場合は、前記分割手段に前記分割数を出力するとともに前記複製手段に前記複製数を出力し、取得したデータピースを受信可能な状態の前記クライアント端末の数が自己の決定した前記データピースの総数未満である場合は、前記データファイル保有サーバに、通知のあったセキュリティレベルが実施不可能である旨を通知することを特徴とする。

50

【 0 0 1 0 】

分割手段でのデータファイルの分割数を増減すれば、セキュリティレベルの高低を調整することができる。そこで、本発明に係るセキュリティレベル制御ネットワークシステムでは、データファイル保有サーバがセキュリティレベル通知手段を備え、データ配信サーバがセキュリティレベル決定手段を備える。これにより、データファイル保有サーバの通知するセキュリティレベルに応じてデータファイルの分割数を増減させることができるので、管理ユーザのサービス要求に見合ったセキュリティレベルでのバックアップを可能にすることができる。

【 0 0 1 1 】

分割手段が分割したデータピースの複製数を増減すれば、データファイルの復元確率を調整することができる。そこで、本発明に係るセキュリティレベル制御ネットワークシステムでは、データ配信サーバが複製手段をさらに備え、セキュリティレベル決定手段は、データファイル保有サーバの通知するセキュリティレベルに応じてデータピースの複製数を増減させる。これにより、管理ユーザのサービス要求に見合ったデータファイルの復元確率でのバックアップを可能にすることができる。

10

【 0 0 1 2 】

それぞれのクライアント端末が応答手段を備え、監視サーバがクライアント端末リスト作成手段を備え、データ配信サーバのセキュリティレベル決定手段はクライアント端末リストに基づいてセキュリティレベルが十分か否かを判定する。これにより、データファイル保有サーバの通知するセキュリティレベルを確保することができる。また、遊休状態にあるクライアント端末を有効活用したバックアップシステムを構築することができる。

20

【 0 0 1 3 】

本発明に係るセキュリティレベル制御ネットワークシステムでは、前記データファイル保有サーバ及び前記データ配信サーバと通信ネットワークで接続されたウェブサーバをさらに備え、

前記データファイル保有サーバは、前記データファイル保有サーバ固有の情報及び予め定められたセキュリティレベルを格納するデータファイル保有サーバ認証手段をさらに備え、

前記セキュリティレベル通知手段は、前記データファイル保有サーバ認証手段に格納されている前記データファイル保有サーバ固有の情報及び前記セキュリティレベルを前記ウェブサーバに通知し、

30

前記ウェブサーバは、

前記データファイル保有サーバ固有の情報を予め格納する固有情報格納手段と、前記セキュリティレベル通知手段からの前記データファイル保有サーバ固有の情報を受信すると、受信した前記固有の情報が前記固有情報格納手段に格納されているか否かを判定するウェブサーバ認証手段と、前記セキュリティレベル通知手段からの前記データファイル保有サーバ固有の情報が前記固有情報格納手段に格納されていると前記ウェブサーバ認証手段が判定すると、前記セキュリティレベル通知手段からの前記セキュリティレベルを、前記データ配信サーバに通知するセキュリティレベル転送手段と、を備え、

前記セキュリティレベル決定手段は、前記セキュリティレベル転送手段からセキュリティレベルを取得することが好ましい。

40

本発明に係るセキュリティレベル制御ネットワークシステムでは、ウェブサーバをさらに備え、データファイル保有サーバがデータファイル保有サーバ認証手段をさらに備えるので、管理ユーザの意に反してセキュリティレベルが変更されることを防ぎ、データファイル保有サーバ認証手段に応じたセキュリティレベルを確保することができる。

【 発明の効果 】

【 0 0 1 4 】

本発明によれば、データファイルを分割し、当該分割されたデータピースを暗号化した後に、非常に多くのクライアント端末に分散転送するバックアップ技術を用い、管理ユーザのサービス要求に見合ったセキュリティレベルでのバックアップが可能となる。

50

【発明を実施するための最良の形態】

【0015】

添付の図面を参照して本発明の実施の形態を説明する。以下に説明する実施の形態は本発明の構成の例であり、本発明は、以下の実施の形態に制限されるものではない。

【0016】

図1は、本実施形態に係るセキュリティレベル制御ネットワークシステムの構成概略図である。本実施形態に係るセキュリティレベル制御ネットワークシステムは、データファイル保有サーバ10と、データ配信サーバ20と、複数のクライアント端末30と、監視サーバ40と、ウェブサーバ50と、を備える。

