(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2006-48158
(P2006-48158A)
(43)公開日　平成18年2月16日(2006.2.16)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	510F	5B017
		G06F	12/14	540A	

審査請求 未請求　請求項の数 10　OL　（全 16 頁）

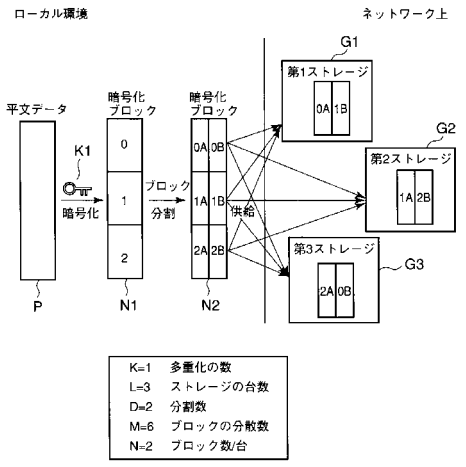
(21)出願番号　特願2004-224487 (P2004-224487)
(22)出願日　平成16年7月30日 (2004.7.30)

(71)出願人　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　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100075672
弁理士　峰　隆司
(74)代理人　100109830
弁理士　福原　淑弘

最終頁に続く

(54)【発明の名称】データ格納方法及びデータ処理装置

(57)【要約】
【課題】事故等に対するデータ保存の強化と共に、不正な第三者の暗号破りに対しても十分なセキュリティをもたせることができるデータ格納方法を提供する。
【解決手段】データを複数のストレージに分割して格納するデータ格納方法であり、平文データに第１暗号鍵に基づくブロック暗号化を施すことにより、暗号化ブロックを単位とする複数の暗号化ブロックへ暗号化し、複数の暗号化ブロックを複数の分割暗号化ブロックへとそれぞれ分割し、複数の分割暗号化ブロックをネットワークを介して複数のストレージに分散して供給し格納させるデータ格納方法。
【選択図】図１



【特許請求の範囲】
【請求項１】
データを所定数のストレージに分割して格納するデータ格納方法であり、
平文データに第１暗号鍵に基づくブロック暗号化を施すことにより、暗号化ブロックを単位とする複数の暗号化ブロックへ暗号化し、
前記複数の暗号化ブロックを、第２所定数により、複数の分割暗号化ブロックへとそれぞれ分割し、
前記複数の分割暗号化ブロックを、ネットワークを介して複数のストレージに分散して供給し格納させることを特徴とするデータ格納方法。
【請求項２】
前記平文データに基づく複数の分割暗号化ブロックは、２以上の整数である多重化数に多重化した上で、前記所定数のストレージに分散して供給し格納させることで、前記所定数のストレージの少なくとも一台が再生不可能となっても、残りのストレージから前記複数の分割暗号化ブロックを回収して復号することで前記平文データの全てを復元することを特徴とする請求項１記載のデータ格納方法。
【請求項３】
前記複数の分割暗号化ブロックの配列を並べ替えた上で、このときの並べ替え情報を暗号化し分散して、前記分割暗号化ブロックと共に前記複数のストレージに格納することを特徴とする請求項１記載のデータ格納方法。
【請求項４】
前記ネットワークを介して前記複数のストレージに働きかけることで、前記複数のストレージに格納された前記複数の分割暗号化ブロックを受信して取得し、
前記複数の分割暗号化ブロックを結合させて、前記複数の暗号化ブロックを復元し、
前記複数の暗号化ブロックを前記第１暗号鍵で前記平文データに復号することで、前記平文データを復元することを特徴とする請求項１記載のデータ格納方法。
【請求項５】
前記複数の分割暗号化ブロックの配列を並べ替え、このときの並べ替え情報と、前記複数のストレージへの前記分割暗号化ブロックの配分を示す第１ストレージアドレス情報とを復元情報とし、この復元情報を第２暗号鍵に基づいて暗号化復元情報に暗号化し、
前記暗号化復元情報を分割して前記分割暗号化ブロックと共に前記複数のストレージに格納し、
前記暗号化復元情報の前記複数のストレージへの配分を示す第２ストレージアドレス情報と前記第２暗号鍵とを復元予備情報として保存し、
前記平文データの復元の際には、前記復元予備情報を読み出し、前記第２ストレージアドレス情報に基づき、前記ネットワークを介して前記複数のストレージに働きかけることで、前記暗号化復元情報を取得し前記第２暗号鍵で復号し、この復元情報の前記第１ストレージアドレスに基づいて、前記複数のストレージに格納された前記複数の分割暗号化ブロックを受信して取得し、
前記複数の分割暗号化ブロックを前記並べ替え情報に基づき順番を並べ替え、更に、前記複数の分割暗号化ブロックを結合させて前記暗号化ブロックを復元し、前記暗号化ブロックを前記第１暗号鍵で前記平文データに復号することで、前記平文データを復元することを特徴とする請求項１記載のデータ格納方法。
【請求項６】
データをネットワーク上の所定数のストレージに分割し格納するデータ処理装置であり、
平文データに第１暗号鍵に基づくブロック暗号化を施すことにより、暗号化ブロックを単位とする複数の暗号化ブロックへ暗号化する暗号化部と、
平文データに第１暗号鍵に基づくブロック暗号化を施すことにより、暗号化ブロックを単位とする複数の暗号化ブロックを生成する分割部と、
前記複数の分割暗号化ブロックを、ネットワークを介して複数のストレージに分散して

供給し格納させる通信部とを具備することを特徴とするデータ処理装置。
【請求項７】
前記平文データに基づく複数の分割暗号化ブロックは、２以上の整数である多重化数に多重化した上で、前記所定数のストレージに分散して供給し格納させることで、前記所定数のストレージの少なくとも一台が再生不可能となっても、残りのストレージから前記複数の分割暗号化ブロックを回収して復号することで前記平文データの全てを復元する多重化部を更に有することを特徴とする請求項６記載のデータ処理装置。
【請求項８】
前記複数の分割暗号化ブロックの配列を並べ替えた上で、このときの並べ替え情報を暗号化し分散して、前記分割暗号化ブロックと共に前記複数のストレージに格納する並べ替え部を更に有することを特徴とする請求項６記載のデータ処理装置。
【請求項９】
前記ネットワークを介して前記複数のストレージに働きかけることで、前記複数のストレージに格納された前記複数の分割暗号化ブロックを受信して取得し、
前記複数の分割暗号化ブロックを結合させて、前記複数の暗号化ブロックを復元し、
前記複数の暗号化ブロックを前記第１暗号鍵で前記平文データに復号することで、前記平文データを復元するべく各部を制御する制御部を更に有することを特徴とする請求項６記載のデータ処理装置。
【請求項１０】
前記複数の分割暗号化ブロックの配列を並べ替え、このときの並べ替え情報と、前記複数のストレージへの前記分割暗号化ブロックの配分を示す第１ストレージアドレス情報とを復元情報とし、この復元情報を第２暗号鍵に基づいて暗号化復元情報に暗号化し、
前記暗号化復元情報を分割して前記分割暗号化ブロックと共に前記複数のストレージに格納し、
前記暗号化復元情報の前記複数のストレージへの配分を示す第２ストレージアドレス情報と前記第２暗号鍵とを復元予備情報として保存し、
前記平文データの復元の際には、前記復元予備情報を読み出し、前記第２ストレージアドレス情報に基づき、前記ネットワークを介して前記複数のストレージに働きかけることで、前記暗号化復元情報を取得し前記第２暗号鍵で復号し、この復元情報の前記第１ストレージアドレスに基づいて、前記複数のストレージに格納された前記複数の分割暗号化ブロックを受信して取得し、
前記複数の分割暗号化ブロックを前記並べ替え情報に基づき順番を並べ替え、更に、前記複数の分割暗号化ブロックを結合させて前記暗号化ブロックを復元し、前記暗号化ブロックを前記第１暗号鍵で前記平文データに復号することで、前記平文データを復元するべく各部を制御する制御部を更に有することを特徴とする請求項６記載のデータ処理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データを分割して複数のストレージへ格納するデータ格納方法に関し、特に、ブロック暗号で生成した暗号化ブロックを更に分割して複数ストレージに分散させるデータ格納方法及びデータ処理装置に関する。
【背景技術】
【０００２】
最近、多くの種類のデジタル情報機器が普及し盛んに利用されてきているという状況があり、このようなデジタル情報機器においては、大量のデジタルデータをセキュリティを確保しながら確実に保存し再生することが求められてきている。このような技術として、一つのストレージだけではなく、複数のストレージにデータを分散して格納する技術が知られている。
【０００３】
特許文献１には、ファイルを複数に分割して、これを複数のストレージに分散して格納

