(19)日本国特許庁(JP)　(12)特　許　公　報(B1)　(11)特許番号

特許第4342595号
(P4342595)

(45)発行日　平成21年10月14日(2009.10.14)　(24)登録日　平成21年7月17日(2009.7.17)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601C
G06F 9/46	(2006.01)	H04L	9/00	601E
G06F 21/24	(2006.01)	G06F	9/46	350
H04L 9/14	(2006.01)	G06F	12/14	540A
		G06F	12/14	540P

請求項の数 13　(全 15 頁)　最終頁に続く

(21)出願番号　特願2008-123908 (P2008-123908)
(22)出願日　平成20年5月9日 (2008.5.9)
審査請求日　平成21年2月6日 (2009.2.6)

早期審査対象出願

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100075672
弁理士　峰　隆司

最終頁に続く

(54)【発明の名称】情報処理装置、情報処理システム、および暗号化情報管理方法

(57)【特許請求の範囲】
【請求項１】
論理的に複数に分割された記憶装置を含む計算資源にユーザ用仮想マシンおよび管理用仮想マシンを割り当て、前記ユーザ用仮想マシンおよび管理用仮想マシン内でそれぞれオペレーティングシステムが同時動作する情報処理装置であって、
前記ユーザ用仮想マシンは、
データを暗号化するための暗号鍵を生成する手段と、
前記暗号鍵を用いてデータを暗号化する暗号手段と、
前記暗号化されたデータを復号するために必要な情報を生成する情報生成手段と、
前記暗号鍵の生成を監視する監視手段と、
前記監視手段が前記暗号鍵の生成を検出した場合に、前記情報生成手段に前記情報の生成を指示する指示手段と、
前記指示手段の指示に応じて生成された情報を前記管理用仮想マシンに送信する送信手段とを有し、
前記管理用仮想マシンは、
前記送信手段から送信された情報を受信する手段と、
前記受信した情報を管理用仮想マシンに割り当てられている記憶装置に格納する手段とを有する
ことを特徴とする情報処理装置。
【請求項２】

前記送信手段が前記情報を前記管理用仮想マシンに送信した後、前記ユーザ用仮想マシン内の前記情報を削除することを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記暗号鍵は、公開鍵暗号方式でデータを暗号化するための公開鍵から構成され、
前記ユーザ用仮想マシンは、共通鍵を用いてユーザが指定したデータを暗号化する手段と、前記共通鍵を前記公開鍵によって暗号化する手段とを更に具備することを特徴とする請求項１に記載の情報処理装置。
【請求項４】
論理的に複数に分割された記憶装置を含む計算資源にユーザ用仮想マシンおよび管理用仮想マシンを割り当て、前記ユーザ用仮想マシンおよび管理用仮想マシン内でそれぞれオペレーティングシステムが同時動作する情報処理装置がネットワークに接続されている情報処理システムであって、
前記各情報処理装置の前記ユーザ用仮想マシンは、
データを暗号化するための暗号鍵を生成する手段と、
前記暗号鍵を用いてデータを暗号化する手段と、
前記暗号化されたデータを復号するために必要な情報を生成する情報生成手段と、
前記暗号鍵の生成を監視する監視手段と、
前記監視手段が前記暗号鍵の生成を検出した場合に、前記情報生成手段に前記情報の生成を指示する指示手段と、
前記指示手段の指示に応じて生成された情報を前記管理用仮想マシンに送信する送信手段とを有し、
前記各情報処理装置の前記管理用仮想マシンは、
前記送信手段から送信された情報を受信する手段と、
前記受信した情報を複数のブロックに分割し、分割された情報をネットワークに接続されている他の情報処理装置の管理用仮想マシンに分散して送信する手段と、
他の管理用仮想マシンから送信された情報を自己の管理用仮想マシンに割り当てられている記憶装置に格納する手段とを有する
ことを特徴とする情報処理システム。
【請求項５】
前記送信手段が前記情報を前記管理用仮想マシンに送信した後、前記ユーザ用仮想マシン内の前記情報を削除することを特徴とする請求項４に記載の情報処理システム。
【請求項６】
前記受信した情報を複数のブロックに分割した後、前記分割される前の情報を前記管理用仮想マシン内から削除することを特徴とする請求項４に記載の情報処理システム。
【請求項７】
前記暗号鍵は、公開鍵暗号方式でデータを暗号化するための公開鍵から構成され、
前記ユーザ用仮想マシンは、共通鍵を用いてユーザが指定したデータを暗号化する手段と、前記共通鍵を前記公開鍵によって暗号化する手段とを更に具備することを特徴とする請求項４に記載の情報処理システム。
【請求項８】
論理的に複数に分割された記憶装置を含む計算資源にユーザ用仮想マシンおよび管理用仮想マシンを割り当て、前記ユーザ用仮想マシンおよび管理用仮想マシン内でそれぞれオペレーティングシステムが同時動作する情報処理装置の暗号化情報管理方法であって、
前記ユーザ用仮想マシンによって、暗号化するための暗号鍵を生成し、
前記ユーザ用仮想マシンによって、前記暗号鍵を用いてデータを暗号化し、
前記ユーザ用仮想マシンによって、前記暗号鍵の生成を監視し、
前記ユーザ用仮想マシンによって、前記暗号鍵の生成を検出した場合に、前記暗号化されたデータを復号するために必要な情報の生成を指示し、
前記ユーザ用仮想マシンによって、前記指示に応じて前記暗号化されたデータを復号するために必要な情報を生成し、