【0017】

データファイル保有サーバ10とデータ配信サーバ20は通信ネットワーク100で接続される。データ配信サーバ20と複数のクライアント端末30は通信ネットワーク100で接続される。データファイル保有サーバ10とウェブサーバ50は通信ネットワーク100で接続される。データ配信サーバ20と監視サーバ40は通信ネットワーク100で接続される。監視サーバ40と複数のクライアント端末30は通信ネットワーク100で接続される。データ配信サーバ20とウェブサーバ50は直接接続される。実際には、ウェブサーバ50は、データセンタ内でLAN(Local Area Network)によりウェブサーバ50と結合されている場合や、または、データセンタとは、全く別の地理的な場所にあり、WAN(Wide Area Network)のような広域ネットワークまたはインターネットによってウェブサーバ50と結合されている場合もあり

【0018】

ここで、通信ネットワーク100は共通のネットワークを用いてもよいし、いずれかが独立していてもよい。例えば、データファイル保有サーバ10とデータ配信サーバ20を接続する通信ネットワーク100は、データファイルを伝送するので専用線であることが好ましい。また、データ配信サーバ20と監視サーバ40を接続する通信ネットワーク100は、秘匿性の要求されるクライアント端末リストを伝送するので専用線であることが好ましい。また、本実施形態では、データ配信サーバ20とウェブサーバ50は直接接続される例を示したが、通信ネットワーク100を介して接続されていてもよい。また、データファイル保有サーバ10と、データ配信サーバ20と、複数のクライアント端末30と、監視サーバ40と、ウェブサーバ50と、のうちの、任意の組み合わせから成る複数が一体化され、1つの構成となってもよい。

【0019】

一般に、バックアップ対象となっているデータファイルの分割数やデータピースの複製数に応じた、決定される暗号レベル及び復元確率の値は決定される。そこで、本実施形態に係るセキュリティレベル制御ネットワークシステムではこの点に着目し、管理ユーザが支払うバックアップ費用に見合う形態で、随意にセキュリティレベル及び復元確率を変更するためのネットワークメカニズムを組み込むことを特徴とする。本実施形態に係るセキュリティレベル制御ネットワークシステムの詳細な構成の一例を、図2、図3、図4、図5及び図6を用いて説明する。

【0020】

図2は、データファイル保有サーバ10の一例を示す概略構成図である。データファイル保有サーバ10は、データファイル格納手段11と、セキュリティレベル通知手段12と、データファイル送信手段13と、入力手段14と、データファイル保有サーバ認証手段15と、を備える。

【0021】

図3は、データ配信サーバ20の一例を示す概略構成図である。データ配信サーバ20は、データ配信サーバ受信手段21と、データ配信サーバ格納手段22と、セキュリティレベル決定手段23と、分割手段24と、データピース送信手段25と、複製手段26と、暗号化手段27と、一体化手段28と、を備える。

【 0 0 2 2 】

図 4 は、クライアント端末 3 0 の一例を示す概略構成図である。それぞれのクライアント端末 3 0 は、クライアント端末受信手段 3 1 と、クライアント端末格納手段 3 2 と、応答手段 3 3 と、を備える。図 5 は、監視サーバ 4 0 の一例を示す概略構成図である。監視サーバ 4 0 は、クライアント端末リスト作成手段 4 1 と、クライアント端末リスト格納手段 4 2 と、を備える。図 6 は、ウェブサーバ 5 0 の一例を示す概略構成図である。ウェブサーバ 5 0 は、固有情報格納手段 5 1 と、ウェブサーバ認証手段 5 2 と、セキュリティレベル転送手段 5 3 と、を備える。

【 0 0 2 3 】

本実施形態に係るセキュリティレベル制御ネットワークシステムは、データファイル保有サーバ 1 0 の保有するデータファイルをデータ配信サーバ 2 0 で分割して、複数のクライアント端末 3 0 に分散させる。このときに、データファイルの分割数がデータファイル保有サーバ 1 0 から可変になっている。この場合、以下の構成とすることが好ましい。

【 0 0 2 4 】

入力手段 1 4 からデータファイル格納手段 1 1 の格納しているデータファイルのセキュリティレベルが入力されると、セキュリティレベル通知手段 1 2 は、入力されたデータファイルのセキュリティレベルをデータ配信サーバ 2 0 に通知する。データファイル送信手段 1 3 は、データファイル格納手段 1 1 の格納しているデータファイルをデータ配信サーバ 2 0 に送信する。

