(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2008-257726
(P2008-257726A)
(43)公開日　平成20年10月23日(2008.10.23)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	530D	5B017
G06F 12/00	(2006.01)	G06F	12/00	531M	5B082
H04L 9/32	(2006.01)	G06F	12/00	537D	5J104
		G06F	12/14	530P	
		H04L	9/00	675D	

審査請求 未請求　請求項の数 20　ＯＬ　（全 15 頁）

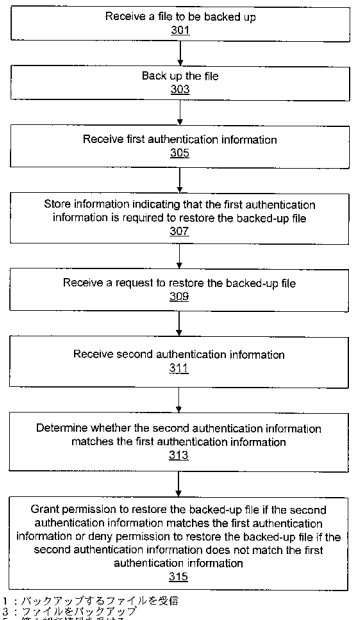
(21)出願番号　特願2008-89980 (P2008-89980)
(22)出願日　平成20年3月31日 (2008.3.31)
(31)優先権主張番号　11/731,113
(32)優先日　平成19年3月30日 (2007.3.30)
(33)優先権主張国　米国 (US)

(71)出願人　508097548
データ　センター・テクノロジーズ
アメリカ合衆国・９５０１４・カリフォルニア州・クーパーティノ・スティーブンス　クリーク　ブーレバート・２０３００
(74)代理人　100064621
弁理士　山川　政樹
(74)代理人　100098394
弁理士　山川　茂樹
(72)発明者　トム・デ・コニンク
ベルギー国・９０００　ゲント・アポステルフイツェン・５９
(72)発明者　ハンス・パイプ
ベルギー国・９８１０　ナザレ・スネップシュトラート・２９

最終頁に続く

(54)【発明の名称】バックアップされたファイルのパスワード保護

(57)【要約】
【課題】ファイルのバックアップ処理を実施するためのシステム及び方法を提供する。
【解決手段】バックアップするファイルを保護するために、コンピュータシステム上にあるファイルと関連付けられるパスワード又は他の認証情報をコンピュータシステムのユーザーが提供できるように動作する。ユーザー（又は他の個人又はソフトウェアエージェント）がパスワード保護下にあるファイルのバックアップコピーを復元、又はそれ以外の目的でアクセスしようと試みた場合、ユーザーはパスワードを入力するように促される。本方法は、そのファイルの復元を許可する前に、入力されたパスワードがそのファイルに関連付けられたパスワードと一致するかどうかを検証するように動作することができる。
【選択図】図１



３０１：バックアップするファイルを受信
３０３：ファイルをバックアップ
３０５：第１認証情報を受ける
３０７：バックアップされたファイルを復元するためには第１認証情報が要求されたことを示す情報が記憶される
３０９：バックアップされたファイルの復元要求を受ける
３１１：第２認証情報を受ける
３１３：第２認証情報が第１認証情報と一致するかどうかが判定される
３１５：第２認証情報が第１認証情報と一致した場合はバックアップされたファイルの復元が許可される、又は第２認証情報が第１認証情報と一致しない場合はバックアップされたファイルの復元が拒絶される

【特許請求の範囲】
【請求項１】
バックアップすべきファイルを受信するステップと；
前記ファイルをバックアップするステップと；
第１認証情報を受けるステップと；
前記バックアップされたファイルの復元に、前記第１認証情報を要求することを示す情報を記憶するステップと；
を実行することができるプログラム命令を含むコンピュータ可読記憶媒体。
【請求項２】
前記プログラム命令が：
前記バックアップされたファイルの復元要求を受けるステップと；
第２認証情報を受けるステップと；
前記第２認証情報が前記第１認証情報と一致するか否かを判定するステップと；
前記第２認証情報が前記第１認証情報に一致した場合は前記バックアップされたファイルの復元を許可し、前記第２認証情報が前記第１認証情報に一致しない場合は前記バックアップされたファイルの復元を拒絶するステップと；
をさらに実行することができることを特徴とする請求項１に記載のコンピュータ可読記憶媒体。
【請求項３】
前記プログラム命令が：
前記バックアップされたファイルの前記復元要求に呼応して、前記第２認証情報の入力を促すステップ；をさらに実行することができ、
前記第２認証情報を受けるステップが、前記第２認証情報の入力を促すステップに呼応して、ユーザー入力を受けるステップを含むことを特徴とする請求項２に記載のコンピュータ可読記憶媒体。
【請求項４】
前記プログラム命令が：
前記第１認証情報を記憶するステップ；及び／又は
前記第１認証情報から派生する情報を記憶するステップ；のうち、１つ以上を実施することができることを特徴とする請求項１に記載のコンピュータ可読記憶媒体。
【請求項５】
前記ファイルを受信するステップが、第１コンピュータシステムから前記ファイルを受信するステップを含み；
前記第１認証情報を受けるステップが、前記第１コンピュータシステムから前記第１認証情報を受けるステップを含み；
前記ファイルをバックアップするステップが、前記ファイルを、前記第１コンピュータシステム以外の１つ以上のコンピュータシステム上に記憶するステップを含むことを特徴とする請求項１に記載のコンピュータ可読記憶媒体。
【請求項６】
前記プログラム命令が：
前記バックアップされたファイルを第２コンピュータシステムから復元する要求を受けるステップと；
前記要求に呼応して第２認証情報の入力を促すステップと；
前記第２認証情報を前記第２コンピュータシステムから受けるステップと；
前記第２認証情報が前記第１認証情報と一致するか否かを判定するステップと；
前記第２認証情報が前記第１認証情報と一致した場合は前記バックアップされたファイルの復元を許可し、前記第２認証情報が前記第１認証情報に一致しない場合は前記バックアップされたファイルの復元を拒絶するステップと；をさらに実行することができることを特徴とする請求項５に記載のコンピュータ可読記憶媒体。
【請求項７】