前記ユーザ用仮想マシンによって、前記指示に応じて生成された情報を前記管理用仮想マシンに送信し、
前記管理用仮想マシンによって、前記送信手段から送信された情報を受信し、
前記管理用仮想マシンによって、前記受信した情報の少なくとも一部を管理用仮想マシンに割り当てられている記憶装置に格納する
ことを特徴とする暗号化情報管理方法。
【請求項９】
前記情報を前記管理用仮想マシンに送信した後、前記ユーザ用仮想マシン内の前記情報を削除することを特徴とする請求項８に記載の暗号化情報管理方法。
【請求項１０】
前記管理用仮想マシンによって、前記受信した情報を複数のブロックに分割し、分割された情報をネットワークに接続されている他の情報処理装置の管理用仮想マシンに分散して送信することを特徴とする請求項８に記載の暗号化情報管理方法。
【請求項１１】
他の管理用仮想マシンから送信された情報を自己の管理用仮想マシンに割り当てられている記憶装置に格納することを特徴とする請求項９に記載の暗号化情報管理方法。
【請求項１２】
前記受信した情報を複数のブロックに分割した後、前記分割される前の情報を前記管理用仮想マシン内から削除することを特徴とする請求項９に記載の暗号化情報管理方法。
【請求項１３】
前記暗号鍵は、公開鍵暗号方式でデータを暗号化するための公開鍵から構成され、
前記ユーザ用仮想マシンは、共通鍵を用いてユーザが指定したデータを暗号化する手段と、前記共通鍵を前記公開鍵によって暗号化する手段とを更に具備することを特徴とする請求項８に記載の暗号化情報管理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号鍵を生成し、暗号鍵を用いて暗号化されたデータを復元するのに必要な情報を管理する情報処理装置、情報処理システム、および暗号化情報管理方法に関する。
【背景技術】
【０００２】
Ｗｉｎｄｏｗｓ（登録商標）２０００以降のオペレーティングシステムでは、では、ＥＦＳといわれる、フォルダ、ファイル単位で暗号化を行うことができる機能をサポートしている製品がある。
【０００３】
ＥＦＳでは、管理者権限がないユーザでもファイルの暗号化を行うことができ、ファイルの暗号化を行った時に公開暗号鍵方式での暗号鍵と証明書を自動的に作成する。ファイル自体の暗号化は共通暗号鍵方式で暗号化されこの共通暗号鍵を公開暗号鍵で暗号化する。
【０００４】
また、ユーザが復号に必要な鍵を紛失した場合に備えて、暗号化されたデータを回復するのに必要な情報（以下、回復証明書）を生成し、生成された情報を用いてデータを回復することが可能である。回復証明書を別のＵＳＢドライブなどの媒体で保管するなどの機能を併用する必要がある。
【０００５】
回復証明書は、他人の手に渡ると暗号化されたデータを復元することが出来るため、取り扱いに注意が必要である。
【０００６】
特許文献１には、仮想マシンを利用した情報処理装置で、２系統の仮想マシンのうち一方にのみ機密文書を処理させることにより、気密性を保持する技術が開示されている。

【特許文献１】特開２００７－２３３７０４号公報
【発明の開示】
【発明が解決しようとする課題】
【０００７】
回復証明書は、Ｗｉｎｄｏｗｓドメイン環境下ではドメインコントローラで一括して行われる。ところが、ワークグループなどで利用されるスタンドアローン環境の場合、ユーザが、回復証明書の作成の指示／管理を実施する必要がある。
【０００８】
上述した管理は、Ｗｉｎｄｏｗｓの操作に慣れていない人にとっては、困難なことである。また、もし、回復証明書を作成出来たとしても、回復証明書の保管場所を忘れたりすることもあって、ユーザが復号に必要な鍵が壊れた場合に、回復証明書が無く、ファイルを復旧することが出来ない恐れもある。
【０００９】
本発明の目的は、暗号鍵が生成された場合に、暗号鍵を用いて暗号化されたデータを復元するのに必要な情報を管理することが可能な情報処理装置、情報処理システム、および暗号化情報管理方法を提供することにある。
【課題を解決するための手段】
【００１０】
本発明の一例に係わる情報処理装置は、論理的に複数に分割された記憶装置を含む計算資源にユーザ用仮想マシンおよび管理用仮想マシンを割り当て、前記ユーザ用仮想マシンおよび管理用仮想マシン内でそれぞれオペレーティングシステムが同時動作する情報処理装置であって、前記ユーザ用仮想マシンは、データを暗号化するための暗号鍵を生成する手段と、前記暗号鍵を用いてデータを暗号化する暗号手段と、前記暗号化されたデータを復号するために必要な情報を生成する情報生成手段と、前記暗号鍵の生成を監視する監視手段と、前記監視手段が前記暗号鍵の生成を検出した場合に、前記情報生成手段に前記情報の生成を指示する指示手段と、前記指示手段の指示に応じて生成された情報を前記管理用仮想マシンに送信する送信手段とを有し、前記管理用仮想マシンは、前記送信手段から送信された情報を受信する手段と、前記受信した情報を管理用仮想マシンに割り当てられている記憶装置に格納する手段とを有することを特徴とする。
【００１１】
本発明の一例に係わる情報処理システムは、論理的に複数に分割された記憶装置を含む計算資源にユーザ用仮想マシンおよび管理用仮想マシンを割り当て、前記ユーザ用仮想マシンおよび管理用仮想マシン内でそれぞれオペレーティングシステムが同時動作する情報処理装置がネットワークに接続されている情報処理システムであって、前記各情報処理装置の前記ユーザ用仮想マシンは、データを暗号化するための暗号鍵を生成する手段と、前記暗号鍵を用いてデータを暗号化する手段と、前記暗号化されたデータを復号するために必要な情報を生成する情報生成手段と、前記暗号鍵の生成を監視する監視手段と、前記監視手段が前記暗号鍵の生成を検出した場合に、前記情報生成手段に前記情報の生成を指示する指示手段と、前記指示手段の指示に応じて生成された情報を前記管理用仮想マシンに送信する送信手段とを有し、前記各情報処理装置の前記管理用仮想マシンは、前記送信手段から送信された情報を受信する手段と、前記受信した情報を複数のブロックに分割し、分割された情報をネットワークに接続されている他の情報処理装置の管理用仮想マシンに分散して送信する手段と、他の管理用仮想マシンから送信された情報を自己の管理用仮想マシンに割り当てられている記憶装置に格納する手段とを有する
ことを特徴とする。
【００１２】
本発明の一例に係わる暗号化情報管理方法は、論理的に複数に分割された記憶装置を含む計算資源にユーザ用仮想マシンおよび管理用仮想マシンを割り当て、前記ユーザ用仮想マシンおよび管理用仮想マシン内でそれぞれオペレーティングシステムが同時動作する情報処理装置の暗号化情報管理方法であって、前記ユーザ用仮想マシンによって、暗号化す