【 0 0 2 5 】

データ配信サーバ受信手段 2 1 は、データファイル送信手段 1 3 からのデータファイルを受信する。データ配信サーバ格納手段 2 2 は、データ配信サーバ受信手段 2 1 の受信するデータファイルを格納する。セキュリティレベル決定手段 2 3 は、セキュリティレベル通知手段 1 2 からセキュリティレベルを取得すると、取得したセキュリティレベルに応じたデータファイルの分割数を決定する。暗号化手段 2 7 は、データ配信サーバ格納手段 2 2 からデータファイルを取得し、取得したデータファイルを暗号化する。一体化手段 2 8 は、暗号化手段 2 7 の暗号化したデータファイルを複数のデータピースに分割してデータピース同士を可逆演算することで一体化処理を行なう。分割手段 2 4 は、一体化手段 2 8 からデータファイルを取得し、取得したデータファイルをセキュリティレベル決定手段 2 3 の決定する分割数に分割する。データピース送信手段 2 5 は、分割手段 2 4 の分割したデータピースを複数のクライアント端末 3 0 に分散して送信する。

【 0 0 2 6 】

暗号化手段 2 7 は、例えばストリーム暗号等の共通鍵暗号でデータファイルをランダムな状態にする。この場合、共通鍵暗号として、加法的暗号のような高速なストリーム暗号を用いることが好ましい。一体化は、暗号化したデータファイルを複数のデータピースに分割してデータピース同士を可逆演算する。一体化は、例えば、データの空間分散化である。可逆演算は、例えば、加算、減算又は E O R、あるいは、これらの組み合わせである。データピース送信手段 2 5 は、送信する各データピースを、それぞれ異なる暗号鍵で暗号化することが好ましい。例えば、データ配信サーバ 2 0 と各クライアント端末 3 0 が V P N (V i r t u a l P r i v a t e N e t w o r k) で接続されていることが好ましい。

【 0 0 2 7 】

クライアント端末受信手段 3 1 は、データピース送信手段 2 5 からのデータピースを受信する。クライアント端末格納手段 3 2 は、クライアント端末受信手段 3 1 の受信するデータピースを格納する。

【 0 0 2 8 】

上記構成とすることで、データファイルのバックアップや災害発生時の復元動作を要求する管理ユーザ数が急激に増えた場合であっても、管理ユーザのサービス要求にあったセキュリティレベルを保証することができる。

【 0 0 2 9 】

10

20

30

40

50

データファイルの復元確率は、調整可能であることが好ましい。特に、データファイル保有サーバ10からファイルデータの復元確率が調整可能であることが好ましい。この場合、以下の構成とすることが好ましい。

【0030】

データファイル保有サーバ10において、セキュリティレベル通知手段12は、保有しているデータファイルの復元確率を、セキュリティレベルとしてデータ配信サーバ20にさらに通知する。

データ配信サーバ20において、セキュリティレベル決定手段23は、セキュリティレベルとしてデータファイルの復元確率を取得すると、取得した復元確率に応じたデータベースの複製数をさらに決定する。この場合、セキュリティレベル決定手段23は、自己の決定した分割数及び複製数によって生成されるデータベースの総数を決定する。複製手段26は、分割手段24からデータベースを取得し、取得したデータベースのそれぞれをセキュリティレベル決定手段の決定する複製数に複製する。データベース送信手段25は、複製手段26の複製したデータベースを、複数のクライアント端末30に分散して送信する。

10

【0031】

本実施形態に係るセキュリティレベル制御ネットワークシステムでは、重要なデータファイルのバックアップに協力することを承諾した個人の端末をクライアント端末30として利用することを前提としている。そのため、クライアント端末30が起動した状態であるか否かをデータ配信サーバ20は知りえない。そこで、データ配信サーバ20は、個々のクライアント端末30が動作可能な状態であることを確認した上でデータベースを分散させることが好ましい。この場合、以下の構成とすることが好ましい。

20

【0032】

複数のクライアント端末30において、応答手段33は、データ配信サーバ20からのデータベースを格納可能であるか否かの判定を指示する応答要求を監視サーバ40から受けると、自己のデータ配信サーバからのデータベースを格納可能であるか否かを判定し、当該判定結果を監視サーバ40に返信する。監視サーバ40において、クライアント端末リスト作成手段41は、複数のクライアント端末30に、応答要求を送信し、応答手段33からの判定結果を収集して、クライアント端末30のそれぞれがデータベースを受信可能な状態であるか否かをリスト化する。クライアント端末リスト格納手段42は、クライアント端末リスト作成手段41の作成するクライアント端末リストをデータ配信サーバ20から参照可能な状態で格納する。

