(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)
(22)出願日　平成20年10月9日 (2008.10.9)
審査請求日　平成21年1月23日 (2009.1.23)

早期審査対象出願

(73)特許権者　800000068
学校法人東京電機大学
東京都千代田区神田錦町２－２
(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　宮保　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、

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】

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、

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、

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。

【００１０】
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。
【００１１】
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。
【００１２】
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。
【００１３】
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、
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。
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】
【００１４】
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。

【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えることはいうまでもない。
【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、任意の組み合せから成る複数が一体化され、１つの構成となっていてもよい。
【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。

【００２２】
図４は、クライアント端末３０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３０は、クライアント端末受信手段３１と、クライアント端末格納手段３２と、応答手段３３と、を備える。図５は、監視サーバ４０の一例を示す概略構成図である。監視サーバ４０は、クライアント端末リスト作成手段４１と、クライアント端末リスト格納手段４２と、を備える。図６は、ウェブサーバ５０の一例を示す概略構成図である。ウェブサーバ５０は、固有情報格納手段５１と、ウェブサーバ認証手段５２と、セキュリティレベル転送手段５３と、を備える。
【００２３】
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の保有するデータファイルをデータ配信サーバ２０で分割して、複数のクライアント端末３０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１０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。
【００２４】
入力手段１４からデータファイル格納手段１１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１２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２０に通知する。データファイル送信手段１３は、データファイル格納手段１１の格納しているデータファイルをデータ配信サーバ２０に送信する。
【００２５】
データ配信サーバ受信手段２１は、データファイル送信手段１３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２２は、データ配信サーバ受信手段２１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２３は、セキュリティレベル通知手段１２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２７は、データ配信サーバ格納手段２２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２８は、暗号化手段２７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２４は、一体化手段２８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２３の決定する分割数に分割する。データピース送信手段２５は、分割手段２４の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。
【００２６】
暗号化手段２７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ＥＯＲ、あるいは、これらの組み合せである。データピース送信手段２５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２０と各クライアント端末３０がＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）で接続されていることが好ましい。
【００２７】
クライアント端末受信手段３１は、データピース送信手段２５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３２は、クライアント端末受信手段３１の受信するデータピースを格納する。
【００２８】
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。
【００２９】

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ピ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ピースの総数を決定する。複製手段２６は、分割手段２４からデータピースを取得し、取得したデータピ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。データピース送信手段２５は、複製手段２６の複製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。

【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かを確認した上でデータピ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。

【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。

【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ピ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ピ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ピ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ピ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。

【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。

【００３５】
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。
【００３６】
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。
【００３７】
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。
【００３８】
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。
【００３９】
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。
【００４０】
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

ィレベルが含まれる。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。割り当てが可能な場合は第４のステップに移行し、割り当てが不可能な場合は第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。

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。

【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、従来の方式に比べて、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せは２０！ある。２０！　2^{61}　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。

分割数が４０のとき、データピースの並べ方の組み合せは４０！ある。４０！　2^{160}　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せは８０！ある。８０！　2^{400}　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。

【００４９】

ＲＦＩＤ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。

【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。

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関係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（＜＜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。

復元確率＝（１－ｐ^{m}）^{n}　１－ｎｐ^{m}　　（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

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。

【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

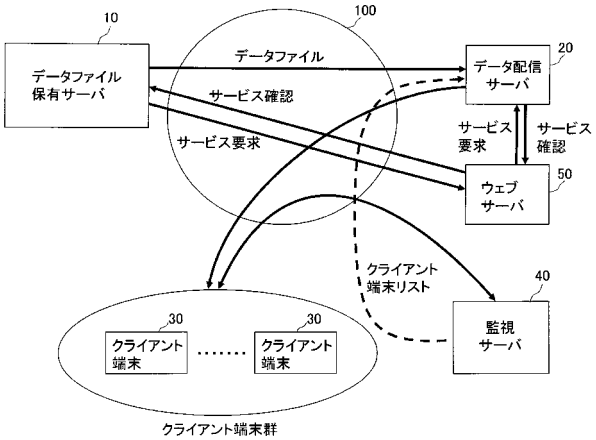
【要約】

【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。

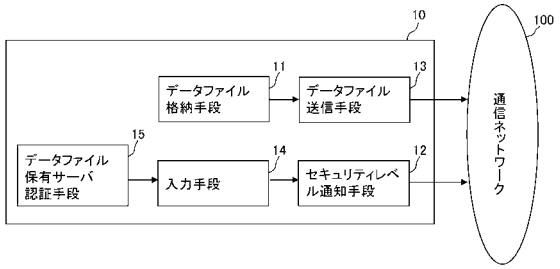
【解決手段】本発明に係るセキュリティレベル制御ネットワークシステムは、データファイル保有サーバ１０に保有されているデータファイルを分割し、当該分割したデータピースを複数のクライアント端末３０に分散して送信するデータ配信サーバ２０に、データファイル保有サーバ１０から通知されたセキュリティレベルに応じてデータファイルの分割数を制御するセキュリティレベル決定手段を設けたことを特徴とする。

【選択図】図１

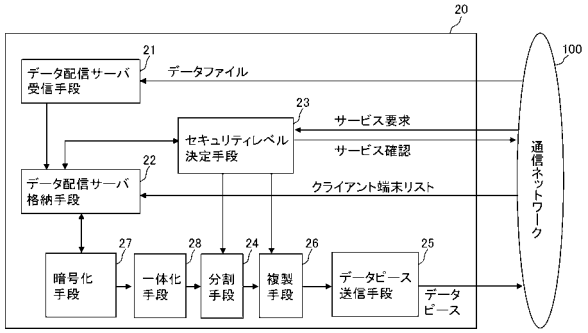
【図１】



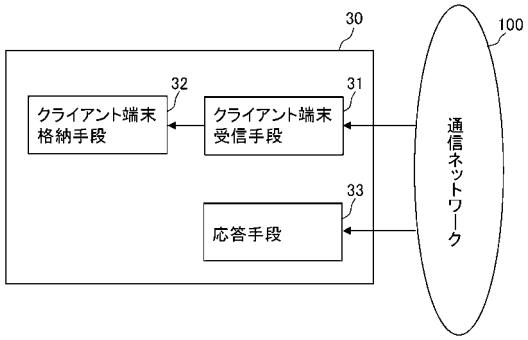
【図２】



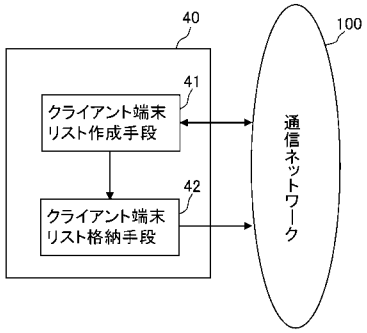
【図３】



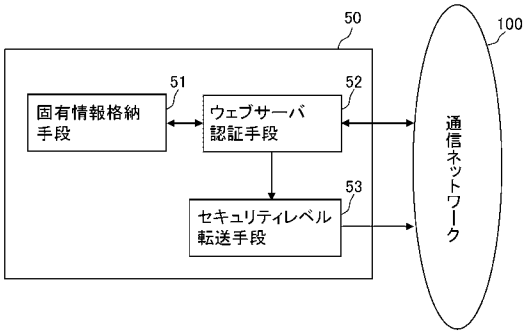
【図４】



【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