前記ファイルを受信するステップが、前記ファイルを第１コンピュータシステムから受信するステップを含み；
前記ファイルをバックアップするステップが、ファイルを複数のセグメントに分割するステップと、そして前記複数のセグメントを前記第１コンピュータシステム以外の複数のコンピュータシステムへと分散するステップとを含むことを特徴とする請求項１に記載のコンピュータ可読記憶媒体。
【請求項８】
前記第１認証情報がパスワードを含むことを特徴とする請求項１に記載のコンピュータ可読記憶媒体。
【請求項９】
前記第１の認証情報がバイオメトリック情報を含むことを特徴とする請求項１に記載のコンピュータ可読記憶媒体。
【請求項１０】
前記バイオメトリック情報が：
フィンガプリント情報；
音声情報；及び／又は
網膜スキャン情報；のうち、１つ以上を含むことを特徴とする請求項９に記載のコンピュータ可読記憶媒体。
【請求項１１】
１つ以上のプロセッサ及びプログラム命令を記憶するメモリを具備するコンピュータシステムであって、前記１つ以上のプロセッサが：
バックアップすべきファイルを受信するステップと；
前記ファイルをバックアップするステップと；
第１認証情報を受けるステップと；
前記バックアップされたファイルの復元に、前記第１認証情報を要求することを示す情報を記憶するステップと；を行うプログラム命令を実行するものであることを特徴とするコンピュータシステム。
【請求項１２】
前記１つ以上のプロセッサが：
前記バックアップされたファイルの復元要求を受けるステップと；
第２認証情報を受けるステップと；
前記第２認証情報が前記第１認証情報と一致するか否かを判定するステップと；
前記第２認証情報が前記第１認証情報に一致した場合は前記バックアップされたファイルの復元を許可し、前記第２認証情報が前記第１認証情報に一致しない場合は前記バックアップされたファイルの復元を拒絶するステップと；を行うプログラム命令をさらに実行するものであることを特徴とする請求項１１に記載のコンピュータシステム。
【請求項１３】
前記１つ以上のプロセッサが：
前記バックアップされたファイルの復元要求に呼応して、前記第２認証情報の入力を促すステップを行うプログラム命令をさらに実行し；
前記第２認証情報を受けるステップが、前記第２認証情報の入力を促すステップに呼応して、ユーザー入力を受けるステップを含むことを特徴とする請求項１２に記載のコンピュータシステム。
【請求項１４】
前記１つ以上のプロセッサが：
前記第１認証情報を記憶するステップ；及び／又は
前記第１認証情報から派生する情報を記憶するステップ；のうち、１つ以上を行うプログラム命令をさらに実行することを特徴とする請求項１０に記載のコンピュータシステム。
【請求項１５】

前記コンピュータシステムが第１コンピュータシステムであって；
前記ファイルを受信するステップが第２コンピュータシステムからファイルを受信するステップを含み；
前記第１認証情報を受けるステップが、前記第２コンピュータシステムから前記第１認証情報を受けるステップを含むことを特徴とする請求項１０に記載のコンピュータシステム。
【請求項１６】
バックアップすべきファイルを受信するステップと；
前記ファイルをバックアップするステップと；
第１認証情報を受けるステップと；
前記バックアップされたファイルの復元に、前記第１認証情報を要求することを示す情報を記憶するステップと；を含む方法。
【請求項１７】
前記バックアップされたファイルの復元要求を受けるステップと；
第２認証情報を受けるステップと；
前記第２認証情報が前記第１認証情報と一致するか否かを判定するステップと；
前記第２認証情報が前記第１認証情報に一致した場合は前記バックアップされたファイルの復元を許可し、前記第２認証情報が前記第１認証情報に一致しない場合は前記バックアップされたファイルの復元を拒絶するステップと；をさらに含む請求項１６に記載の方法。
【請求項１８】
前記バックアップされたファイルの前記復元要求に呼応して、前記第２認証情報の入力を促すステップ；をさらに含み、
前記第２認証情報を受けるステップが、前記第２認証情報の入力を促すステップに呼応して、ユーザー入力を受けるステップを含むことを特徴とする請求項１７に記載の方法。
【請求項１９】
前記第１認証情報を記憶するステップ；及び／又は
前記第１認証情報から派生する情報を記憶するステップ；のうち、１つ以上をさらに含むことを特徴とする請求項１６に記載の方法。
【請求項２０】
前記ファイルを受信するステップが、前記ファイルを第１コンピュータシステムから受信するステップを含み；
前記第１認証情報を受けるステップが、前記第１コンピュータシステムから前記第１認証情報を受けるステップを含み；
前記ファイルをバックアップするステップが、前記ファイルを前記第１コンピュータシステム以外の１つ以上のコンピュータシステム上に記憶するステップを含むことを特徴とする請求項１６に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は一般に、コンピュータシステム中のファイルをバックアップするためのファイルバックアップソフトウェアに関する。
【背景技術】
【０００２】
コンピュータシステムは一般に情報をファイルシステムにより系統化されたファイルとして記憶する。各ファイルはディスクドライブ、光学式ドライブ、又はテープドライブのような記憶装置に記憶される。これらを他の記憶装置へコピーするなどにより、ファイルシステム中のファイルをバックアップしなければならないことが多い。バックアップ処理は、たとえばデータロスに対する備えとしてある時点でのファイルのスナップショットを作るために、あるいは他の目的でファイルの複製を作るために実施する。