30

【0033】

データ配信サーバ20において、セキュリティレベル決定手段23は、クライアント端末リスト格納手段42の格納するクライアント端末リストからデータベースを受信可能な状態のクライアント端末の数を取得する。そして、取得したクライアント端末30の数が自己の決定したデータベースの総数以上であるか否かを判定する。この結果、取得したクライアント端末30の数が自己の決定したデータベースの総数以上である場合は、分割手段24に分割数を出力し、複製手段26に複製数を出力する。一方、取得したクライアント端末の数が自己の決定したデータベースの総数未満である場合は、セキュリティレベル決定手段23は、データファイル保有サーバ10に、セキュリティレベルが十分でない旨を通知する。このとき、セキュリティレベル決定手段23は、セキュリティレベルが十分でない旨に加えて、その時点で対応可能なセキュリティレベルを通知することが好ましい。

40

【0034】

データファイルが秘匿性の要求される重要な内容をもつ場合、データ配信サーバ20は、予め定められた端末を除いてアクセス不能とすることが好ましい。そのため、データ配信サーバ20とは異なるウェブサーバ50で一旦認証を行い、その上でデータ配信サーバ20にログイン可能とすることが好ましい。この場合、以下の構成とすることが好ましい。

50

【 0 0 3 5 】

データファイル保有サーバ10において、データファイル保有サーバ認証手段15は、データファイル保有サーバ10固有の情報及び予め定められたセキュリティレベルを格納する。データファイル保有サーバ認証手段15は、例えば、RFIDである。入力手段14は、データファイル保有サーバ認証手段15に格納されている固有の情報及びセキュリティレベルを読み出す。セキュリティレベル通知手段12は、入力手段14の読み出した情報すなわちデータファイル保有サーバ認証手段15に格納されている固有の情報及びセキュリティレベルをウェブサーバ50に通知する。

【 0 0 3 6 】

ウェブサーバ50において、固有情報格納手段51は、データファイル保有サーバ10の固有の情報を予め格納する。ウェブサーバ認証手段52は、セキュリティレベル通知手段12からの固有の情報を受信すると、受信した固有の情報が固有情報格納手段51に格納されているか否かを判定する。セキュリティレベル転送手段53は、セキュリティレベル通知手段12からの固有の情報が固有情報格納手段51に格納されていると判定すると、セキュリティレベル通知手段12からのセキュリティレベルを、データ配信サーバに通知する。

【 0 0 3 7 】

ファイルバックアップを行うデータファイル保有サーバ10がRFIDを使用して、自身の認証情報、重要ファイルのバックアップを行う際のセキュリティレベル情報、復元確率のレベル値等の指示情報を、RFIDリーダー、データファイル保有サーバ10を介して、データセンタのあるウェブサーバ50にアクセスする。ここで、RFIDは、安全性の面からは、暗号化された、認証情報や、サービスグレード等を書き込んだものを、1つまたは複数個を、通信事業者側またはサービス提供者が準備し、ファイルバックアップを要求する管理ユーザに貸与する形態が望ましい。このようにすると、責任ある立場の管理ユーザのみが、当該のウェブサーバをアクセスできる権限を持つことにより、一層のセキュリティ上の確保が可能となるからである。

【 0 0 3 8 】

近年においては、電磁波と対応する送受信アンテナを利用した非接触型の自動認識技術としてRFID(Radio Frequency Identification)技術が実用化され、電池を持たない半永久的に利用可能なものまでが商用化されている。RFIDでは、微小な無線電波を送受信するICチップを活用し、タグ形態に加工された数cm程度の大きさのアンテナ付ICチップを用いている。ICチップに対して情報の読み取りや書き込みを行うリーダー/ライターの利用により、情報の送受信が可能となる。このRFID技術は、従来は流通業界でバーコードに代わる商品識別・管理技術として実用化が進められてきたが、それに留まらず社会のIT化を推進する上での基盤技術として注目が高まっている。例えば、非接触タイプのRFIDタグをリーダー/ライターにかざすことで買い物などを行うことを可能にした携帯電話やICカード乗車券が、NTTドコモの「おサイフケータイ」(登録商標)やJR東日本のICカード乗車券「Suica」(登録商標)として提供されている。

【 0 0 3 9 】

例えば、管理ユーザに貸与されたRFIDにはバックアップするセキュリティレベルが格納されていることを想定できる。データファイル保有サーバ10の入力手段14は、RFIDに格納されているセキュリティレベルを読み取り、セキュリティレベル通知手段12から通知する。このとき、管理ユーザは、RFIDに格納されているセキュリティレベルを勘案してRFIDタグを選択する。ここで、RFIDには、セキュリティレベル、ID情報及びパスワードなどの認証に必要な情報が書き込まれていることが好ましい。RFID種別により、これらのセキュリティレベルを、管理ユーザが任意に選択できる。