する技術が示されており、単に一つのストレージに格納した際に、ストレージが失われると情報も同時に消失することを防いでいる。
【特許文献１】特開２００４－２９９３４号公報。
【発明の開示】
【発明が解決しようとする課題】
【０００４】
従来技術においては、一つのストレージを失っても、他のストレージからデータを復元することができるように、複数のストレージに分散してデータを分割しているので、一つのストレージを失ってもデータを復活することができる。しかしながら、データの復活のためのデータの分割処理であるため、第三者に対する十分なセキュリティを得ることができないという問題がある。
【０００５】
本発明は、事故等に対するデータ保存の強化と共に、不正な第三者の暗号破りに対しても十分なセキュリティをもたせることができるデータ格納方法及びデータ処理装置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】
【０００６】
本発明の一実施形態に係るデータ格納方法は、データを所定数のストレージに分割して格納するデータ格納方法であり、平文データに第１暗号鍵に基づくブロック暗号化を施すことにより、暗号化ブロックを単位とする複数の暗号化ブロックへ暗号化し、前記複数の暗号化ブロックを、第２所定数により、複数の分割暗号化ブロックへとそれぞれ分割し、前記複数の分割暗号化ブロックを、ネットワークを介して複数のストレージに分散して供給し格納させることを特徴とするデータ格納方法である。
【発明の効果】
【０００７】
上記したデータ格納方法においては、平文データの暗号化処理にブロック暗号を用いて、これにより生成した暗号化ブロックをそのまま複数のストレージに分配するのではなく、少なくとも暗号化ブロックを所定数Ｄ（２又は３等）により分割して、複数ストレージに分散して供給する。これにより、不当な第三者は、一つのストレージにより、幾つかの分割暗号化ブロックを入手したとしても、暗号化ブロックが分割されているため、この分割暗号化ブロックを復号することは、著しく困難となる。従って、この暗号化ブロックの分割処理により、第三者の暗号破りに対する十分なセキュリティを得ることが可能となる。
【０００８】
なお、暗号の際の鍵情報、分割情報、並べ替え情報、アドレス情報等である復元情報の分散処理、更に、この復元情報を暗号化する際の暗号鍵及びアドレス情報を管理する復元予備情報等を更に用いることにより、このデータ格納方法のセキュリティを一層向上させることができ、第三者のデータの盗用を非常に困難にさせるものである。
【発明を実施するための最良の形態】
【０００９】
以下、この発明の一実施形態について図面を参照して詳細に説明する。
図１は、本発明の一実施形態に係るデータ格納方法の一例を示す説明図、図２は、同じくデータ格納方法を示す説明図、図３は、同じくデータ格納方法を示す説明図、図４は、同じくデータ格納方法を示す説明図、図５は、同じくデータ格納方法において、ストレージを破損した際の復活処理を示す説明図、図６は、同じくデータ格納方法において、５台のストレージに４重化して保存する場合を示す説明図、図７は、同じくデータ格納方法において、５台のストレージに４重化して保存した際のストレージ破損に対する復元処理を示す説明図、図８は、同じくデータ格納方法を、復元情報と共に示す説明図、
図９は、同じくデータ格納方法の復元方法の一例を示す説明図、図１０は、同じく３分割を行うデータ格納方法を示す説明図、図１１は、同じくデータ格納方法を行う情報処理装

置の構成の一例を示すブロック図、図１２は、同じくデータ格納方法の際の、ストレージ１台当たりの分割ブロック数を決定するフローチャート、図１３は、同じくデータ格納方法の一例を示すフローチャート、図１４は、同じくデータ格納方法に対する復元方法の一例を示すフローチャートである。

【００１０】

（データ処理装置）

はじめに、本発明の一実施形態に係るデータ格納方法が、一例として、図１１に示すデータ処理装置１００等の構成を用いて行われる場合を図面を用いて、詳細に説明する。データ処理装置１００は、図１１において、平文データＰ等を格納するハードディスドライバ等の記憶部１１１と、この平文データＰを暗号化し又暗号化データを復号する暗号化復号部１１２と、暗号化した暗号化データを更に２次暗号化データに分割し又これを結合させるブロック分割・結合部１１３と、暗号化データを所定の順序で並べ替え又これを復元する並べ替え・復元部１１４と、全体の動作を司る制御部１１５と、外部との通信を行うＩ／Ｆ部１１６と、これに接続され例えばインターネットを介してそれぞれ接続される第１ストレージＧ１乃至第３ストレージＧ３とを有している。

【００１１】

（データ格納方法のパラメータ）

次に、この実施形態に係る主要なパラメータを以下のように表記する。

【００１２】

多重化の数　　：Ｋ（≧１、推奨は≧２）
ストレージの台数　　：Ｌ（≧Ｋ＋１）
暗号化ブロックの分割数：Ｄ
データの分散数　　：Ｍ（≧Ｋ＋１）＝Ｄ×ａ
分割ブロック数／台　　：Ｎ（≧（ＫＭ）／Ｌ、≦Ｍ－１）

多重化の数Ｋは、ネットワーク全体でデータが多重化されている数を表す。断片化されたデータが全てネットワーク上に少なくとも２個ずつあればＫ＝２であり、少なくとも３個ずつあればＫ＝３である。

【００１３】

ストレージ台数Ｌは、ネットワーク上に存在しデータの読み書きが可能な台数を指し、ローカル環境のストレージは含まない。この台数Ｌは、多重化の数Ｋよりも大きな値となる。これは同値以下では１つのストレージにデータの全てが置かれるか、又は同じデータを重複しておくという、この実施形態で意図していない状態となってしまうからである。

【００１４】

データの分散数Ｍはデータ全体を幾つに分散するかを示しており、これは多重化の数よりも大きくなくてはならない。理由はストレージ台数Ｌと同じように、同値以下では１つのストレージにデータの全てが置かれるか、又は同じデータを重複しておくという、この実施形態で意図していない状態となってしまうからである。

【００１５】

ストレージ１台あたりの分割ブロック数Ｎは、各ネットワーク上のストレージＧ１乃至Ｇ３に分割暗号化ブロックの断片を幾つ保存するかを示し、Ｋ，Ｌ，Ｄ，Ｍの値によって一定の範囲に制限される。ただし、この値はデータの同一の断片が１台のストレージに複数置かれることはないものとして数える。

【００１６】

又、各ストレージに保存される分割ブロックの組み合わせは、ストレージ間で可能な限り異なっているほうが望ましい。十分な種類の組み合わせがないのに、同一の組み合わせが存在する場合には、ストレージ損壊時のロバストネスの低下に繋がる場合がある。１つの基準としては${}_{M}C_{N} \geqq L$の場合は全てのストレージで異なる分割暗号化ブロックの組み合わせであることが望ましい。逆に十分な種類の組み合わせが存在するように分割暗号化ブロックの断片を分散させれば、（Ｋ－１）台のストレージが破損しても、データを復元することができる。