【０００３】
コンピュータシステムはファイルのバックアップをするために、代表的にはバックアップソフトウェアを実行する。バックアップソフトウェアは、いつ、又はどの頻度でバックアップを実行するのか、どのファイルをバックアップするのか、そのファイルをどこにバックアップするのか、などのようなファイルバックアップ処理用の様々なオプションをユーザー又は管理者が設定することができるユーザーインターフェースを設けている。
【発明の開示】
【課題を解決するための手段】
【０００４】
本明細書においては、ファイルバックアップ処理を実施するための様々なシステム及び方法の実施態様が記載される。本方法の一実施態様によれば、バックアップすべきファイルが受信される。受信されたファイルは、たとえばそのデータを１つ以上の記憶装置上のファイル中に記憶することによりバックアップされる。本方法はさらに、後にバックアップファイルへのアクセスを試みる個人又はソフトウェアエージェントが、そのための認可を適正に受けているかどうかを確認するパスワード、バイオメトリック情報、又は他の利用可能な手段などのような第１認証情報を受けるステップを含む。本方法は、バックアップされたファイルを復元するために第１認証情報が要求されることを示す情報を記憶するように動作する。
【０００５】
本発明の他の実施態様によれば、バックアップされたファイルを復元するための要求は、たとえばファイルがバックアップされた後に受信される。本方法はさらに、第２認証情報を受けるステップと、その第２認証情報が第１認証情報に一致するかどうかを判定するステップを含んでいる。第２認証情報が第１認証情報に一致した場合、バックアップファイルの復元許可が与えられる。また、逆の場合、バックアップファイルの復元は拒絶される。
【０００６】
添付図を参照しつつ以下の詳細説明を考察することにより、本発明に対するより深い理解を得ることができる。
【発明を実施するための最良の形態】
【０００７】
本発明には様々な変更及び改変形態が可能であるが、その特定の実施形態を例示目的で図示し、詳細に説明する。しかしながら、図と詳細な説明は、本発明を開示した特定の形態に限定することを意図したものではなく、むしろ本発明は、本願請求項に定義された本発明の精神及び範囲に入る全ての変更形態、均等物、改変形態を網羅することを意図したものである。
【０００８】
ここでファイルバックアップ処理を実施するためのシステム及び方法の様々な実施形態を説明する。方法は、バックアップされたファイルを保護するなどのために、コンピュータシステム上のファイルと関連付けられるパスワード又は他の認証情報を、コンピュータシステムのユーザーが提供するように動作する。たとえば、ユーザー（又は他の個人又はソフトウェアエージェント）がパスワード保護下にあるファイルのバックアップコピーを復元する又は他の目的でアクセスしようと試みた場合、ユーザーにパスワードの入力を促す。方法は、入力されたパスワードがそのファイルに関連付けられたパスワードであることを検証した後に、そのファイルの復元許可を出すように動作する。
【０００９】
図１は本方法の一実施形態を説明するフロー図である。方法は、１つ以上のコンピュータシステム上で起動するバックアップ管理ソフトウェアにより実施することができる。
【００１０】
ステップ３０１においては、バックアップ管理ソフトウェアはバックアップすべきファイルを受信する。たとえば、そのファイルを、バックアップ処理中に１つ以上の他のファ

イルとは別に、又は一緒に受信する。一部の実施形態においては、バックアップ管理ソフトウェアは、バックアップすべきファイルが元々記憶されているコンピュータと同じコンピュータシステム上で実行することができる。他の実施形態においては、バックアップ管理ソフトウェアは、バックアップすべきファイルが元々記憶されているコンピュータとは別のコンピュータシステム上で実行され、ネットワークを介してそのファイルを受けることができる。

【００１１】

ステップ３０３においては、バックアップ管理ソフトウェアがそのファイルをバックアップする。ファイルをバックアップするステップには、たとえばそのファイルが元々記憶されていた記憶装置とは別の１つ以上の記憶装置に記憶するなど、そのファイル中のデータを記憶するステップが含まれる。たとえばそのファイルの１つ以上のバックアップコピーは、別の１つ以上の記憶装置で作成されることがある。

【００１２】

ステップ３０５においては、第１認証情報を受けることができる。第１認証情報は、そのファイルのバックアップコピーへのアクセスを保護するために使用される。第１認証情報には、そのファイルのバックアップコピーにアクセスしようと試みる個人又はソフトウェアエージェントが、それをすることについて適正に認可されていることを検証するために利用可能な、いずれかの種類の情報が含まれる。たとえば、一部の実施形態において第１認証情報はパスワードを含む。他の実施形態においては、第１認証情報にはフィンガプリント、音声情報、網膜スキャンなどのバイオメトリック情報が含まれる。たとえば、パスワード又はバイオメトリック情報は、そのファイルが元々記憶されているコンピュータシステムのユーザーは提供することができる。

【００１３】

ステップ３０７においては、バックアップ管理ソフトウェアがバックアップされたファイルの復元に第１認証情報を要求することを示す情報を記憶する。たとえば、バックアップ管理ソフトウェアは、そのバックアップされたファイルの復元を試みる個人又はソフトウェアエージェントが第１認証情報を提供しなければならないことを示すための情報を、データベース中、又はそのファイルに関連付けられたデータ構造中に記憶することができるのである。

【００１４】

バックアップ管理ソフトウェアはさらに、第１認証情報自体、又はその第１認証情報から派生した情報も記憶することができる。たとえば、第１認証情報がパスワードを含む場合、バックアップ管理ソフトウェアはそのパスワードを（できれば暗号化された形態で）記憶する。他の例として、バックアップ管理ソフトウェアは、パスワードにハッシング関数又は他のアルゴリズムを適用し、そのハッシング関数の結果を記憶することができる。

【００１５】

ステップ３０９においては、バックアップされたファイルを復元する要求を受信する。これはたとえばステップ３０３において記憶されたファイルデータを取得し、そのデータに基づいてそのファイルを再生し、又はそのファイルの新たなバージョンを作成する要求である。たとえば、ファイルのバックアップが作られた後のある時点において復元処理が実施される時にこの要求を受けることができる。たとえば一部の実施形態においては、バックアップされたファイルの復元を要求するために、ユーザーがバックアップ管理ソフトウェアのグラフィカルユーザーインターフェース（ＧＵＩ）と交信することができる。他の実施形態においては、ユーザーが他のクライアントアプリケーションと交信してバックアップされたファイルの復元を要求すると、次にそのクライアントアプリケーションがバックアップ管理ソフトウェアと通信を行い、バックアップされたファイルの復元を要求する。

【００１６】

ステップ３１１においては、バックアップ管理ソフトウェアは第２認証情報を受ける。一部の実施形態においては、第２認証情報は、バックアップされたファイルの復元要求の

一部として受けられるてもよい。他の実施形態においては、バックアップ管理ソフトウェアがバックアップされたファイルの復元要求に呼応して第２認証情報の入力を促し、その後バックアップ管理ソフトウェアへと第２認証情報が別に提示される。たとえば、バックアップ管理ソフトウェアはバックアップされたファイルの復元要求に呼応して、ステップ３０７において記憶された情報に基づき、バックアップファイルの復元には第１認証情報を要すると判断する。よってバックアップ管理ソフトウェアは、第２認証情報を提供するように促し、これが次に、たとえば以下に説明するようにバックアップされたファイルへのアクセスの認可に用いられる。