【 0 0 4 0 】

セキュリティレベル通知手段12は、管理ユーザのサービス要求をウェブサーバ50に送信する。サービス要求には、例えばRFIDに格納されているID情報及びセキュリテ

10

20

30

40

50

イレベルが含まれる。ウェブサーバ50は、データ配信サーバ20とのやり取りを行って、要求されたセキュリティレベルを実施可能であるか否かを確認する。このとき、ウェブサーバ50は、データ配信サーバ20から対応可能なセキュリティレベルを取得する。

そして、要求されたセキュリティレベルを実施可能である場合には、ウェブサーバ50は、認証確認の旨とともに要求されたセキュリティレベルが実施可能である旨をデータファイル保有サーバ10に通知する。

一方、要求されたセキュリティレベルを実施可能でない場合には、ウェブサーバ50は、その旨をデータファイル保有サーバ10に通知する。このとき、ウェブサーバ50は、データ配信サーバ20とのやり取りの際に取得した対応可能なセキュリティレベルもデータファイル保有サーバ10に通知することが好ましい。

【0041】

今後、RFIDタグの小型化とコストダウンが進み、この、RFIDタグを、ファイルバックアップを要求する際の、セキュリティレベル等の変更を実施するための、ツールとして活用する。すなわち、本実施形態では、RFID技術に着目することにより、重要ファイルのバックアップを行う際の、セキュリティレベルの向上、並びに復元確率の向上または、バックアップコストの低減化に変わる指示情報としても、活用できる。

【0042】

本実施形態に係るセキュリティレベル制御ネットワークシステムの動作の一例について、図1を用いて説明する。ウェブサーバ50は、データファイル保有サーバ10を操作可能な管理ユーザからのログインアクセスに対する認証を行う。そして、認証が成功した時点で、ウェブサーバ50は、データ配信サーバ20に対して、管理ユーザが要求するセキュリティレベルの実現可能性を打診する。データ配信サーバ20は、クライアント端末リスト格納手段42を参照することでネットワークリソースを勘案して、ネットワークリソースの充当が可能である場合には、対応する課金処理の準備を行った後に、ウェブサーバ50に対して、サービス要求受け入れ確認の通知を行う。

【0043】

ここで、データ配信サーバ20が、ネットワークリソースを勘案して、ネットワークリソースの充当が不可能である場合には、その旨を通知する。ウェブサーバ50は、データ配信サーバ20からのサービス確認情報に基づいて、管理ユーザに対して、当該サービス要求に関わる確認情報を通知する。その後、ウェブサーバ50は、ネットワークリソースの使用状況に見合うネットワークコストを勘案して、管理ユーザに対する課金処理を施す。データファイル保有サーバ10が新たなデータファイル転送を実施してきた場合には、データ配信サーバ20は、サービス要求のセキュリティレベルに応じて、クライアント端末30群に対してデータピースの分散配信を実施すると共に、関連するメタデータを監視サーバ40に送信する。ここで、メタデータは、データピースを除くデータファイルを復元するために必要なデータをいう。

【0044】

以上述べたデータセンタにおける、管理ユーザからのサービス要求に対応する処理シーケンスの一例を説明する。

第1のステップでは、データ配信サーバ20が、サービス要求をウェブサーバ50から受信する。これによって、管理ユーザは、要求するバックアップ対象データファイルに対する分割数と複製数の設定情報の要求を行う。

第2のステップでは、データ配信サーバ20が、分割数及び複製数に基づくクライアント端末数、配信地域の決定が可能かどうかのリソースの見積もりを行う。

第3のステップでは、管理ユーザの要求をみたすネットワークリソースの割り当てが可能かどうかを判定する。割り当てが可能場合は第4のステップに移行し、割り当てが不可能場合は第5のステップに移行する。

第4のステップでは、データ配信サーバ20が、管理ユーザの要求に応じた課金処理の実施準備を行うと共に、ウェブサーバ50に対して、要求サービスの受け入れを通知する。そして、第6のステップに移行する。

10

20

30

40

50

第5のステップでは、データ配信サーバ20が、ウェブサーバ50に対して、要求サービスの受け入れができない旨を通知する。そして、第6のステップに移行する。

第6のステップでは、ウェブサーバ50が、管理ユーザに対して、認証確認の結果と、要求サービスの実施が可能であるか否かを通知する。

第7のステップでは、データファイル保有サーバ10が、ウェブサーバ50からの要求サービスの受け入れの有無を取得する。

【0045】

第1のステップから第7のステップを実行することで、管理ユーザは、要求サービスの受け入れの有無を確認することができる。また、次回からのデータファイルのバックアップ時には、データ配信サーバ20が要求サービスに応じたセキュリティレベルでバックアップを行うことを管理ユーザが確認することができる。