るための暗号鍵を生成し、前記ユーザ用仮想マシンによって、前記暗号鍵を用いてデータを暗号化し、前記ユーザ用仮想マシンによって、前記暗号鍵の生成を監視し、前記ユーザ用仮想マシンによって、前記暗号鍵の生成を検出した場合に、前記暗号化されたデータを復号するために必要な情報の生成を指示し、前記ユーザ用仮想マシンによって、前記指示に応じて前記暗号化されたデータを復号するために必要な情報を生成し、前記ユーザ用仮想マシンによって、前記指示に応じて生成された情報を前記管理用仮想マシンに送信し、前記管理用仮想マシンによって、前記送信手段から送信された情報を受信し、前記管理用仮想マシンによって、前記受信した情報の少なくとも一部を管理用仮想マシンに割り当てられている記憶装置に格納することを特徴とする。

【発明の効果】

【００１３】

本発明によれば、暗号鍵が生成された場合に、暗号鍵を用いて暗号化されたデータを復元するのに必要な情報を管理することが可能になる。

【発明を実施するための最良の形態】

【００１４】

本発明の実施の形態を以下に図面を参照して説明する。

【００１５】

（第１の実施形態）

まず、図１を参照して、本発明の第１の実施形態に係る情報処理装置の構成について説明する。この情報処理装置は、パーソナルコンピュータ１０として実現されている。コンピュータ１０には、例えば、ＸＥＮ，ＶＭＷＡＲＥなどで提供される仮想化技術（Virtual Monitor）を実行する環境が整えられている。

【００１６】

コンピュータ１０は、ハードウェア層（計算資源）１１、仮想マシンモニタ１２、ユーザ用仮想マシン２０、暗号鍵管理用仮想マシン３０等を有する。

【００１７】

ハードウェア層１１は、ディスプレイ、ハードディスクドライブ（ＨＤＤ）、ネットワークインターフェスカード、キーボード、およびマウス等を有する。

【００１８】

仮想マシンモニタ１２は、ハードウェア層１１を管理し、各仮想マシン２０，３０に対してリソース割り当てを行う。また仮想マシンモニタ１２は、ハードウェア層（計算資源）１１を論理的に複数に分割して各仮想マシンを割り当て、各仮想マシンの実行スケジュールと仮想マシンからのＩ／Ｏ要求をハードウェア層１１へ振り分ける。

【００１９】

ユーザ用仮想マシン２０は、ユーザオペレーティングシステム（ユーザＯＳ）２１、ユーザアプリケーション（ユーザＡＰＰ）２２等を有する。ユーザオペレーティングシステム２１は、ユーザが一般的に使用する環境を提供するためのオペレーティングシステムである。一般的には、ユーザオペレーティングシステム２１としては、ウインドウズ（登録商標）系のオペレーティングシステムが用いられる。ユーザアプリケーション２２は、ユーザオペレーティングシステム２１上で動作するアプリケーションソフトウェアである。

【００２０】

管理用仮想マシン３０は、サービスオペレーティングシステム３１、管理用アプリケーション（管理用ＡＰＰ）３２、および証明書管理用ストレージ３３等を有する。サービスオペレーティングシステム３１は、管理用アプリケーション３２を動作させるためのオペレーティングシステムである。例えば、Ｌｉｎｕｘ（登録商標）がサービスオペレーティングシステム３１として用いられる。証明書管理用ストレージ３３は、論理的に分割された、ハードウェア層１１を構成する記憶装置（例えば、ハードディスクドライブ）のうち、暗号鍵管理用仮想マシン３０に割り当てられている資源である。

【００２１】

なお、ユーザ用仮想マシン２０は、管理用仮想マシン３０内のデータをみることが出来

ず、データに直接アクセスすることができない。

【００２２】

ところで、ユーザオペレーティングシステム２１は、ＥＦＳ（encrypting file system）と言われる暗号化ファイルシステムでありフォルダ、ファイル単位で暗号化を行うことができる機能を提供する。

【００２３】

ＥＦＳでは、管理者権限がないユーザでもファイルの暗号化を行うことができ、ファイルの暗号化を行った時に公開暗号鍵方式での暗号鍵と証明書を自動的に作成する。ファイル自体の暗号化は共通暗号鍵方式で暗号化されこの共通暗号鍵を公開暗号鍵で暗号化する。

【００２４】

また、ユーザが紛失した場合に備えて回復エージェントによるデータ回復が可能である。回復エージェントはポリシーとしてドメインで管理することもできる。

【００２５】

図２および図３を参照して、ＥＦＳによる暗号化の手順について説明する。

【００２６】

図２は、ＥＦＳにおけるファイルまたはフォルダの暗号化を実行するＥＦＳ暗号化部を示すブロック図である。

【００２７】

図２に示すように、ＥＦＳ暗号化部は、ＥＦＳ鍵生成部４１、証明書ストア４２、データ暗号化部４３、共通暗号鍵暗号化部４４、証明書発行部４５等を有する。

【００２８】

ＥＦＳ鍵生成部４１は、公開暗号方式の暗号鍵を生成する。ＥＦＳ鍵生成部４１は暗号化証明書を生成し、証明書ストア４２に登録する。データ暗号化部４３は、ユーザが指定したファイル、またはフォルダ内のデータを共通鍵で暗号化する。共通鍵暗号化部４４は、共通鍵を公開鍵で暗号化する。暗号化された共通鍵は、所定の場所に格納される。ＥＦＳ証明書発行部４５は、暗号化ファイルシステム証明書（以下、ＥＦＳ証明書）、またはファイル回復証明書（EFS DRA 証明書）を作成する。ＥＦＳ証明書には、秘密鍵および暗号化証明書が格納される。また、ファイル回復証明書には、暗号化証明書が格納される。