【００１７】
（データ格納方法：第１実施形態：図１）
次に、このデータ格納方法の第１実施形態として、図１を用いて、Ｋ＝１、Ｌ＝３、Ｄ＝２、Ｍ＝６、Ｎ＝２の場合のネットワークストレージへの保存法を示す。ローカル環境であるデータ処理装置１００によりネットワークストレージＧ１，Ｇ２，Ｇ３に対してデータを保存する場合、データ処理装置１００は、記憶部１１１等に保存されている平文データＰを第１暗号鍵Ｋ１により、例えば、ＣＢＣ暗号化等のブロック暗号処理を施し、３つの暗号化ブロック“０”、“１”、“２”を生成する。次に、この３つの暗号化ブロックＮ１を、分割数Ｄ＝２でそれぞれ二分割した暗号化ブロックＮ２を生成する。そして、Ｉ／Ｆ部１１６を介して、ネットワーク上の第１乃至第３ストレージＧ１乃至Ｇ３にそれぞれ分散して保存する。この際に、分散された暗号化ブロックＮ２について、例えば、暗号化ブロック０Ａは、第１ストレージＧ１とすると、その後に、暗号化ブロック０Ｂを供給するのではなく、暗号化ブロック１Ｂを供給する。このように分割暗号化ブロックを１つ（又はそれ以上）ずらした上で、複数のストレージに分散して供給することにより、不当な第三者が第１ストレージＧ１のみを取得したとしていも、連続した分割暗号化ブロック０Ａ，０Ｂが得られないため、暗号化ブロックを復元することができないので、暗号化ブロックの復号を著しく困難とするため、セキュリティを向上させることが可能となるものである。
【００１８】
この例で示された分割暗号化ブロックＮ２の分散は、一例であり、これは異なる方式でも構わないし、並びを記録した変換表を持つなど復元時に並びを元に戻す方法があれば、よりランダムな方法でも構わず、本発明に係る実施形態では、この方法について特に制限はしない。
【００１９】
又、ここで、暗号化ブロックＮ１の暗号化ブロックの分割処理は、任意に分割数を選ぶことができ、図１０に示すように分割数Ｄ＝３とした時は、暗号化ブロックＮ１の暗号化ブロックは暗号化ブロックＮ５の暗号化ブロックとして３分割され、各ストレージＧ１乃至Ｇ３に分配されるものである。
【００２０】
又、ここで用いる暗号化方法は共通暗号鍵Ｋ１を用いたＣＢＣ暗号に分類されるものが望ましいが、１ブロックのサイズや鍵のビット数は任意のものでかまわない。又、ここでは、ブロック暗号は、一例としてＣＢＣ暗号としたが、必ずしもＣＢＣ暗号に制限する必要はなく、他のブロック暗号を用いる場合も、同様な効果を期待することができる。なお、ＣＢＣ暗号のように、一つの暗号化ブロックが他のブロックのデータを利用して暗号化する方法によれば、一つのブロックだけを取得しても、これによって完全な復号ができないため、高いセキュリティを実現することができる。従って、あるブロックの暗号化に、他のブロックの平文または演算経過のデータを用いる連鎖的な暗号が好適である。
【００２１】
しかしながら、ＣＢＣ暗号のように他のブロックのデータを利用する暗号化方法でなく、一つのブロックだけで完結するブロック暗号であっても、暗号化ブロックが分割され分散されて格納されるので、第三者の暗号破りに対する高いセキュリティを持たせることが可能となる。
又、更に、所定のデータ単位で暗号化され、復号の際に、このデータ単位で復号されることを要求する暗号処理であれば、必ずしもブロック暗号という称号を必要とするものではなく、ＣＢＣ暗号を用いた場合と同等の作用効果を示すものである。
【００２２】
（データ格納方法：第２実施形態：図２）
次に、このデータ格納方法の多重化を伴う第２実施形態として、図２を用いて、Ｋ＝２、Ｌ＝３、Ｄ＝２、Ｍ＝６、Ｎ＝４の場合のネットワークストレージへの保存法を示す。ここでは、多重化数Ｋ＝２として、ローカル環境であるデータ処理装置１００によりネッ

トワークストレージＧ１，Ｇ２，Ｇ３に対してデータを保存する場合を示している。

【００２３】

ここでは、３つに分けて並び替えられた暗号化ブロックＮ１の暗号化ブロック“０”、“１”、“２”を、分割数Ｄ＝２でそれぞれ二分割し、Ｍ＝６として、６つに分散された暗号化ブロックＮ２を得るまでは、第１実施形態の図１のデータ格納方法と同様である。しかし、その後、暗号化ブロックＮ２を多重化数Ｋ＝２として２倍に多重化して、三つのストレージＧ１乃至Ｇ３に供給するものである。このため、ストレージ１台当たりの分割ブロック数Ｎ＝４となり、データが多重化されて複数のストレージＧ１乃至Ｇ３に格納されることとなる。

【００２４】

これにより、例えば、ストレージＧ２が故障したとしても、ストレージＧ１とＧ３とのデータを読み出しこれらを合成することで、全ての暗号化ブロックＮ２を得ることができ、これを更に第１暗号鍵Ｋ１で復号することで、初めの平文データＰを復元することが可能となる。

【００２５】

又、第１実施形態と同様に、暗号化ブロックを分割数Ｄで分割しずらした上で複数のストレージに分散して供給することで、同様に、不当な第三者に対するセキュリティ向上を図るものである。

【００２６】

（データ格納方法：第３実施形態：図３）

次に、このデータ格納方法の多重化及び並べ替えを伴う第３実施形態として、図３を用いて、Ｋ＝２、Ｌ＝３、Ｄ＝２、Ｍ＝６、Ｎ＝４の場合のネットワークストレージへの保存法を示す。ここでは、多重化数Ｋ＝２として、ローカル環境であるデータ処理装置１００によりネットワークストレージＧ１，Ｇ２，Ｇ３に対してデータを保存する場合を示している。

【００２７】

データ処理装置１００は、記憶部１１１等に保存されている平文データＰを第１暗号鍵Ｋ１によりＣＢＣ暗号化を行い、例えば２５個の暗号化ブロックＮ１１を生成する。そして、分割数Ｄ＝２でそれぞれ二分割した暗号化ブロックＮ１２とする。

【００２８】

更に、これらの複数の暗号化ブロックＮ１２を、３ｎ、３ｎ＋１、３ｎ＋２（ｎ＝０，・・・）番目のデータのように、任意の並べ替え方法により３つに分けて並べ替え、暗号化ブロックＮ１３を得る。次に、並べ替えられた暗号化ブロックＮ１３を、多重化数Ｋ＝２で多重化して、３つのストレージＧ１乃至Ｇ３に、１台当たりの分割ブロック数Ｎ＝４として４つずつ保存する。

【００２９】

これにより、図５に示すように、例えば、ストレージＧ２が故障したとしても、ストレージＧ１とＧ３とのデータを読み出しこれらを合成することで、全ての暗号化ブロックＮ２を得ることができ、これを更に第１暗号鍵Ｋ１で復号することで、初めの平文データＰを復元することが可能となる。

【００３０】

又、図４に示すように、第１実施形態と同様に、暗号化ブロックを分割数Ｄにより分割し更にずらしてストレージに分散して供給することで、同様に、不当な第三者に対するセキュリティ向上を図るものである。すなわち、不当な第三者が一つのストレージから分割暗号化ブロックを入手しても、一つのストレージの分割暗号化ブロックだけでは、本来の複数の暗号化ブロックは再現することができないため、その後の暗号化ブロックの復号を行うことができない。これにより、第三者の暗号破りに対する高いセキュリティを示すものとなっている。