【００１７】

ステップ３１３においては、第２認証情報が第１認証情報と一致するかどうかをバックアップ管理ソフトウェアが判定する。様々な実施形態においては、第２認証情報が第１認証情報に一致しているかどうかを判定するために、たとえば認証情報のタイプに応じてなど、いずれの種類のアルゴリズム又は技術を利用してもよい。たとえば第１認証情報が第１パスワードを含み、第２認証情報が　第２パスワードを含む場合、バックアップ管理ソフトウェアはその第２パスワードが第１パスワードと同一であるかどうかを判定する。他の例をあげると、第１認証情報が第１フィンガプリントであり、第２認証情報が第２フィンガプリントである場合、バックアップ管理ソフトウェアは分析アルゴリズムを実施して第２フィンガプリントが第１フィンガプリントと同一であるかどうかを判定する。

【００１８】

ステップ３１５に示すように、バックアップ管理ソフトウェアは、第２認証情報が第１認証情報と一致した場合には、バックアップされたファイルを復元する許可を与え、第２認証情報が第１認証情報と一致しない場合にはバックアップされたファイルの復元を拒絶する。たとえば、第２認証情報が第１認証情報と一致した場合、バックアップ管理ソフトウェアは、バックアップされたファイルのコピーを、ファイルがもともとバックアップされた記憶装置上又はコンピュータシステム上に、又は他の要求された記憶装置上又はコンピュータシステム上に作ることにより、バックアップされたファイルの復元を進める。

【００１９】

一方で、逆に第２認証情報が第１認証情報と一致しない場合、バックアップ管理ソフトウェアは、たとえばステップ３０９にて受けた要求に対して第２認証情報が一致しなかったことを示す応答を返す、及び／又は第２認証情報が一致しなかったことを示す情報を表示させることができる。

【００２０】

様々な実施形態において、図１に示すステップは組み合わせること、省くこと、又は異なる順序で実施することが可能である。たとえば第１認証情報を、ファイルがバックアップされる時に関連して様々な時に受けることができる。たとえば、一部の実施形態においては、第１認証情報をバックアップ時に受けることができる。たとえば、ファイルのバックアップが実行された時に、そのファイルが元々記憶されているコンピュータシステムのユーザーが第１認証情報を指定する。

【００２１】

他の実施形態においては、第１認証情報を、バックアップ前に受ける。たとえば、そのファイルが元々記憶されているコンピュータシステムのユーザーは、将来的なバックアップ処理においてバックアップされるファイルを保護するために使用されるパスワード又は他の認証情報を指定する。

【００２２】

他の実施形態においては、第１認証情報をバックアップ後に受ける。たとえば、そのファイルが元々記憶されているコンピュータシステムのユーザーは、既にバックアップされているファイルに関連付けるべきパスワード又は他の認証情報を指定する。

【００２３】

さらに図１の方法は、バックアップされたファイルを、復元処理以外のタイプのアクセスから保護するために利用可能である点に留意されたい。たとえば、一部の実施形態にお

いては、バックアップ管理ソフトウェアは、ユーザーがバックアップされたファイル内容を必ずしも復元することなく閲覧することができるグラフィカルユーザーインターフェースを表示するように作動可能である。パスワード又は他の認証情報がファイルに関連付けられていれば、バックアップ管理ソフトウェアは、バックアップされたファイル内容の閲覧を許可する前に、ユーザーにその認証情報の入力を要求する。

【００２４】

様々な実施形態において図１の方法は、いずれのタイプのコンピュータシステム上、又はいずれの種類のコンピューティング環境中で動作する。たとえば一部の実施形態においては、本方法は、たとえば図２に示すコンピュータシステム８２のような、単一のコンピュータシステムにおいて使用する。コンピュータシステム８２は、コンピュータシステム８２のハードドライブ又は他の記憶装置に記憶されたファイルをバックアップするよう操作可能なバックアップ管理ソフトウェアを実行する。たとえばこれを他の記憶装置上にバックアップコピーを作成することにより実施し、そのバックアップコピーはパスワード又は他の認証情報により保護される。

【００２５】

他の実施形態においては、図１の方法はネットワーク化されたコンピューティング環境中で用いることができる。たとえば、図３は、複数のクライアントコンピュータ１０２が１つのバックアップサーバコンピュータ１００と接続された例を描いたものである。各クライアントコンピュータ１０２は、複数のファイルを格納している。バックアップサーバコンピュータ１００は、クライアントコンピュータ１０２のファイルをバックアップサーバ１００へバックアップするために、各クライアントコンピュータ１０２と通信することができるバックアップ管理ソフトウェアを実行する。

【００２６】

図４は、一実施形態に基づくバックアップサーバコンピュータ１００の一例を描いたものである。バックアップサーバコンピュータ１００は、メモリ１２２に結合するプロセッサ１２０を含んでいる。一部の実施形態においては、メモリ１２２は、ダイナミックランダムアクセスメモリ（ＤＲＡＭ）又は同期型ＤＲＡＭ（ＳＤＲＡＭ）のようなＲＡＭの１つ以上の形態を含む。しかしながら、他の実施形態においては、メモリ１２２は代わりの、又は追加としての他のいずれのタイプのメモリを含むことができる。

【００２７】

メモリ１２２は、プログラム命令及び／又はデータを記憶するように構成されている。具体的には、メモリ１２２はプロセッサ１２０により実行が可能なバックアップ管理ソフトウェア１９０を記憶する。バックアップ管理ソフトウェア１９０は、図１を参照しつつ上述した処理のように、本願に記載のファイルバックアップ法の様々な態様を実施するように動作する。以下に説明するように、各クライアントコンピュータ１０２は、バックアップサーバコンピュータ１００上にあるバックアップ管理ソフトウェア１９０がファイルバックアップの実施の際に通信を行うバックアップクライアントソフトウェア１８０を実行する。