【００２９】

図３は、ＥＦＳによる暗号化の手順を説明するための図である。

ユーザがファイルやフォルダ等のデータＤに対して、暗号化を設定する。すると、ＥＦＳ鍵生成部４１は、公開暗号方式の暗号鍵Ｋｅを生成する。暗号鍵Ｋｅは、公開鍵Ｋｐと秘密鍵Ｋｓとから構成される。また、暗号鍵Ｋｅの生成の伴い、ＥＦＳ鍵生成部４１は暗号化証明書ＥＣを発行する。

【００３０】

対象となるフォルダでファイルの作成、変更、移動が行われた場合、データ暗号化部は、ユーザが指定したファイル、またはフォルダ内のデータを共通鍵Ｋｃで暗号化する。

【００３１】

また、共通鍵暗号化部４４は、共通鍵Ｋｃを公開鍵Ｋｐを用いて暗号化する。暗号鍵Ｋｅおよび証明書ＥＣは、Ｗｉｎｄｏｗｓのファイルシステムで管理されている。

【００３２】

ユーザの指定により、証明書発行部は、ＥＦＳ証明書C_{EFS}、またはファイル回復証明書C_{EFS_DRA}を作成する。

【００３３】

ところで、ＥＦＳ証明書C_{EFS}、またはファイル回復証明書C_{EFS_DRA}（以下、まとめて証明書Ｃと記す）は、他人に取得されると、容易に暗号化を解除することが可能なので、安全な場所に保管する必要がある。本コンピュータ１０では、ユーザ用仮想マシン２０で作成された証明書Ｃを暗号鍵管理用仮想マシン３０で管理し、他人が証明書Ｃを盗めないようにしている。

【００３４】
以下に、ユーザ用仮想マシン２０内で作成された証明書Ｃを暗号鍵管理用仮想マシン３０で管理するための構成および処理の手順について説明する。
【００３５】
図４は、本発明の第１の実施形態に係わる証明書を管理するための構成を示すブロック図である。
【００３６】
図４に示すように、ユーザ用仮想マシン２０は、ＥＦＳ証明書発行部４５、およびファイルエクスプローラ４６、システム監視モジュール５０等を有する。データ暗号化部４１、ＥＦＳ証明書発行部４５、およびファイルエクスプローラ４６は、ユーザオペレーティングシステム２１によって提供されているソフトウェアモジュールである。
【００３７】
また、暗号鍵管理用仮想マシン３０は、仮想マシン連携部６１、および証明書管理用ストレージ３３を有する。
【００３８】
以下に、ユーザ用仮想マシン２０および暗号鍵管理用仮想マシン３０による証明書の管理処理について説明する。
【００３９】
システム監視モジュール５０は、ユーザオペレーティングシステム２１上で動作するプログラムであり、システムに常駐してオペレーティングシステム２１の動作を監視する。システム監視モジュール５０は、エクスプローラ設定監視部５１、ファイル操作監視部５２、証明書生成指示部５３、および仮想マシン連携部５４等から構成される。
【００４０】
ユーザはファイルまたはフォルダの暗号化を実施する際にファイル管理プログラム(例えばファイルエクスプローラ)４６を使用して暗号化の設定を行う。エクスプローラ設定監視部５１は、ファイルエクスプローラ４６の動作を監視し、暗号化設定が実施されたかを監視する。エクスプローラ設定監視部５１は、暗号化の設定を検出した場合、ファイル操作監視部５２を呼び出す。
【００４１】
暗号化設定が実施された場合、暗号鍵が生成されるのは暗号化対象のフォルダ内にフォルダが作成されるか、最初にファイルが作成、移動された場合となる。ファイル操作監視部５２は、ファイルエクスプローラ４６の動作を監視し、該当動作が発生した場合、証明書生成指示部５３を呼び出す。
【００４２】
証明書生成指示部５３は、ＥＦＳ証明書発行部４５に証明書Ｃの発行を指示する。証明書生成指示部５３は、発行された証明書Ｃを取得する。証明書生成指示部５３は、仮想マシン連携部５４を呼びだし、取得した証明書Ｃを仮想マシン連携部５４に渡す。
【００４３】
ユーザ用仮想マシン２０側の仮想マシン連携部５４は、証明書Ｃを暗号鍵管理用仮想マシン３０側の仮想マシン連携部６１に送信（移動）する。送信後、仮想マシン連携部５４は、ユーザ用仮想マシン２０内に残る証明書Ｃを削除する。仮想マシン連携部６１は、証明書管理用ストレージ３３に証明書Ｃを格納する。
【００４４】
以上の処理により、ユーザ用仮想マシン２０内から証明書Ｃは削除されると共に、証明書Ｃが暗号鍵管理用仮想マシン３０によって管理される。なお、ユーザ用仮想マシン２０に障害が生じ、証明書Ｃが必要な場合には、新たにインストールされたユーザ用仮想マシン２０やコンピュータ１０に接続された他のコンピュータからから情報を入力して、証明書管理用ストレージ３３内の証明書Ｃを参照する。なお、証明書の参照は、仮想マシン連携部６１を通じて行う。
【００４５】