【００３１】

又、更に、任意の並べ替え方法により暗号化ブロックＮ１２を並べ替えているため、並

べ替え方法を知らない不当な第三者が、一つ、又は、複数のストレージからこの暗号化ブロックＮ１３の一部を取得したとしても、並べ替えた暗号化ブロックＮ１３を元に戻すことができない。又、暗号データの並びによらず、個別のブロック毎に暗号破りを試みようとしても、暗号化ブロックが分割されているため、個別のブロックの暗号破りも困難となり、不当な第三者に対するセキュリティを有するものとなっている。

【００３２】

この例では、並び替えの方法は先頭のストレージから順に振り分ける方法を取っているが、これは異なる方式でも構わないし、並びを記録した変換表を持つなど復元時に並びを元に戻す方法があれば、よりランダムな方法でも構わず、本発明に係る実施形態では、この方法について特に制限はしない。

【００３３】

又、ここで用いる暗号化方法は共通暗号鍵Ｋ１を用いたＣＢＣ暗号に分類されるものが望ましいが、１ブロックのサイズや鍵のビット数は任意のものでかまわない。又、ここではブロック暗号であるＣＢＣ暗号としたが、暗号文の一部を復号するために、他の部分の暗号文又は復号文を必要とし、そのつながりが暗号文の全体に及ぶような連鎖的な暗号であれば、必ずしもＣＢＣ暗号に制限する必要はなく、同様な効果が期待できる。

【００３４】

しかしながら、ＣＢＣ暗号のように他のブロックのデータを利用する暗号化方法でなく、一つのブロックだけで完結するブロック暗号であっても、暗号化ブロックが分割され分散されて格納されるので、第三者の暗号破りに対する高いセキュリティを持たせることが可能となる。

【００３５】

又、更に、所定のデータ単位で暗号化され、復号の際に、このデータ単位で復号されることを要求する暗号処理であれば、必ずしもブロック暗号という称号を必要とするものではなく、ＣＢＣ暗号を用いた場合と同等の作用効果を示すものである。

【００３６】

又、上記した暗号化ブロックの分割処理と、暗号化ブロックの並べ替え処理は、必ずしも分割処理が並べ替え処理に先行する必要はなく、並べ替え処理が分割処理に先行するものであっても、同等の作用効果を有するものである。又、更に、後述する復元処理の際においても、結合処理と並べ替え処理との順序は、どちらを先にすることも可能である。

【００３７】

（データ格納方法：第４実施形態：図６）

次に、このデータ格納方法の第４実施形態として、図６を用いて、Ｋ＝４、Ｌ＝５、Ｄ＝２、Ｍ＝１０、Ｎ＝８の場合のネットワークストレージへの保存法を示す。第４実施形態では、５台のネットワークストレージＧ１乃至Ｇ５に分割暗号化ブロックＮ４を４重に多重化してストレージに保存している。このように、分割暗号化ブロックＮ４が、高い多重化数で多重化して分散されていれば、図７に示すように、５台中３台のストレージＧ２乃至Ｇ４までもが破損しても、分割暗号化ブロックＮ４を復元することができ、これにより、平文データＰを復号することが可能となる。

【００３８】

（データ格納方法の詳細な説明：図８）

次に、このデータ格納方法につき、復元情報１１と復元予備情報１７とを用いた図８に示す詳細な実施形態を、図１２及び図１３のフローチャートを用いて説明する。

【００３９】

初めに、図１２のフローチャートにおいて、このデータ格納方法のパラメータの決定方法について説明する。一例として、各パラメータのうち、特に、多重化数Ｋ、ストレージ台数Ｌ、暗号化ブロック分割数Ｄは、ユーザが任意に与えることができることが好適であるが、これに限るものではない。

【００４０】

すなわち、図１１のデータ処理装置１００において、制御部１１５に内蔵されたプログ

ラム等の働きに応じて、図示しない操作部からのユーザの指示に応じて、多重化の数Ｋ（ただし、Ｋ≧２）を設定し（Ｓ１１）、次に、ストレージの台数Ｌ（ただし、Ｌ≧Ｋ＋１）を、ユーザの指示に応じて設定し（Ｓ１２）、更に、暗号化ブロックの分割数Ｄをユーザの指示に応じて設定する（Ｓ１３）。この時、これらのパラメータについて、ユーザはどんな数でも選ぶことができるわけではなく、上記した不等式が示すように多少の制約をもつものである。更に、これらのパラメータＫ，Ｌ，Ｄに応じたブロック分散数Ｍを、制御部１１５等の働きにより、例えば、（Ｍ≧Ｋ＋１、Ｍ＝Ｄ×ａ（ａは自然数））という制約の中で自動設定する（Ｓ１４）。又は、自動設定が困難な場合、又はユーザの希望によりユーザが直接入力することで、データ分散数Ｍを設定する（Ｓ１４）。そして、この場合、（（ＫＭ）／Ｌ≦Ｍ－１）となるストレージ１台あたりの暗号化ブロック数Ｎが成立すれば（Ｓ１５）、このときのＮを、１台当たりの暗号化ブロック数として設定して終了する（Ｓ１６）。しかし、ここで条件を満たすＮがなければ、再び、ブロック分散数Ｍを設定するステップＳ１４に戻り、適切なＭを設定するものである。

【００４１】

このようにして、設定された図８に示される実施形態のパラメータは、例えば、Ｋ＝２、Ｌ＝３、Ｄ＝２、Ｍ＝６、Ｎ＝４であり、以下に、この場合の、ネットワークストレージへの保存法を、図１３のフローチャートを用いて説明する。すなわち、図１１のデータ処理装置１００において、制御部１１５に内蔵されたプログラム等の働きに応じて、初めに、平分データＰが、第１暗号鍵Ｋ１を用いてブロック暗号の一例であるＣＢＣ暗号で暗号化される（Ｓ２０）。次に、この複数の暗号化ブロックに、それぞれＩＤを付与する（Ｓ２１）。そして、ユーザから設定された多重化の数Ｋ、ストレージの台数Ｌ、暗号化ブロックの分割数Ｄの値に応じて分散数Ｍを決定し、暗号化ブロックをこれらに応じて分割し、更に、任意の並べ替え情報１４に基づいて、暗号化ブロックＮ１３に並べ替える（Ｓ２２）。又、分割暗号化ブロックをＭ個に分類し、ＩＤとＭ個の分類の対応を並べ替え情報１４として保存する（Ｓ２３）。又、Ｌ台のストレージに対する各Ｍ個に分類した分割暗号化ブロックのＮ個ずつの割当を決定する（Ｓ２４）。

【００４２】

ここで、${}_{M}C_{N} \geqq L$であれば（Ｓ２５）、割り当てのパターンは、Ｌ種類となるまで（Ｓ２６）、重複するパターンを変更する（Ｓ２７）。更に、${}_{M}C_{N} \geqq L$でなければ（Ｓ２５）、割り当てのパターンは、${}_{M}C_{N}$種類となるまで（Ｓ２８）、重複するパターンを変更していく（Ｓ２９）。このようにして、各ストレージのネットワーク上のアドレスと割り当てを示すストレージアドレス表１５を完成し、復元情報１１の一部として保存する（Ｓ３０）。

【００４３】

そして、完成したストレージアドレス表１５に従って、分割された暗号化ブロックＮ１３を、Ｉ／Ｆ部１１６等を介して、例えば、インターネットを経由し、各ネットワークストレージＧ１乃至Ｇ３へと保存する（Ｓ３１）。

【００４４】

次に、データ復元に必要な情報である復元情報１１、一例として、第１暗号鍵１２と、分割情報１３と並べ替え情報１４とストレージアドレス表１５とを、第２暗号鍵Ｋ２により暗号化し、この暗号文１６を、各ネットワークストレージＧ１乃至Ｇ３へと分散して多重化して保存する（Ｓ３２）。更に、このときの第２暗号鍵Ｋ２と、ストレージアドレス表１５とを復元予備情報１７として、データ処理装置１００の記憶部１１１等であるサーバの記憶領域に保存する（Ｓ３３）。これにより、平文データＰは、高いセキュリティを保ちながら、更に、ストレージの故障に対しても再現性を確保しつつ、複数のストレージＧ１乃至Ｇ３上に保存することが可能となる。又、この復元情報１１と復元予備情報１７との使用は任意であり、必ずしもこのような方法で制御情報を格納させなければならないわけではなく、所望の領域に最小限の制御情報を格納するという方法も可能である。