【００２８】

一部の実施形態においては、バックアップ管理ソフトウェア１９０はさらに、システム内でのファイルバックアップ処理に関わる様々な管理タスクの、管理者による実施を実現することができる。たとえば、バックアップ管理ソフトウェア１９０は、システム中の様々なクライアントコンピュータ１０２上でバックアップ処理をいつ実施するのかを指定する時間と条件を、管理者が設定することができるグラフィカルユーザーインターフェースを表示するように動作する。

【００２９】

プロセッサ１２０は、いずれのタイプのプロセッサの典型であってもよい点に留意されたい。たとえば、一実施形態におけるプロセッサ１２０はｘ８６アーキテクチャに互換性を持ち、他の実施形態におけるプロセッサ１２０はＳＰＡＲＣ™系のプロセッサに互換性を持つ。さらに一実施形態においては、バックアップサーバコンピュータ１００は複数の

プロセッサ１２０を含むものであってもよい。

【００３０】

バックアップサーバコンピュータ１００はまた、１つ以上の記憶装置１２５を含む、又はこれに結合されている。クライアントコンピュータ１０２からバックアップサーバコンピュータ１００へバックアップされるファイルは、記憶装置１２５に記憶される。様々な実施形態において記憶装置１２５は、光学式記憶装置、ハードドライブ、テープドライブなど、データを記憶するための様々な種類の記憶装置のいずれを含む。一例として、記憶装置１２５は個別に設定された１つ以上のハードディスクとして、又はディスクストレージシステムとして実現することができる。他の例としては、記憶装置１２５は１つ以上のテープドライブとして実現することができる。一部の実施形態においては、記憶装置１２５は、通信バス又はネットワークを介してバックアップサーバコンピュータ１００が通信するストレージシステム又はライブラリ装置中で作動するものであってもよい。

【００３１】

バックアップサーバコンピュータ１００はさらに、バックアップサーバコンピュータ１００のユーザーからユーザー入力を受けるための１つ以上の入力装置１２６を含んでいる。入力装置１２６は、キーボード、キーパッド、マイク又は指示装置（たとえばマウス又はトラックボール）など、様々なタイプの入力装置のいずれであってもよい。バックアップサーバコンピュータ１００はさらに、ユーザーに出力を表示するための１つ以上の出力装置１２８を含んでいる。出力装置１２８は、ＬＣＤスクリーン又はモニタ、ＣＲＴモニタなど、様々なタイプの出力装置のいずれであってもよい。

【００３２】

バックアップサーバコンピュータ１００はさらに、バックアップサーバコンピュータ１００がクライアントコンピュータ１０２へ繋がるネットワーク接続１２９を含むことができる。ネットワーク接続１２９は、たとえばそのネットワークタイプに応じ、バックアップサーバコンピュータ１００をネットワークへと繋げるためのいずれかのタイプのハードウェアを含む。様々な実施形態においては、バックアップサーバコンピュータ１００は、いずれのタイプのネットワーク又はネットワーク群の組み合わせを介してクライアントコンピュータ１０２へと接続されていてもよい。ネットワークは、たとえばローカルエリアネットワーク（ＬＡＮ）、ワイドエリアネットワーク（ＷＡＮ）、イントラネット、インターネットなど、いずれかのタイプ、又はそれらの組み合わせを含む。ローカルエリアネットワークの例としては、イーサーネット、光ファイバ分散データインターフェース（ＦＤＤＩ）ネットワーク、トークンリングネットワークが含まれる。さらに、各コンピュータは、いずれのタイプの有線又は無線接続媒体を使ってネットワークへと接続されるものでもよい。たとえば有線媒体には、イーサーネット、ファイバチャンネル、ＰＯＴＳ（音声通話のみ可能な旧来の電話サービス）に接続するモデムなどが含まれる。無線接続媒体には、衛星リンク、携帯電話サービスを通じたモデムリンク、Ｗｉ－Ｆｉ™のような無線リンク、ＩＥＥＥ８０２．１１（無線イーサーネット）やブルートゥースなどのような無線通信プロトコルを用いた無線接続が含まれる。

【００３３】

図５は、一実施形態に基づく各クライアントコンピュータ１０２の例を描いた図である。クライアントコンピュータ１０２は、上述した図４の説明と同様にメモリ１２２に結合されたプロセッサ１２０を含んでいる。メモリ１２２は、プロセッサ１２０により実行することができるバックアップクライアントソフトウェア１８０を記憶する。クライアントコンピュータ１０２はさらに、クライアントコンピュータ１０２のユーザーからのユーザー入力を受ける１つ以上の入力装置１２６と共に、ユーザーに出力を表示するための１つ以上の出力装置１２８を含んでいる。クライアントコンピュータ１０２はさらに、ファイルを記憶する１つ以上の記憶装置１２５を含むか、又はそれらに接続することができる。

【００３４】

クライアントコンピュータ１０２の記憶装置１２５からバックアップサーバコンピュータ１００へファイルをバックアップするにあたり、クライアントコンピュータ１０２上で

起動するバックアップクライアントソフトウェア１８０は、バックアップサーバコンピュータ１００上で起動するバックアップ管理ソフトウェア１９０と通信する。たとえば一部の実施形態においては、バックアップサーバコンピュータ１００上のバックアップ管理ソフトウェア１９０は、クライアントコンピュータ１０２上のバックアップクライアントソフトウェア１８０と通信することにより、バックアップすべきファイルを受ける。バックアップ管理ソフトウェア１９０はさらに、バックアップクライアントソフトウェア１８０からのファイルのバックアップコピーを保護するための第１認証情報を受ける。一部の実施形態においては、バックアップ管理ソフトウェア１９０はさらに、ファイルのバックアップコピーへのアクセスを認可するために使われる第２認証情報に加え、ファイルのバックアップコピーを復元するための後の要求もバックアップクライアントソフトウェア１８０から受ける。