10

【0046】

次に、分割数を増減させた場合のセキュリティレベルの効果について説明する。本方式では、複数地域に分散されたクライアント端末30へデータピースを配布する際に、データファイルの復元に関しては、分割されたデータファイルに対する総当り方式での解読の施行が必要となるため、高い暗号強度の達成が、従来方式に比べて、容易に実現できる。以下は、既存の暗号方式との定量的な、暗号強度の比較結果の一例である。

【0047】

分割数が20のとき、データピースの並べ方の組み合わせは20!ある。 $20! = 2^{61} \cdot 10^{18}$ であるので、分割数20でデータファイルを分割することで、54bit暗号のDES以上の安全性をもつことになる。

20

分割数が40のとき、データピースの並べ方の組み合わせは40!ある。 $40! = 2^{160} \cdot 10^{47}$ であるので、分割数40でデータファイルを分割することで、128bit暗号のAES以上の安全性をもつことになる。

分割数が80のとき、データピースの並べ方の組み合わせは80!ある。 $80! = 2^{400} \cdot 10^{120}$ であるので、分割数80でデータファイルを分割することで、400bit暗号以上の安全性をもつことになる。400bit暗号レベルに匹敵する安全性をもつ暗号はまだ実用化されていない。

【0048】

分割数を増大させることで、分割化されたデータピースの正常な組み合わせ方を発見することそのものが殆ど困難となる。更に、仮に、正しい組み合わせ方が、何らかの方法で見つけ出されたとしても、データファイルは、データファイル全体が一体化処理による暗号化を同時に施されているため、盗聴者によるデータファイルの復元はほとんど困難となる。したがって、データファイルの空間的な分散転送と一体化処理とを組み合わせれば、これらの相乗効果により暗号強度の大幅な向上を実現することができる。

30

【0049】

R F I Dに格納されているセキュリティレベルの一例を示す。最高度レベル、高度レベル、中高度レベル、中度レベルの4つのセキュリティレベルが格納されている。最高度レベル、高度レベル、中高度レベル、中度レベルが、管理ユーザの要求するセキュリティレベルである。これらのセキュリティレベルに応じて、通信事業者の設定するセキュリティレベルと、セキュリティレベル決定手段23の決定する分割数及び複製数とが決まる。

40

【0050】

例えば、セキュリティレベルが最高度レベルのとき、通信事業者等の設定するセキュリティレベルでは、暗号強度をAESで400bit以上とし、回復確率を $1 - (10^{-20})$ 以上とする。このとき、セキュリティレベル決定手段23は、分割数を80、複製数を100に決定する。

セキュリティレベルが高度レベルのとき、通信事業者等の設定するセキュリティレベルでは、暗号強度をAESで128bit以上とし、回復確率を $1 - (10^{-8})$ 以上とする。このとき、セキュリティレベル決定手段23は、分割数を40、複製数を50に決定する。

50

セキュリティレベルが中高度レベルのとき、通信事業者等の設定するセキュリティレベルでは、暗号強度をAESで128bit以上とし、回復確率を $1 - (10^{-5})$ 以上とする。このとき、セキュリティレベル決定手段23は、分割数を40、複製数を20に決定する。

セキュリティレベルが中度レベルのとき、通信事業者等の設定するセキュリティレベルでは、暗号強度をAESで64bit以上とし、回復確率を $1 - (10^{-4})$ 以上とする。このとき、セキュリティレベル決定手段23は、分割数を20、複製数を10に決定する。

【0051】

次に、データファイルの分割数及びデータピースの複製数と復元確率の具体的な関係について説明する。データファイルの分割数を n 、データピースの複製数を m 、クライアント端末30の故障率を p ($p \ll 1$)とし、クライアント端末30もランダムに故障すると想定すると、データファイルの復元確率は、)は次式で表される。

$$\text{復元確率} = (1 - p^m)^n = 1 - n p^m \quad (1)$$

【0052】

例えば、合計で100MBのデータファイルを分割数20で分割し、分割した5MBのデータピースを複製数10で複製した場合を考える。このときの復元確率は、分散された先のクライアント端末30での故障率が20%とすると、前出の式(1)より、復元確率は0.999998となり、極めて高い安全性を確保することが分かる。

【0053】

冗長度 m の値を大きくすれば、復元確率の値は飛躍的に大きくできるが、必要となるクライアント端末30の数やネットワークリソースが増えることになる。したがって、データファイルのバックアップ時に、バックアップに必要な分割数及び複製数を、管理ユーザが保守費用を勘案して、任意に設定できることが好ましい。また、クライアント30の故障率は状況に応じて適宜見積もることが好ましい。