【００４５】

（データ復元方法の詳細な説明：図９）

次に、この実施形態に係るデータ復元方法について、復元情報１１と復元予備情報１７とを用いた図９に示す詳細な実施形態を、図１４のフローチャートを用いて説明する。

【００４６】

すなわち、図１１のデータ処理装置１００において、制御部１１５に内蔵されたプログラム等の働きに応じて、図示しない操作部からのユーザの指示に応じて、データ復元が開始されると、例えば、記憶部１１１に格納されていた復元予備情報１７が読み出される。そして、この復元予備情報１７のストレージアドレス表１８を読み出して、各ストレージＧ１乃至Ｇ３から暗号化復元情報ｘｙｚを取得し、これを鍵Ｋ２で復号する（Ｓ４１）。

【００４７】

そして、復号された復元情報であるストレージアドレス表１５を用いて、各ストレージＧ１乃至Ｇ３から、分割された暗号化ブロックをそれぞれ読み出す（Ｓ４２）。Ｍ個に分散されている分割暗号化ブロックが全て読み出されると（Ｓ４３）、ストレージアドレス表１５に従って、元のＩＤ順に暗号化ブロックを並べ替える（Ｓ４４）。そして、分割暗号化ブロックを結合して暗号化ブロックに戻し、この暗号化ブロックを第１暗号鍵Ｋ１を用いて、ＣＢＣ暗号で平文データＰへと復号する（Ｓ４５）。これにより、複数のストレージＧ１乃至Ｇ３上に格納されていた平文データＰを完全に復元することができる。

【００４８】

一方、ステップＳ４３でのデータの読み出しが、全てのストレージアドレス１５に働き掛けても完了しない場合は（Ｓ４６）、平文データＰの復元が不可能である旨を表示するための表示信号を生成して出力し（Ｓ４７）、データ復元方法を完了するものである。

【００４９】

本発明の一実施形態に係るデータ格納方法及びデータ処理装置においては、特に、暗号化ブロックを分割処理して、複数のストレージに配分することにより、不当な第三者に対して高いセキュリティを示すものである。

【００５０】

又、更に、復元処理のための手がかりとして、鍵情報１２、分割情報１３、並べ替え情報１４、ストレージアドレス表１５等を含む復元情報１１、更に、この暗号化し複数ストレージに分散させた復元情報１１を元に戻すための復元予備情報１７等を用いて管理情報を分散させることで、ローカル環境での保存データを最小限にとどめ、管理を容易にし、ローカル環境でのディスク破損等によって復元不能になるリスクを低減することができる。なお、これら復元情報１１、復元予備情報１７等は、保存先は、上記した場合に限らず、任意の場所に置くことも好適となる。

【００５１】

又、上述したデータ格納方法及びデータ復元方法は、ネットワークストレージやローカル環境に特別なハードウェアを追加しなくても、ネットワークストレージを利用可能なローカル環境に、上述したデータ格納方法及びデータ復元方法を実行するソフトウェアを実装することで容易に実現が可能となる。

【００５２】

以上、本発明の一実施形態に係るデータ格納方法及びデータ復元方法によれば、平文データからＣＢＣ暗号等のブロック暗号により生成した暗号化ブロックを分割し、更に複数のストレージに分散して保存する。これにより、たとえ１つのストレージから分割暗号化ブロックを盗まれることがあったとしても、同時にそれを補完する分割暗号化ブロックが盗まれない限り、不当な第三者が暗号化ブロックを入手することができず、従って、暗号化ブロックを復号することができないので、平文データを復元することは不可能であるため、高いセキュリティを保持することができる。

【００５３】

以上記載した様々な実施形態により、当業者は本発明を実現することができるが、更にこれらの実施形態の様々な変形例を思いつくことが当業者によって容易であり、発明的な能力をもたなくとも様々な実施形態へと適用することが可能である。従って、本発明は、開示された原理と新規な特徴に矛盾しない広範な範囲に及ぶものであり、上述した実施形

態に限定されるものではない。

【図面の簡単な説明】

【００５４】

【図１】本発明の一実施形態に係るデータ格納方法の一例を示す説明図。

【図２】本発明の一実施形態に係るデータ格納方法の他の一例を示す説明図。

【図３】本発明の一実施形態に係るデータ格納方法の他の一例を示す説明図。

【図４】本発明の一実施形態に係るデータ格納方法の他の一例を示す説明図。

【図５】本発明の一実施形態に係るデータ格納方法において、ストレージを破損した際の復活処理を示す説明図。

【図６】本発明の一実施形態に係るデータ格納方法において、５台のストレージに４重化して保存する場合を示す説明図。

【図７】本発明の一実施形態に係るデータ格納方法において、５台のストレージに４重化して保存した際のストレージ破損に対する復元処理を示す説明図。

【図８】本発明の一実施形態に係るデータ格納方法を、復元情報と共に示す説明図。

【図９】本発明の一実施形態に係るデータ格納方法の復元方法の一例を示す説明図。

【図１０】本発明の一実施形態に係る３分割を行うデータ格納方法を示す説明図。

【図１１】本発明の一実施形態に係るデータ格納方法を行う情報処理装置の構成の一例を示すブロック図。

【図１２】本発明の一実施形態に係るデータ格納方法の際の、ストレージ１台当たりの分割ブロック数を決定するフローチャート。

【図１３】本発明の一実施形態に係るデータ格納方法の一例を示すフローチャート。

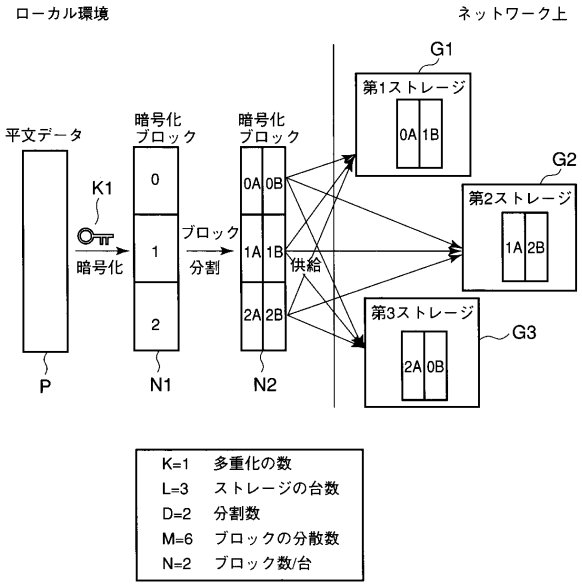
【図１４】本発明の一実施形態に係るデータ格納方法に対する復元方法の一例を示すフローチャート。