【００３５】

他の実施形態においては、ファイルのバックアップコピーの復元要求は、ファイルがバックアップされるクライアントコンピュータ１０２のバックアップクライアントソフトウェア１８０以外のソースから受けることがある。たとえば一部の実施形態において、バックアップ管理ソフトウェア１９０はバックアップサーバコンピュータ１００の出力装置１２８上に管理グラフィカルユーザーインターフェース（ＧＵＩ）を表示するように動作する。このＧＵＩは、コンピューティング環境の管理者がファイルバックアップ処理に関連する様々なタスクを実施することを可能とする。たとえば、クライアントコンピュータ１０２の１つから以前にバックアップされたファイルの復元を要求するために、管理者はＧＵＩと交信する。

【００３６】

バックアップ管理ソフトウェア１９０は要求に応答して、管理者にそのファイルに関わるパスワード又は他の認証情報の入力を促す。したがって、たとえばクライアントコンピュータ１０２のユーザーにより最初にパスワードが指定されていれば、管理者が復元動作を始めるとき、バックアップ管理ソフトウェア１９０へ必要なパスワード又は他の認証情報を提供するために、ユーザーがそのパスワードを管理者に伝えるか、あるいは一緒にいる必要がある。他の実施形態においては、バックアップ管理ソフトウェア１９０はクライアントコンピュータ１０２上のバックアップクライアントソフトウェア１８０と通信するように動作し、これによりユーザーは管理者に対してパスワードを通知する必要なく、そして管理者と同じ場所にいる必要もなく、遠隔から必要な認証情報を提供することができる。たとえば一実施形態においては、管理者がバックアップサーバコンピュータ１００からの復元処理を実行すると、バックアップ管理ソフトウェア１９０がクライアントコンピュータ１０２上のバックアップクライアントソフトウェア１８０と通信を行い、これによりバックアップクライアントソフトウェア１８０がグラフィカルユーザーインターフェースを表示して、ユーザーに管理者がファイルの復元を試みていることを知らせると共に、ユーザーに必要な認証情報を管理者に代わって入力するように促す。

【００３７】

他の実施形態においては、ファイルのバックアップコピーの復元要求が、そのファイルが元々バックアップされたクライアントコンピュータ１０２以外でかつバックアップサーバコンピュータ１００でもないコンピュータシステム上で起動するソフトウェアから受信されることがある。たとえば一部の実施形態においては、バックアップサーバコンピュータ１００がウェブインターフェースを実装しており、これによりユーザーはバックアップサーバコンピュータ上１００のバックアップ管理ソフトウェア１９０と通信を行うことができ、ウェブブラウザアプリケーションを持つどのコンピュータからでも復元を実行することができるようになっている。

【００３８】

本方法の様々な実施形態においては、パスワード又は他の認証情報をバックアップサーバコンピュータ１００へバックアップされるファイルに、あらゆる所望の粒度レベルで関連付けることができる。一部の実施形態においては、バックアップサーバコンピュータ１

００に繋がる各クライアントコンピュータ１０２、又はシステムの各ユーザーに対して、１つのパスワードを関連付ける。したがって所定のクライアントコンピュータ１０２については、同じパスワード（又は他の認証情報）を使ってそのクライアントコンピュータ１０２の全ファイルを保護すること、又は、所定のユーザーに対して、同じパスワードを使ってそのユーザーに関連する全ファイルを保護することができる。

【００３９】

たとえば、図６は、バックアップクライアントソフトウェア１８０がクライアントコンピュータ１０２Ａ上にインストールされた時に、クライアントコンピュータ１０２Ａのユーザーによりパスワードが選択される実施形態を説明するものである。たとえば、インストールの過程において、ユーザーは、後のバックアップ処理でこのクライアントコンピュータ１０２Ａからバックアップされる全てのファイルを保護するために使われることになるパスワードを入力するように促される。

【００４０】

矢印１に示すように、ユーザーが指定したパスワードは、クライアントコンピュータ１０２Ａ上にバックアップクライアントソフトウェア１８０がインストールされる時点でバックアップサーバコンピュータ１００へ伝送される。矢印２に示すように、その後バックアップ処理中に１つ以上のファイルがクライアントコンピュータ１０２Ａからバックアップサーバコンピュータ１００へと送られる。矢印３に示すように、クライアントコンピュータ１０２Ａは、以前にバックアップされた１つ以上のファイルを復元する要求を後でする。矢印４に示すように、バックアップサーバコンピュータ１００はその要求に呼応して、クライアントコンピュータ１０２Ａのユーザーにパスワードを入力するように促す。よって、たとえばクライアントコンピュータ１０２上のバックアップクライアントソフトウェア１８０は、ユーザーにグラフィカルユーザーインターフェースを表示して、要求ファイルのバックアップコピーをアクセスするためのパスワードを入力するように要求する。矢印５に示すように、ユーザーが指定したパスワードがバックアップサーバコンピュータ１００へ送られる。すると、バックアップサーバコンピュータ１００は矢印５で受けたパスワードが、バックアップクライアントソフトウェア１８０がクライアントコンピュータ１０２Ａにインストールされた時点で先に指定されたパスワードと一致するかどうかを判定する。一致した場合、バックアップサーバコンピュータ１００は、矢印６に示すように要求されたファイルのデータをクライアントコンピュータ１０２Ａへ返す。クライアントコンピュータ１０２Ａ上のバックアップクライアントソフトウェア１８０はバックアップサーバコンピュータ１００から受けたデータに基づいて要求ファイルの復元コピーを生成する。

【００４１】

他の実施形態においては、ユーザーは、クライアントコンピュータ１０２Ａ上の異なるファイルについて異なるパスワード又は異なる認証情報を指定したり、又はクライアントコンピュータ１０２Ａ上の一部のファイルをパスワード保護下から外すことができる。たとえば、バックアップクライアントソフトウェア１８０は、たとえば所定のフォルダについてはそのフォルダ内にある全ファイルをそれぞれのパスワードと関連付けるなど、ユーザーが異なるフォルダに異なるパスワードを設定することを可能とするグラフィカルユーザーインターフェースを設ける。したがって、たとえばユーザーが異なるパスワードが設定された異なるフォルダからバックアップされた２つのファイルの復元を後に試みる場合、ユーザーは両方のパスワードの入力を要求される。他の実施形態においては、ユーザーはたとえばファイル毎、ドライブ毎など、別の粒度レベルにてパスワードを設定することができる。