（第２の実施形態）
上述した例では、ユーザ用仮想マシン２０と暗号鍵管理用仮想マシン３０との両方に傷害が生じた場合には、暗号化されたデータを復旧することが出来ない。本実施形態では、証明書Ｃの冗長化を図った例について説明する。
【００４６】
図５は、本発明の第２の実施形態に係わる情報処理システムの構成を示す図である。
【００４７】
図５に示すように、情報処理装置としての複数のコンピュータ７１～７８がネットワーク７９に接続されている。これらの複数のコンピュータ７１～７８は社内ＬＡＮ（有線ＬＡＮ、無線ＬＡＮ）、インターネット、移動体通信網などのネットワーク７９を経由して、お互いに通信ができる。
【００４８】
なお、各コンピュータ７１～７８は、第１の実施形態で説明したコンピュータと同様に、仮想マシンモニタ上でユーザ用仮想マシン２０および暗号鍵管理用仮想マシン３０が同時に動作する。また、各コンピュータ７１～７８のユーザ用仮想マシンの構成は、図４に示すユーザ用仮想マシン２０と同様である。また、各コンピュータ７１～７８の暗号鍵管理用仮想マシン３０の構成は、図４に示すユーザ用仮想マシン２０と同様であるが一部異なる部分があるので。
【００４９】
図６を参照して例としてコンピュータ７１の暗号鍵管理用仮想マシンの構成を説明する。なお、図６において、図４と同一な部位には同一符号を付し、その説明を省略する。
図６に示すように、暗号鍵管理用仮想マシン８０は、分散処理部８４を有する。分散処理部８４は、ユーザ用仮想マシン２０が送信した証明書ＣをＮ（Ｎ＝８）台のコンピュータ７１～７８のそれぞれの管理用仮想マシン３０に証明書Ｃを分割した分割データＣｄを分散且つ多重化して格納するための処理を実行する。証明書管理用ストレージ３３は、図４に示す証明書管理用ストレージ３３と同様に、論理的に分割された、ハードウェア層１１を構成する記憶装置（例えば、ハードディスクドライブ）のうち、暗号鍵管理用仮想マシン３０に割り当てられている資源である。
【００５０】
また、データベースファイルＤＢＦは、証明書管理用ストレージ３３に格納されている分割データに対して作成元のコンピュータの情報と、分割データＣｄが元の証明書Ｃの何番目のデータであるかを示す情報とが関連づけられている情報が格納されている。
【００５１】
次に、図７を参照して各コンピュータ７１～７８に設けられる分散処理部８４の構成を説明する。
各分散処理部８４は、分散保存設定部９１、分散保存部９２、データベース作成部９３、分割データ収集部９４、データ復元部９５、認証処理部９６、分割データ転送部９７等を有する。
【００５２】
分散保存設定部９１は、各コンピュータ７１～７８の証明書管理用ストレージ３３に証明書を分散、且つ多重化して保存する場合に、どのように証明書Ｃを分散させて保存するかを設定する。なお、分散保存設定部９１は、設定情報を各コンピュータに送信し、各コンピュータは設定情報を保存しておくようにしても良い。
【００５３】
分散保存部９２は、分散保存設定部９１が決定した設定に基づいて証明書ＣをＮ分割する。分散保存部９２は、Ｎ分割された証明書Ｃのデータを Ｎ台のコンピュータにＭ重に分散して保存する。なお、分割データＣｄの送信時、証明書Ｃの作成元のコンピュータを識別する作成元識別情報と、データが分割された元の証明書Ｃの何番目のデータであるかを示す分割情報を送る。例えば、これらの情報を送るときのパケットのヘッダに格納する。或いは、分割データＣｄの送信前後に、分割データＣｄのファイル名と、作成元識別情報

と、分割情報とを含むデータを送信する。分散保存部９２は、分割データＣｄを送信した後、元の証明書Ｃを削除する。

【００５４】

データベース作成部９３は、分割データＣｄの保存時に、分割データＣｄに対して作成元識別情報および分割情報が対応づけられた情報が格納されるデータベースデータの作成／更新を行う。データベース作成部９３は、例えば分散保存部９２がデータの送信時に送信した作成元識別情報および分割情報に基づいて、分割データＣｄに対して作成元識別情報および分割情報が関連づけられている情報を作成する。また、データベース作成部９３は、分散保存設定部９１が送信した設定情報から自己の証明書管理用ストレージ３３内に保存される分割されるデータに対して分割データＣｄに対して作成元識別情報および分割情報が関連づけられている情報を作成する。そして、データベース作成部９３は、情報に基づいて証明書管理用ストレージ３３内に保存されるデータベースデータの作成／更新を行う。なお、データベース作成部９３は、自己の証明書管理用ストレージ３３に格納された分割データに対しても作成元情報および分割情報を関連づけた情報を作成し、データベースの作成／更新を行う。

【００５５】

分割データ収集部９４は、（Ｎ－Ｍ＋１）台以上のコンピュータ７１～７８からＮ分割された分割データを選択的にＮ個集める。この時、分割データ収集手段は、自己の証明書管理用ストレージ33_1にない分割データを他のコンピュータから収集する場合に、分割データ転送要求を他のコンピュータ７２～７８に送信する。分割データ転送要求を受信した他のコンピュータ７２～７８の分割データ転送部９７は、分割データ収集部９４から要求された分割データを分割データ転送要求を送信したコンピュータ７１の暗号鍵管理用仮想マシン３０に送信する。

【００５６】

なお、分割データ転送部９７の分割データの転送に先立って、認証処理部９６が分割データ転送要求を送信したコンピュータとの間で認証処理を行う。そして、認証処理が成功した場合に、分割データ転送部９７が分割データを転送する。なお、認証処理を省略して分割データの転送を行うことも可能である。しかし、セキュリティ上、認証処理があった方が好ましい。

【００５７】

データ復元部９５は、分割データ収集部９４によって選択的に集められたＮ個の分割データを結合し元のデータを復元する。

【００５８】

図８に、証明書Ｃを分散して保存する例（Ｎ＝８，Ｍ＝４）を示す。図８に示すように、コンピュータｘ（ｘ：１～８のいずれか）は元データを生成した後、分散処理部８４は元の証明書Ｃを８個の分割データＡ～Ｈに分割する。その後、分散処理部８４は、分散保存設定部９１の設定に基づいて分割データＡ～Ｈを４重に分散して他のコンピュータに保存する。