【符号の説明】

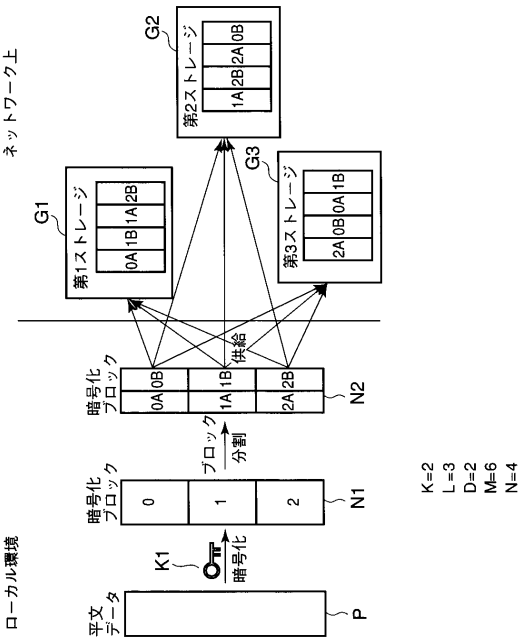
【００５５】

Ｐ…平分データ、Ｎ１…暗号化ブロック、Ｎ２…暗号化ブロック、Ｇ１～Ｇ３…ストレージ。

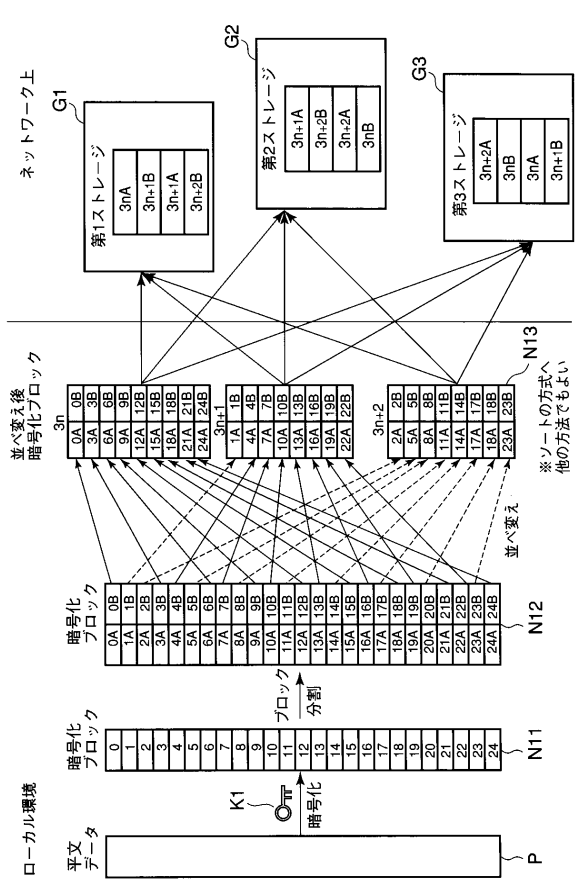
【図１】


ローカル環境
ネットワーク上
平文データ
暗号化ブロック
暗号化ブロック
K1
暗号化
ブロック分割
供給
第1ストレージ
第2ストレージ
第3ストレージ
G1
G2
G3
P
N1
N2
K=1 多重化の数
L=3 ストレージの台数
D=2 分割数
M=6 ブロックの分散数
N=2 ブロック数/台

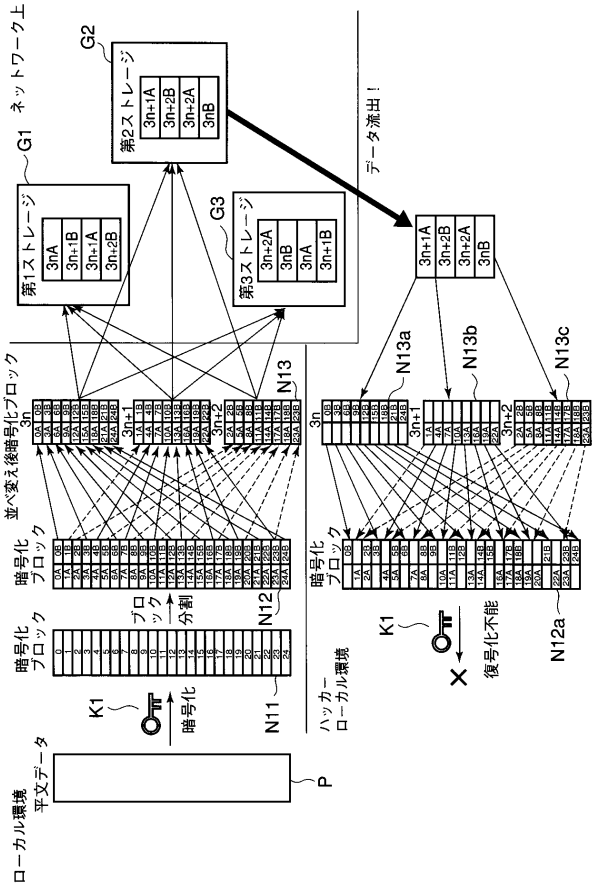
【図２】


ネットワーク上
ローカル環境
第1ストレージ
第2ストレージ
第3ストレージ
G1
G2
G3
暗号化ブロック
ブロック分割
供給
K1
暗号化
平文データ
P
N1
N2
K=2
L=3
D=2
M=6
N=4

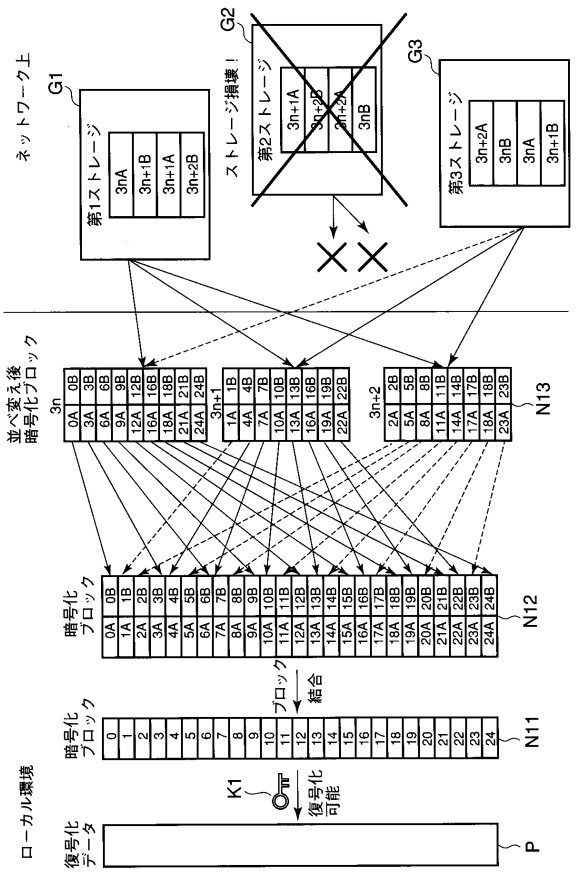
【図３】


ネットワーク上
ローカル環境
第1ストレージ
第2ストレージ
第3ストレージ
G1
G2
G3
並べ変え後暗号化ブロック
暗号化ブロック
ブロック分割
並べ変え
※ソートの方式へ他の方法でもよい
K1
暗号化
平文データ
P
N11
N12
N13

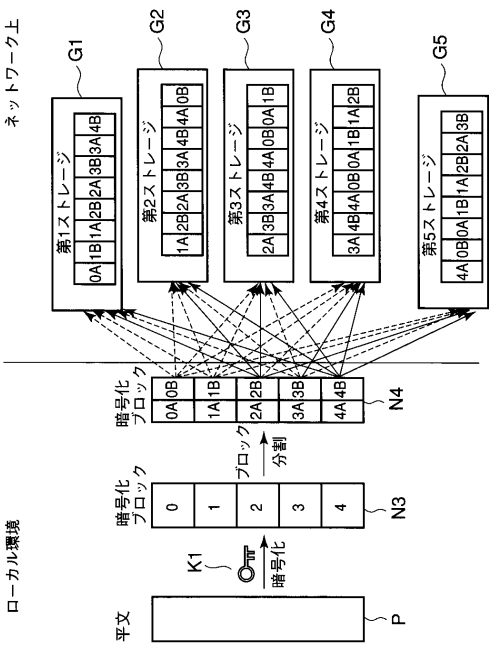
【図４】


ネットワーク上
ローカル環境
ハッカーローカル環境
第1ストレージ
第2ストレージ
第3ストレージ
G1
G2
G3
データ流出！
並べ変え後暗号化ブロック
暗号化ブロック
ブロック分割
K1
暗号化
復号化不能
平文データ
P
N11
N12
N12a
N13
N13a
N13b
N13c