【００４２】

一部の実施形態においては、ファイルはクライアントコンピュータ１０２から複数のバックアップサーバ１００へバックアップすることができる。たとえば、図７は３つのバックアップサーバ１００Ａ～１００Ｃが存在する例を描いたものである（この図にはクライアントコンピュータ１０２は示されていない）。一部の実施形態においては、ファイルが

所定のクライアントコンピュータ１０２からバックアップされた場合、そのファイルの複数のバックアップコピーを複数のバックアップサーバ１００上に記憶する。たとえば、ファイルの３つのバックアップコピーをサーバ１００Ａ、１００Ｂ、１００Ｃの各々に記憶することができる。各バックアップサーバ１００は、それぞれのバックアップサーバ１００からそれぞれのバックアップコピーを復元するためには、そのファイルに関連付けられたパスワード又は他の認証情報が要求されることを示す情報を記憶する場合がある。

【００４３】

他の実施形態においては、ファイルの完全なバックアップコピーを各バックアップサーバ１００に記憶する代わりに、１つのバックアップコピーを複数のバックアップサーバ１００へと分散させることができる。たとえば、ファイルをバックアップする際、そのファイルを複数のセグメントへと分割し、それらのセグメントを複数のバックアップサーバ１００に分散させる。たとえば図７のシステムにおいては、ファイルは１２セグメントへと分割し、４セグメントをバックアップサーバ１００Ａでバックアップし、他の４セグメントをバックアップサーバ１００Ｂでバックアップし、そして残りの４セグメントをバックアップサーバ１００Ｃでバックアップする。バックアップされたファイルを復元するには、クライアントコンピュータ１０２上で起動するバックアップクライアントソフトウェア１８０（又は他のコンピュータシステム上で起動する他のソフトウェア）が１つ以上のバックアップサーバ１００上で起動するバックアップ管理ソフトウェア１９０と通信を行い、たとえば上述したように認証情報を供給してバックアップされたファイルへのアクセスを得る。提供した認証情報が先にそのバックアップされたファイルと関連付けられた認証情報と一致すると、バックアップ管理ソフトウェア１９０は他のバックアップサーバ群１００と調整を行い、ファイルのバックアップされたセグメントを取得し、そのデータをクライアントコンピュータ１０２へと返すことができる。

【００４４】

様々な実施形態はさらに、命令の送受信又は記憶と、そして／又は上述に基づいてコンピュータ可読記憶媒体上に実現されたデータとを含む場合があることに留意が必要である。一般に、コンピュータ可読記憶媒体には、プログラム命令を記憶するためのディスク又はＣＤ－ＲＯＭなどの光媒体、ＲＡＭ（ＳＤＲＡＭ、ＤＤＲ　ＳＤＲＡＭ、ＲＤＲＡＭ、ＳＲＡＭなど）やＲＯＭなどの揮発性又は不揮発性媒体といった記憶媒体が含まれる。このようなコンピュータ可読記憶媒体は、伝送媒体上で送受信されるプログラム命令、又はネットワーク及び／又は無線リンクなどの通信媒体を介して運ばれる電気、電磁又はディジタル信号などの信号を記憶するものである。

【００４５】

上述した実施形態はかなり詳細に説明したものであるが、上記の開示を充分に理解することにより、当業者であれば多数の変更及び改変形態を想至し得るものである。本願請求項は、そのような変更及び改変形態を全て包含することを意図したものである。

【図面の簡単な説明】

【００４６】

【図１】バックアップされるファイルを保護するためにパスワード又は他の認証情報を用いてバックアップ処理を実施する方法の一実施形態を説明するフローチャートである。

【図２】図１の方法の一実施形態を実現することができるスタンドアロン型コンピュータシステムの一実施形態を描いた図である。

【図３】図１の方法の他の実施形態を実現するシステムの一実施形態を描いた図である。

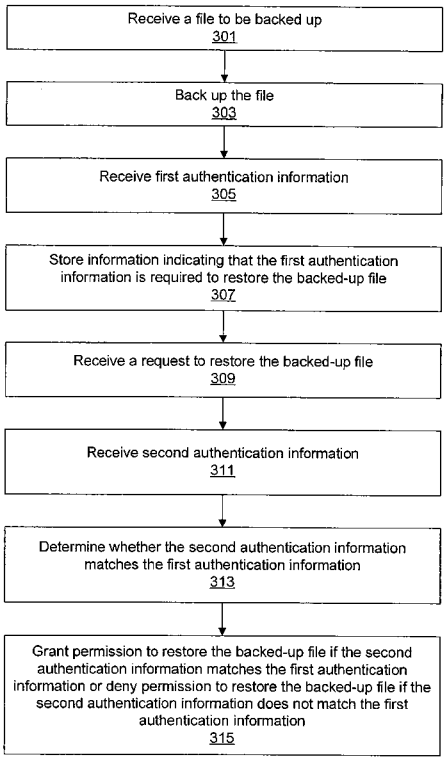
【図４】図３のシステムに示したもののような、バックアップサーバコンピュータの一例を描いた図である。

【図５】図３のシステム中に描かれているもののような、クライアントコンピュータの一例を描いた図である。

【図６】バックアップクライアントソフトウェアをクライアントコンピュータ上にインストールする際に、クライアントコンピュータのユーザーがパスワードを選択し、後のバックアップ処理において、そのパスワードがクライアントコンピュータからバックアップさ

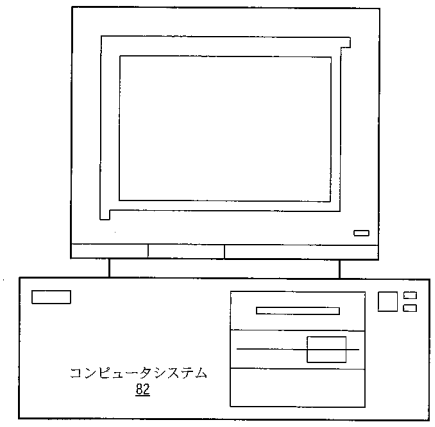
れるファイルの保護に利用されるという実施形態を描いた図である。
【図７】図１の方法の別の実施形態が実現されたシステムの別の実施形態を描いた図であって、システムは複数のバックアップサーバを含んでいる。
【符号の説明】
【００４７】
８２　コンピュータシステム
１００　バックアップサーバ
１０２Ａ～Ｄ　クライアントコンピュータ
１２０　プロセッサ
１２２　メモリ
１２５　記憶装置
１２６　入力装置
１２８　表示装置
１２９　ネットワーク接続
１８０　バックアップクライアントソフトウェア
１９０　バックアップ管理ソフトウェア