【００５９】

この例では、コンピュータ７１の証明書管理用ストレージ33_1がデータＡ～Ｄを保存し、コンピュータ７２の証明書管理用ストレージ33_2がデータＢ～Ｅを保存し、コンピュータ７３の証明書管理用ストレージ33_3がデータＣ～Ｆを保存し、同様にコンピュータ７４～７８の証明書管理用ストレージ33_4～33_8も異なる組み合わせの４個の分割データを保存するように配信している。

【００６０】

次に、上述した手順で保存された分割データから元のデータを復元する手順について説明する。例えば、分割データ収集部９４は、各コンピュータ７１～７８の証明書管理用ストレージ３３に格納されているデータベースデータを参照し、証明書Ｃを復元するのに必要な分割データが格納されているコンピュータ７１～７８と、コンピュータ７１～７８から取得するべき分割データを検出する。そして、分割データ収集部９４は、検出されたコ

ンピュータと分散データとに基づいて、各コンピュータ７１～７８から分割データを取得する。そして、データ復元部９５は、分割データ収集部９４が収集した分散データを用いて元の証明書Ｃを復元する。

【００６１】

図９は、コンピュータｘが８台のコンピュータ７１～７８に分散して、４個ずつ保存された分割データから元の証明書Ｃを復元する場合を示したものである。また、この例では、３台のコンピュータ（コンピュータ７３，コンピュータ７５，コンピュータ７６）が、傷害等の理由でネットワークに接続されていない場合を示している。

【００６２】

図９からわかるように、コンピュータ７３が保存している分割データ（Ｃ，Ｄ，Ｅ，Ｆ）と、コンピュータ７５が保存している分割データ（Ｅ，Ｆ，Ｇ，Ｈ），コンピュータ７６が保存している分割データ（Ｆ，Ｇ，Ｈ，Ａ）に関しては、コンピュータｘはコンピュータ７３、コンピュータ７５、コンピュータ７６からネットワークを経由して参照あるいは受信することができない。

【００６３】

しかしながら、同図をみればわかるように

分割データＣは、コンピュータ７１、コンピュータ７２、およびコンピュータ７８のいずれか１つから参照あるいは受信することができる。

分割データＤは、コンピュータ７１、コンピュータ７２、およびコンピュータ７４のいずれか１つから参照あるいは受信することができる。

分割データＥは、コンピュータ７２、およびコンピュータ７４のいずれか１つから参照あるいは受信することができる。

分割データＦは、コンピュータ７４から参照あるいは受信することができる。

分割データＧは、コンピュータ７４、およびコンピュータ７７のいずれか１つから参照あるいは受信することができる。

分割データＨは、コンピュータ７７、およびコンピュータ７８のいずれか１つから参照あるいは受信することができる。

分割データＡは、コンピュータ７１、コンピュータ７７、およびコンピュータ７８のいずれか１つから参照あるいは受信することができる。

分割データＢは、コンピュータ７１、コンピュータ７２、およびコンピュータ７７のいずれか１つから参照あるいは受信することができる。

【００６４】

従って、コンピュータｘは、ネットワークに接続されている他の４台のコンピュータから、全部で８個の分割データＡ～Ｈを集めることができる。

【００６５】

このように、元の情報をＮ分割し、分割したＮ個の分割情報をＭ個ずつＮ台のコンピュータに分散して保存した場合、（Ｎ－Ｍ＋１）台以上のコンピュータが集まれば、元の証明書Ｃを復元することができる。

【００６６】

この分散ストレージでは、秘密分散により格納された証明書Ｃが分散ストレージを構成するコンピュータシステムに暗号鍵を構成する部分情報として格納されるため、情報の冗長性と秘匿性を向上することが出来る。

【００６７】

上述した実施形態では、ユーザオペレーティングシステムが、Ｗｉｎｄｏｗｓである例を示したが，他のオペレーティングシステムであっても良い。

【００６８】

なお、本発明は、上記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上記実施形態に開示されている複数の構成要素の適宜な組み合せにより種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。更に、異なる実施形

態に亘る構成要素を適宜組み合せてもよい。

【図面の簡単な説明】

【００６９】

【図１】第１の実施形態に係る情報処理装置の構成を示す図。

【図２】ＥＦＳにおけるファイルまたはフォルダの暗号化を実行するＥＦＳ暗号化部を示すブロック図。

【図３】ＥＦＳによる暗号化の手順を説明するための図。

【図４】第１の実施形態に係わる証明書を管理するための構成を示すブロック図。

【図５】第２の実施形態に係わる情報処理システムの構成を示す図。

【図６】暗号鍵管理用仮想マシンの構成を示す図。

【図７】第２の実施形態に係わる分散処理部の構成を示すブロック図。

【図８】データを８分割して、各分割データを８個のコンピュータに４重に分散して保存する例を示す図。

【図９】分割データから元の証明書を復元する例を示す図。

【符号の説明】

【００７０】

１０…パーソナルコンピュータ，１１…ハードウェア層，１２…仮想マシンモニタ，２０…ユーザ用仮想マシン，２０．３０…仮想マシン，２１…ユーザオペレーティングシステム，２２…ユーザアプリケーション，３０…暗号鍵管理用仮想マシン，３１…サービスオペレーティングシステム，３２…管理用アプリケーション，３３…証明書管理用ストレージ，４１…データ暗号化部，４５…ＥＦＳ証明書発行部，４６…ファイルエクスプローラ，５０…システム監視モジュール，５１…エクスプローラ設定監視部，５２…ファイル操作監視部，５３…証明書生成指示部，５４…仮想マシン連携部，６１…仮想マシン連携部，７１～７８…コンピュータ，７１…コンピュータ，８０…暗号鍵管理用仮想マシン，８４…分散処理部，９１…分散保存設定部，９２…分散保存部，９３…データベース作成部，９４…分割データ収集部，９５…データ復元部，９６…認証処理部，９７…分割データ転送部。