【0054】

合計で1GBのデータファイルを分割数40で分割し、分割したデータピースを複製数10で複製した場合を考える。このときの復元確率は、分散された先のクライアント端末30での故障率が33%とした場合であっても、前出の式より、復元確率は0.9996となる。したがって、実用上、1台あたりのクライアント端末30に分散する記憶容量も、5~25MB程度の実用的な値で、かつ、クライアント端末の故障率が3台に1台が故障しているというひどい被害状況の場合であってもデータファイルの復元確率を維持することができる。

【0055】

以上説明したように、本実施形態に係るセキュリティレベル制御ネットワークシステムは、データファイルの分割数とデータピースの複製数を変更することで、セキュリティレベルを調整することができる。したがって、重要データのバックアップを要求する管理ユーザは、ネットワークリソースに基づくバックアップ処理費用なども勘案して、時々刻々と要求するセキュリティレベルや復元確率に関わる条件を適宜、通信ネットワークを通じて、安全に、変更する融通性をもつことができ、データファイルのバックアップに関わる融通性を飛躍的に向上させることができる。

【0056】

すなわち、管理ユーザおよび通信事業者の双方からみて、融通性の高いファイルバックアップシステムの実現メカニズムが実現できることにより、ネットワークリソースの効果的な活用も同時に実現できるため、ファイルバックアップ要求の高い管理ユーザの利便性を向上させることができる。

【産業上の利用可能性】

【0057】

本発明は、データファイルの保全に関わる各種の要求を、管理ユーザの主導において実施し、この際のバックアップファイルの保全に関わるコストを元に、プロバイダが適切に課金処

10

20

30

40

50

理等を実施することの可能なネットワークシステムに利用することができる。

【図面の簡単な説明】

【0058】

【図1】本実施形態に係るセキュリティレベル制御ネットワークシステムの構成概略図である。

【図2】データファイル保有サーバ10の一例を示す概略構成図である。

【図3】データ配信サーバ20の一例を示す概略構成図である。

【図4】クライアント端末30の一例を示す概略構成図である。

【図5】監視サーバ40の一例を示す概略構成図である。

【図6】ウェブサーバ50の一例を示す概略構成図である。

10

【符号の説明】

【0059】

- 10 データファイル保有サーバ
- 11 データファイル格納手段
- 12 セキュリティレベル通知手段
- 13 データファイル送信手段
- 14 入力手段
- 15 データファイル保有サーバ認証手段
- 20 データ配信サーバ
- 21 データ配信サーバ受信手段
- 22 データ配信サーバ格納手段
- 23 セキュリティレベル決定手段
- 24 分割手段
- 25 データピース送信手段
- 26 複製手段
- 27 暗号化手段
- 28 一体化手段
- 30 クライアント端末
- 31 クライアント端末受信手段
- 32 クライアント端末格納手段
- 33 応答手段
- 40 監視サーバ
- 41 クライアント端末リスト作成手段
- 42 クライアント端末リスト格納手段
- 50 ウェブサーバ
- 51 固有情報格納手段
- 52 ウェブサーバ認証手段
- 53 セキュリティレベル転送手段
- 100 通信ネットワーク

20

30

【要約】

40

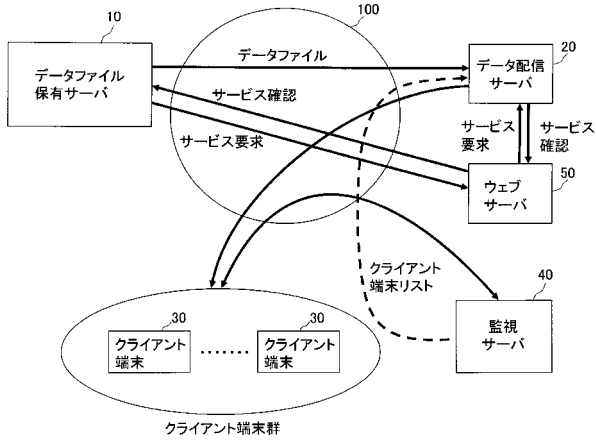
【課題】本発明は、データファイルを分割し、当該分割されたデータピースを複数のクライアント端末に分散転送するバックアップ技術を用い、データファイルを保有する管理ユーザのサービス要求に見合ったセキュリティレベルでのバックアップを可能にすることを目的とする。