【図１】

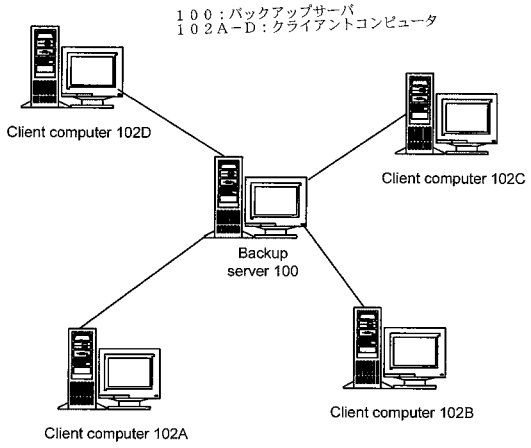


３０１：バックアップするファイルを受信
３０３：ファイルをバックアップ
３０５：第１認証情報を受ける
３０７：バックアップされたファイルを復元するためには第１認証情報が要求されたことを示す情報が記憶される
３０９：バックアップされたファイルの復元要求を受ける
３１１：第２認証情報を受ける
３１３：第２認証情報が第１認証情報と一致するかどうかが判定される
３１５：第２認証情報が第１認証情報と一致した場合はバックアップされたファイルの復元が許可される、又は第２認証情報が第１認証情報と一致しない場合はバックアップされたファイルの復元が拒絶される

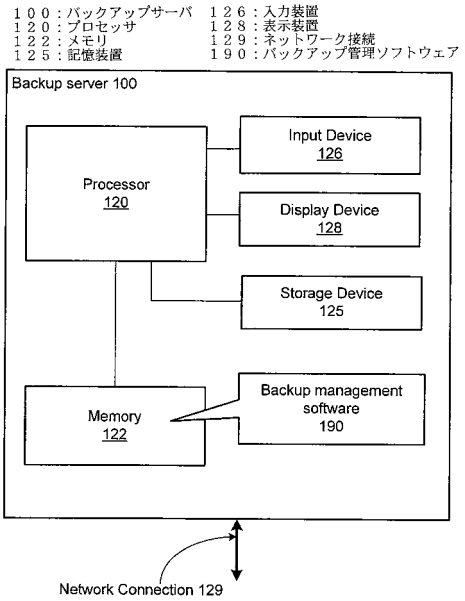
【図２】



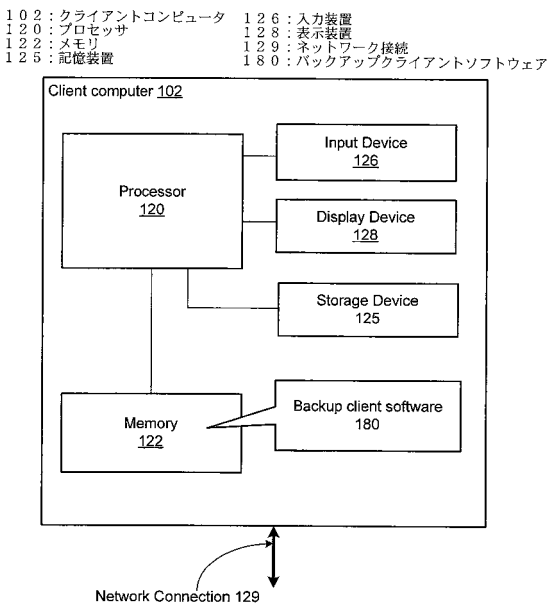
【図３】


１００：バックアップサーバ
１０２Ａ－Ｄ：クライアントコンピュータ
Client computer 102D
Client computer 102C
Backup server 100
Client computer 102A
Client computer 102B

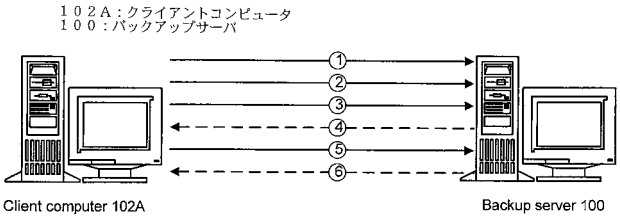
【図４】


１００：バックアップサーバ
１２０：プロセッサ
１２２：メモリ
１２５：記憶装置
１２６：入力装置
１２８：表示装置
１２９：ネットワーク接続
１９０：バックアップ管理ソフトウェア
Backup server 100
Processor 120
Input Device 126
Display Device 128
Storage Device 125
Memory 122
Backup management software 190
Network Connection 129

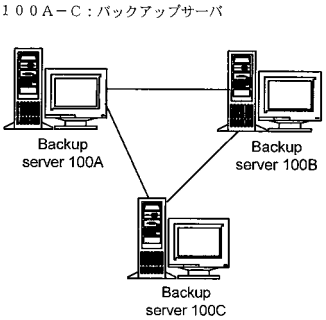
【図５】


１０２：クライアントコンピュータ
１２０：プロセッサ
１２２：メモリ
１２５：記憶装置
１２６：入力装置
１２８：表示装置
１２９：ネットワーク接続
１８０：バックアップクライアントソフトウェア
Client computer 102
Processor 120
Input Device 126
Display Device 128
Storage Device 125
Memory 122
Backup client software 180
Network Connection 129

【図６】


１０２Ａ：クライアントコンピュータ
１００：バックアップサーバ
Client computer 102A
Backup server 100

【図７】


１００Ａ－Ｃ：バックアップサーバ
Backup server 100A
Backup server 100B
Backup server 100C

フロントページの続き

Ｆターム(参考) 5B017 AA03 BA05 CA16
5B082 DE06 EA12
5J104 AA07 AA12 AA16 EA01 EA02 EA03 EA08 EA16 KA02 MA01
MA03 NA05 NA38 PA14