【要約】

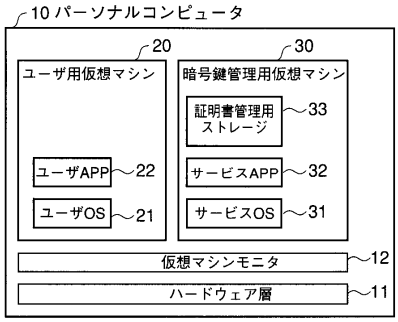
【課題】暗号鍵が生成された場合に、暗号鍵を用いて暗号化されたデータを復元するのに必要な情報を管理すること。

【解決手段】ファイル操作監視部５２は、ファイルエクスプローラ４６を監視することによって、暗号鍵の生成を監視する。暗号鍵の生成を検出した場合に、証明書生成指示部５３は、証明書Ｃの生成をＥＦＳ証明書発行部４５に指示する。ＥＦＳ証明書発行部４５は、前記指示に応じて前記暗号化されたデータを復号するために必要な証明書Ｃを発行する。仮想マシン連携部５４は、証明書Ｃを暗号鍵管理用仮想マシン３０に送信する。仮想マシン連携部６１は、ユーザ用仮想マシン２０から送信された証明書Ｃを受信し、証明書Ｃを管理用仮想マシンに割り当てられている証明書管理用ストレージ３３に格納する。