【解決手段】本発明に係るセキュリティレベル制御ネットワークシステムは、データファイル保有サーバ10に保有されているデータファイルを分割し、当該分割したデータピースを複数のクライアント端末30に分散して送信するデータ配信サーバ20に、データファイル保有サーバ10から通知されたセキュリティレベルに応じてデータファイルの分割数を制御するセキュリティレベル決定手段を設けたことを特徴とする。

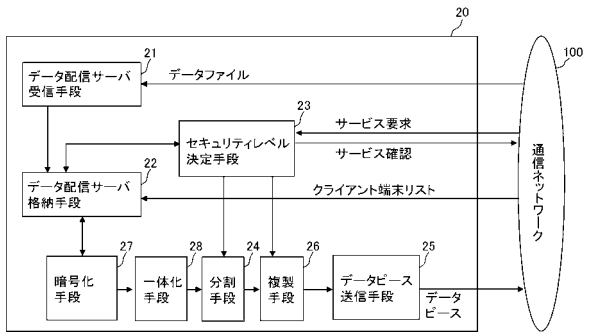
【選択図】図1

50

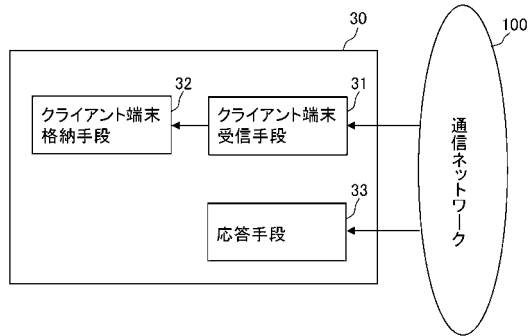
【図1】



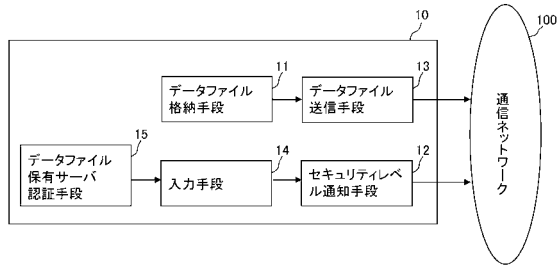
【図3】



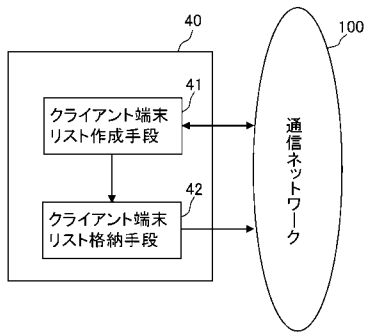
【図4】



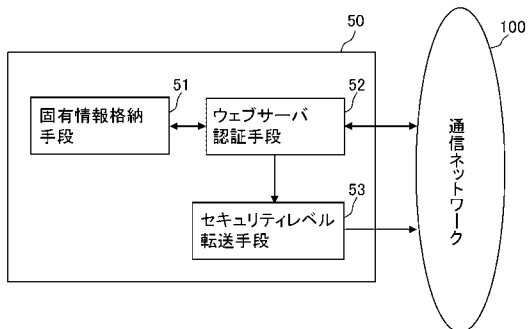
【図2】



【図5】



【図6】



フロントページの続き

- (72)発明者 鈴木 秀一
東京都千代田区神田錦町 2 - 2 学校法人東京電機大学内
- (72)発明者 田窪 昭夫
東京都千代田区神田錦町 2 - 2 学校法人東京電機大学内
- (72)発明者 和田 雄次
東京都千代田区神田錦町 2 - 2 学校法人東京電機大学内
- (72)発明者 森 建二
東京都千代田区神田錦町 2 - 2 学校法人東京電機大学内

審査官 児玉 崇晶

- (56)参考文献 特開 2007 - 122446 (JP, A)
特開 2007 - 078739 (JP, A)
特開 2006 - 350470 (JP, A)
特開 2006 - 048158 (JP, A)
特開 2007 - 128240 (JP, A)
特開 2005 - 215735 (JP, A)
特開 2007 - 172390 (JP, A)
國分 建介 Kensuke KOKUBUN, グリッドコンピューティングを適用したディザスタ・リカバリ・システムの性能評価 Performance evaluation of Disaster Recovery System using Grid Computing technology, 電子情報通信学会技術研究報告IEICE Technical Report, 日本, 社団法人電子情報通信学会 The Institute of Electronics, Information and Communication Engineers, 2007年12月13日, Vol. 107 No. 403, pp. 1 - 6

- (58)調査した分野(Int.Cl., DB名)
- | | |
|------|-------|
| G06F | 21/24 |
| G06F | 12/00 |
| G06F | 13/00 |