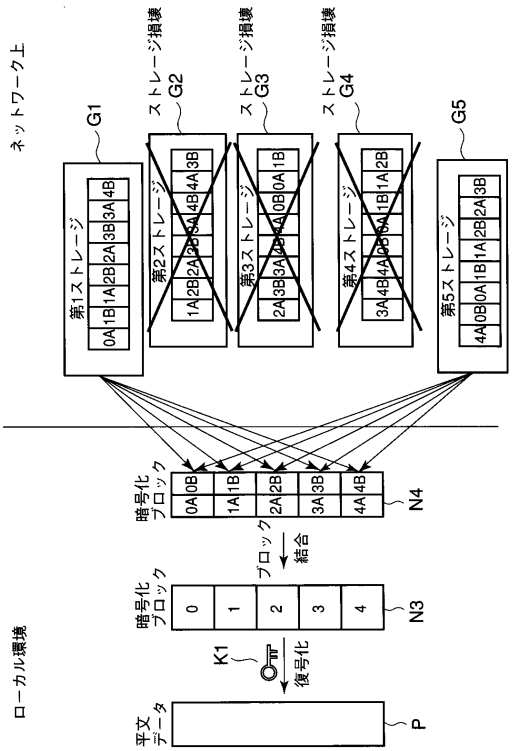
【図５】


ネットワーク上
G1
第1ストレージ
3nA
3n+1B
3n+1A
3n+2B
G2
ストレージ損壊！
第2ストレージ
3n+1A
3n+2B
3n+2A
3nB
G3
第3ストレージ
3n+2A
3nB
3nA
3n+1B
並べ変え後
暗号化ブロック
3n
3n+1
3n+2
N13
暗号化
ブロック
N12
ブロック
結合
暗号化
ブロック
N11
K1
復号化
可能
ローカル環境
復号化
データ
P

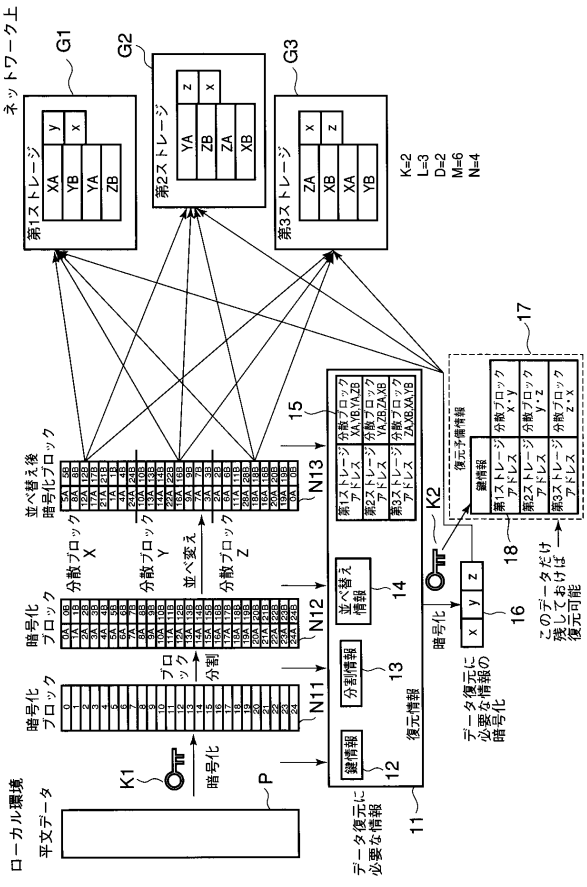
【図６】


ネットワーク上
G1
第1ストレージ
G2
第2ストレージ
G3
第3ストレージ
G4
第4ストレージ
G5
第5ストレージ
暗号化
ブロック
N4
ブロック
分割
暗号化
ブロック
N3
K1
暗号化
平文
P
ローカル環境

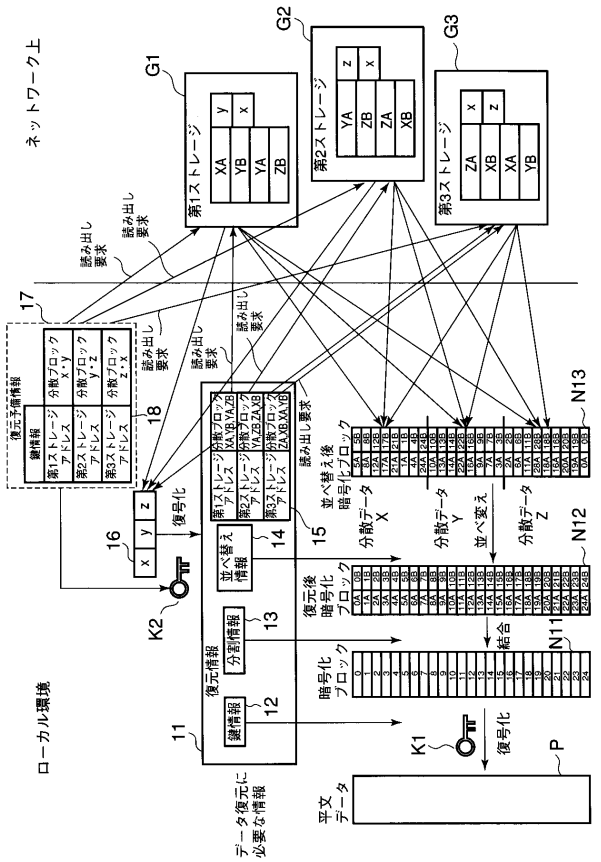
【図７】


ネットワーク上
G1
第1ストレージ
ストレージ損壊
G2
第2ストレージ
G3
第3ストレージ
G4
第4ストレージ
G5
第5ストレージ
暗号化
ブロック
N4
ブロック
結合
暗号化
ブロック
N3
K1
復号化
平文
データ
P
ローカル環境

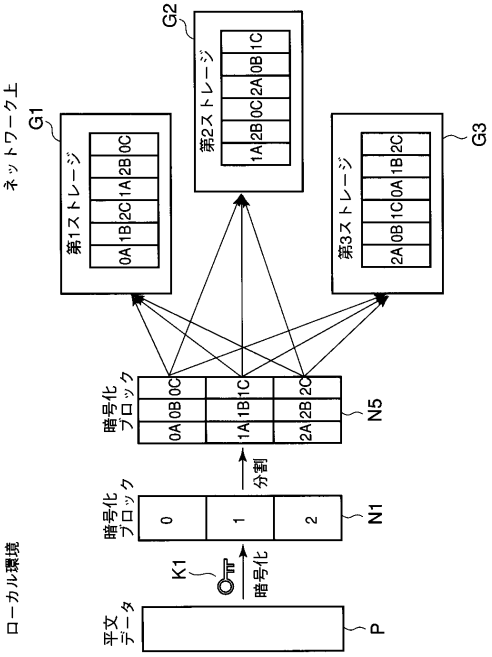
【図８】


ネットワーク上
G1
第1ストレージ
G2
第2ストレージ
G3
第3ストレージ
K=2
L=3
D=2
M=6
N=4
並べ替え後
暗号化ブロック
分散ブロック
X
分散ブロック
Y
並べ変え
分散ブロック
Z
N13
15
暗号化
ブロック
N12
並べ替え
情報
14
K2
暗号化
ブロック
N11
ブロック
分割
分割情報
13
鍵情報
12
復元情報
11
暗号化
K1
平文データ
P
ローカル環境
データ復元に
必要な情報
データ復元に
必要な情報の
暗号化
16
x
y
z
18
このデータだけ
残しておけば
復元可能
17
復元子情報
鍵情報
第1ストレージ
アドレス
第2ストレージ
アドレス
第3ストレージ
アドレス
分散ブロック
x・y
分散ブロック
y・z
分散ブロック
z・x