【選択図】　図４

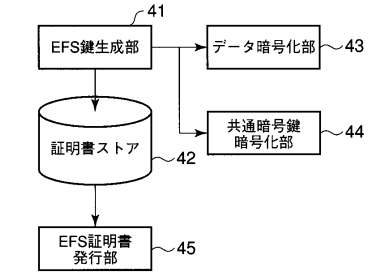
【図１】

図１



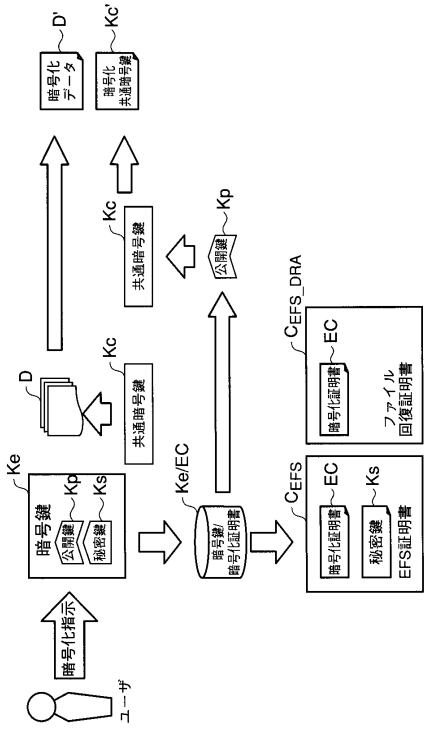
【図２】

図２



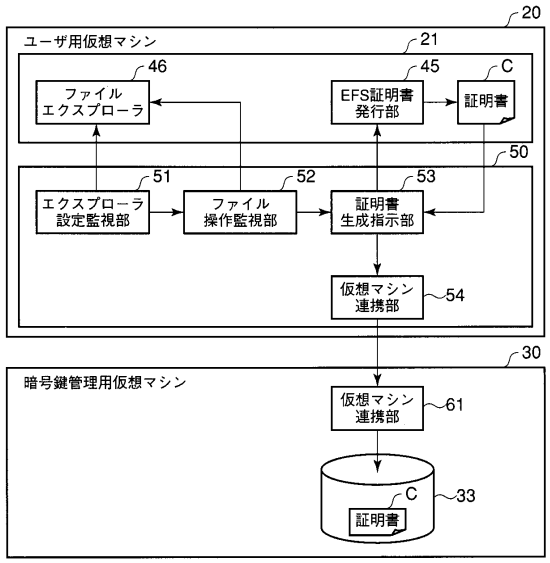
【図３】

図３



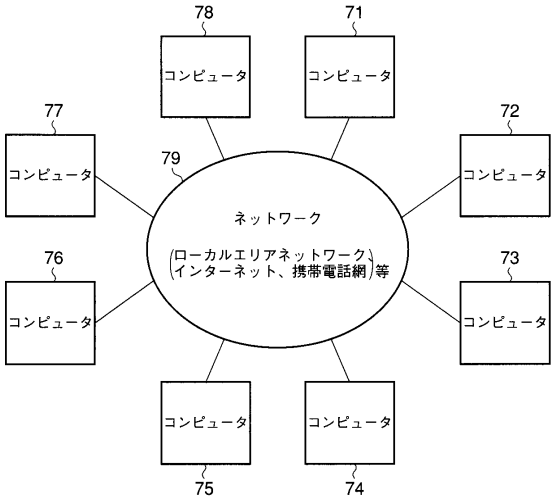
【図４】

図４



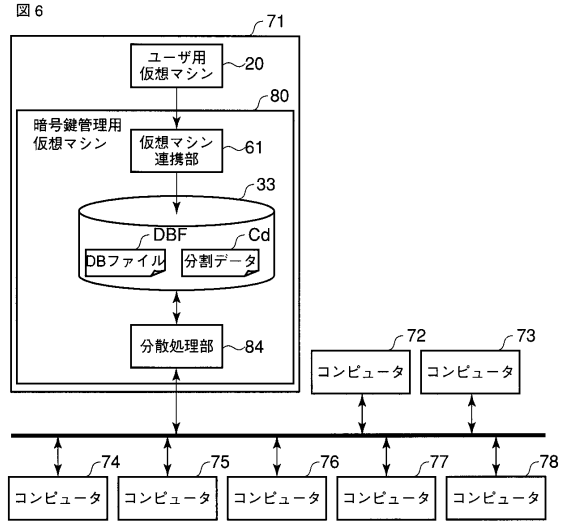
【図５】

図５



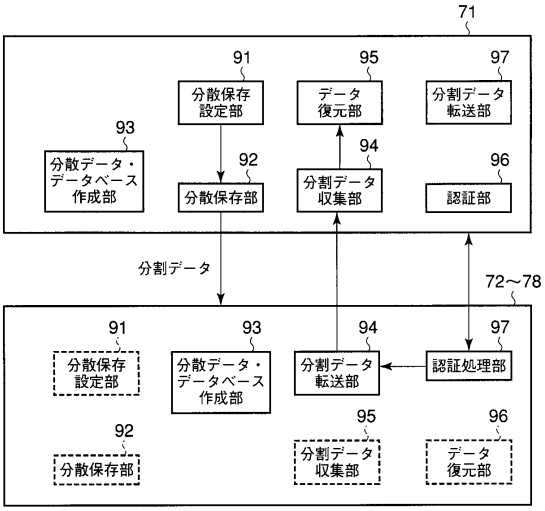
【図６】

図６



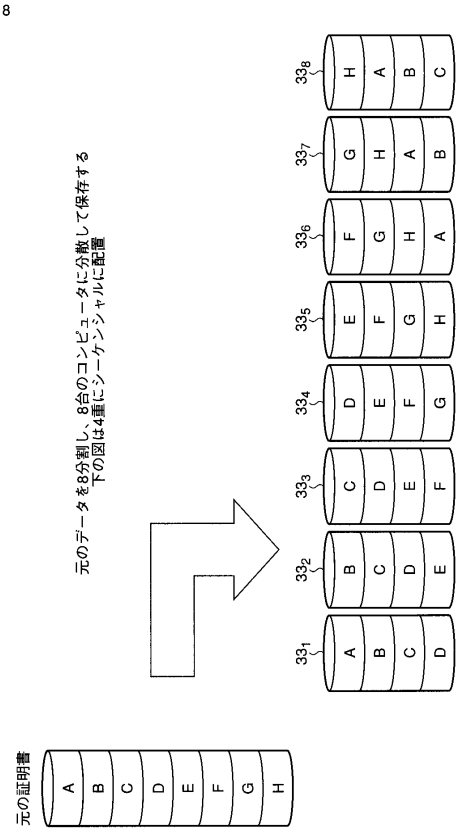
【図７】

図７



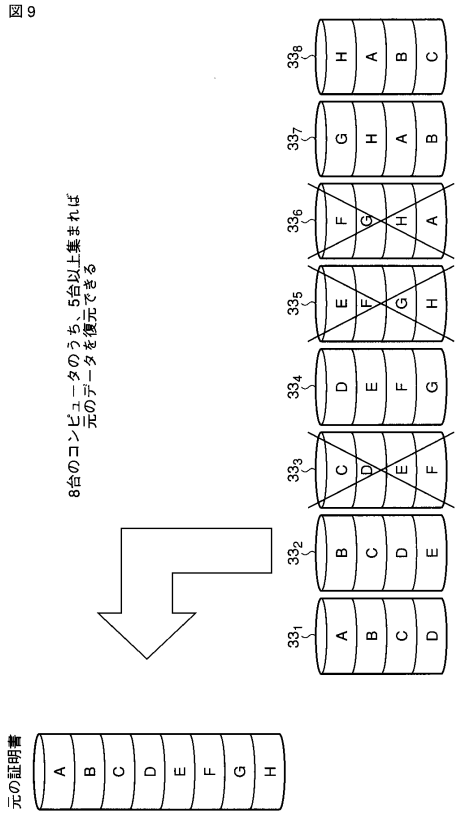
【図８】

図８



【図９】

図９



フロントページの続き

(51)Int.Cl. FI

G06F	12/14	510F
G06F	12/14	560D
G06F	12/14	540B
H04L	9/00	641
H04L	9/00	601F

(74)代理人 100095441
弁理士 白根 俊郎
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100119976
弁理士 幸長 保次郎
(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100140176
弁理士 砂川 克
(74)代理人 100101812
弁理士 勝村 紘
(74)代理人 100092196
弁理士 橋本 良郎
(74)代理人 100100952
弁理士 風間 鉄也
(74)代理人 100070437
弁理士 河井 将次
(74)代理人 100124394
弁理士 佐藤 立志
(74)代理人 100112807
弁理士 岡田 貴志
(74)代理人 100111073
弁理士 堀内 美保子
(74)代理人 100134290
弁理士 竹内 将訓
(74)代理人 100127144
弁理士 市原 卓三
(74)代理人 100141933
弁理士 山下 元
(72)発明者 野々山 明広
東京都港区芝浦一丁目１番１号 株式会社東芝内
(72)発明者 嘉村 幸一郎
東京都港区芝浦一丁目１番１号 株式会社東芝内

審査官 中里 裕正

(56)参考文献 特開２００７－２３３７０４（ＪＰ，Ａ）
特開２００８－０４６８８７（ＪＰ，Ａ）

特開２００６－１２００８９（ＪＰ，Ａ）
Encrypting File System, Mcrosoft TechNet, Microsoft Corporation, ２００８年　5月　1日, ＵＲＬ, http://technet.microsoft.com/en-us/library/cc721923.aspx
EFS を使用したハード ドライブの暗号化でデータを保護する, Microsoft Corporation, ２００５年　3月１７日, ＵＲＬ, http://www.microsoft.com/japan/smallbiz/sgc/articles/protect_data_efs.mspx
Gaspare Sala, Daniele Sgandurra, Fabrizio Baiardi, Security and Integrity of a Distributed File Storage in a Virtual Environment, Fourth International IEEE Security in Storage Workshop, 2007. SISW '07., IEEE, ２００７年１１月２７日, pp.58-69
鶴岡　行雄　Yukio　Tsuruoka, 仮想マシンを用いた暗号トークンの実装　Implementation of Cryptographic Token using Virtual Machine, 情報処理学会研究報告　IPSJ SIG Technical Reports, 日本, 社団法人情報処理学会　Information Processing Society of Japan, ２００８年　3月　6日, Vol.2008, No.21, pp.85-90

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｆ　２１／２４
Ｇ０６Ｆ　９／４６