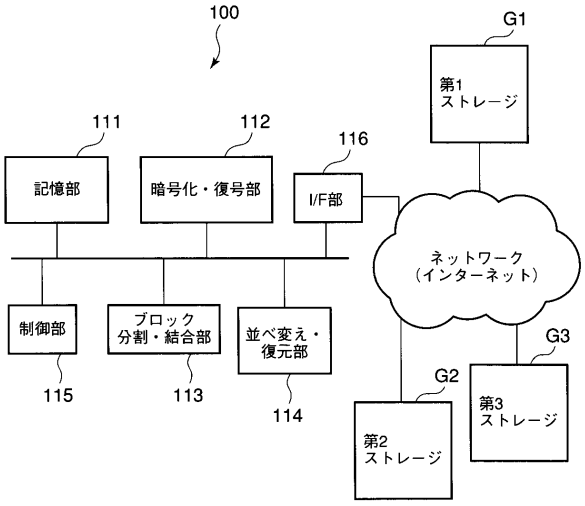
【図９】



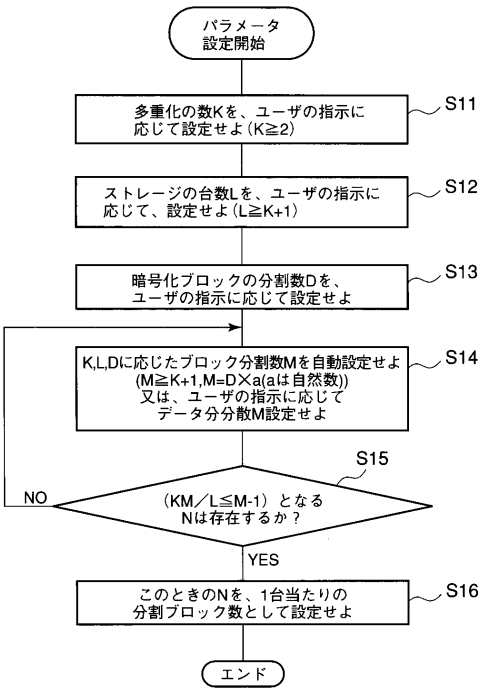
【図１０】



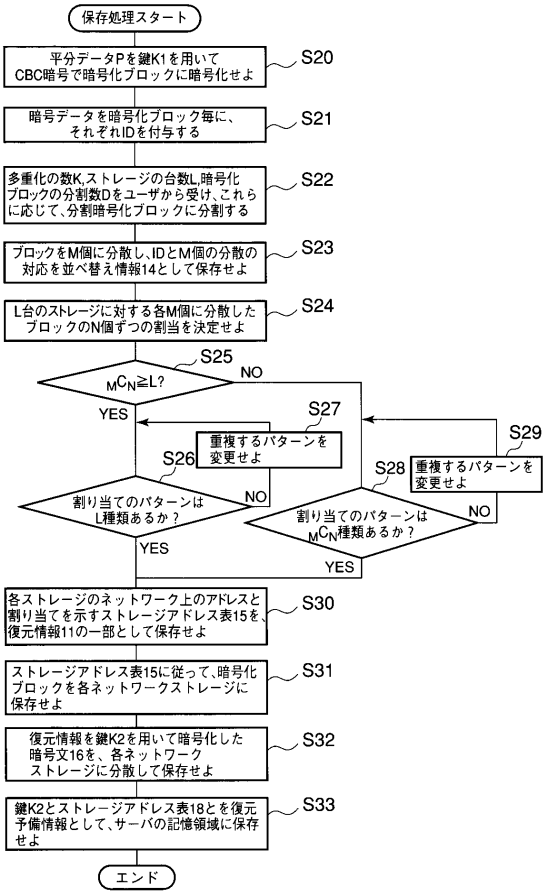
【図１１】



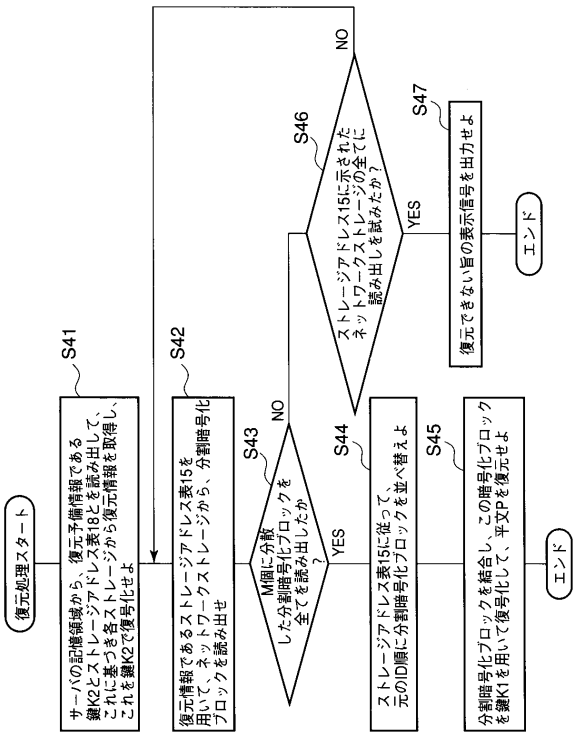
【図１２】



【図１３】


保存処理スタート
平分データPを鍵K1を用いて CBC暗号で暗号化ブロックに暗号化せよ
S20
暗号データを暗号化ブロック毎に、 それぞれIDを付与する
S21
多重化の数K,ストレージの台数L,暗号化 ブロックの分割数Dをユーザから受け、これら に応じて、分割暗号化ブロックに分割する
S22
ブロックをM個に分散し、IDとM個の分散の 対応を並べ替え情報14として保存せよ
S23
L台のストレージに対する各M個に分散した ブロックのN個ずつの割当を決定せよ
S24
S25
NO
YES
S27
重複するパターンを 変更せよ
S29
重複するパターンを 変更せよ
S26
割り当てのパターンは L種類あるか？
NO
S28
割り当てのパターンは 種類あるか？
NO
YES
YES
各ストレージのネットワーク上のアドレスと 割り当てを示すストレージアドレス表15を、 復元情報11の一部として保存せよ
S30
ストレージアドレス表15に従って、暗号化 ブロックを各ネットワークストレージに 保存せよ
S31
復元情報を鍵K2を用いて暗号化した 暗号文16を、各ネットワーク ストレージに分散して保存せよ
S32
鍵K2とストレージアドレス表18とを復元 予備情報として、サーバの記憶領域に保存 せよ
S33
エンド

【図１４】


復元処理スタート
S41
サーバの記憶領域から、復元予備情報である 鍵K2とストレージアドレス表18とを読み出して、 これに基づき各ストレージから復元情報を取得し、 これを鍵K2で復号化せよ
S42
復元情報であるストレージアドレス表15を 用いて、ネットワークストレージから、分割暗号化 ブロックを読み出せ
S43
NO
M個に分散 した分割暗号化ブロックを 全てを読み出したか ？
YES
S44
ストレージアドレス表15に従って、 元のID順に分割暗号化ブロックを並べ替えよ
S45
分割暗号化ブロックを結合し、この暗号化ブロック を鍵K1を用いて復号化して、平文Pを復元せよ
エンド
S46
NO
ストレージアドレス15に示された ネットワークストレージの全てに 読み出しを試みたか？
YES
S47
復元できない旨の表示信号を出力せよ
エンド

フロントページの続き

(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 八島 大亮
東京都青梅市末広町２丁目９番地 株式会社東芝青梅事業所内

Ｆターム(参考) 5B017 AA03 BA07 BA10 CA16