(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2005-293592
(P2005-293592A)
(43)公開日　平成17年10月20日(2005.10.20)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 12/14	G06F 12/14	510F	5B017
G06F 12/00	G06F 12/00	501A	5B082
	G06F 12/00	545A	

審査請求 有　請求項の数 24　ＯＬ　外国語出願　（全 20 頁）

(21)出願番号　特願2005-101729 (P2005-101729)
(22)出願日　平成17年3月31日 (2005.3.31)
(31)優先権主張番号　0407484.5
(32)優先日　平成16年4月1日 (2004.4.1)
(33)優先権主張国　英国 (GB)

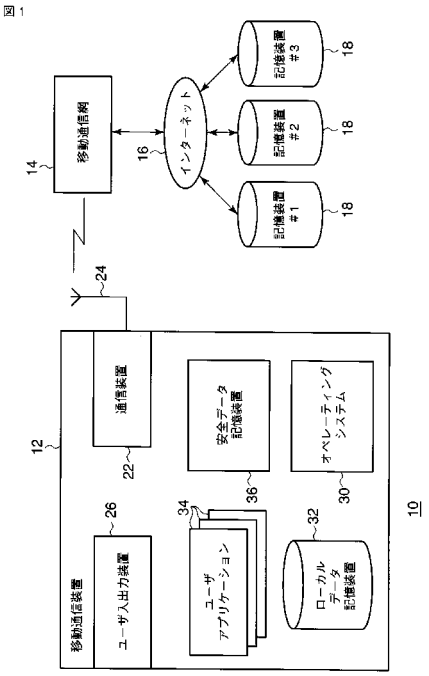
(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100075672
弁理士　峰　隆司
(74)代理人　100109830
弁理士　福原　淑弘

最終頁に続く

(54)【発明の名称】ネットワークでのデータの安全な記憶

(57)【要約】
【課題】ネットワーク内の汎用コンピュータで実行される、データのアイテムを記憶する方法及びネットワークで、ネットワークの遠隔記憶場所でのデータのアイテムの記憶を管理・達成するために動作可能であるコンピュータ装置。
【解決手段】ネットワークで使用可能な記憶手段を特定し、特定使用可能記憶手段のデータ記憶容量の利用可能性に関する情報を収集し、分割ポリシーに従いデータアイテムを分割し、特定使用可能記憶手段の間で分散ポリシーに従い結果データのフラグメントを分散する。ネットワークのネットワークでアクセス可能記憶手段を特定する記憶空間特定手段と、使用可能記憶手段のデータ記憶容量の利用可能性に関する情報を収集する記憶利用可能性情報収集手段と、分割ポリシーに従ってデータアイテムを分割する分割手段と、特定使用可能記憶手段の間で分散ポリシーに従って結果データのフラグメントを分散する分散手段とを備える。
【選択図】図１

図1



【特許請求の範囲】
【請求項１】
ネットワーク内の汎用コンピュータで実行される、データのアイテムを記憶する方法であって、
前記ネットワークにおいて使用可能記憶手段を特定すること、
前記使用可能記憶手段のデータ記憶容量の利用可能性に関する情報を収集すること、
分割ポリシーに従って前記データのアイテムを分割すること、
分散ポリシーに従って結果として生じるデータのフラグメントを、前記特定された使用可能記憶手段の間で分散すること、
を含む、方法。
【請求項２】
前記データを分割する前記ステップに先行して、前記データの分割ポリシーを決定することを含む、請求項１に記載の方法。
【請求項３】
前記データの分割ポリシーを決定する前記ステップは、被分割データのタイプを決定すること、及び前記データのタイプ及び前記データの所定のフラグメントの理解可能性のレベルに基づいて、前記データを分割する前記ステップが前記データを分割させるべきフラグメントの性質及びサイズを決定することを含む、請求項２に記載の方法。
【請求項４】
前記データを分割するステップは、前記データのセグメントを識別すること、前記セグメントの非近接の多数を前記データの一セグメントとして識別することを含み、データの結果フラグメントは前記データの交互配置部分フラグメントにより構成される、請求項１から３のいずれか１項に記載の方法。
【請求項５】
前記データを分散する前記ステップに先行して、前記データの分散ポリシーを決定することを含む、請求項１から４のいずれか１項に記載の方法。
【請求項６】
前記データの分散ポリシーを決定するステップは、前記データを分割する前記ステップで生成されるデータのフラグメントの数、及び使用可能記憶手段の数に基づいて実行される、請求項５に記載の方法。
【請求項７】
前記データの分散ポリシーを決定する前記ステップは、前記ステップが実行されるデータのタイプに基づいて実行される、請求項５または６に記載の方法。
【請求項８】
前記使用可能記憶手段のデータ記憶容量の前記利用可能性に関する情報を収集する前記ステップは、前記特定された記憶手段に関する情報を収集することを含み、この情報に基づいて分散ポリシーが決定できる、請求項５から７のいずれか１項に記載の方法。
【請求項９】
前記情報は、前記記憶手段に記憶される情報の情報検索速度、物理的な場所及び／または前記汎用コンピュータからの物理的な距離、前記記憶手段の予定休止時間、及び前記記憶手段の所有者により課される前記記憶手段の料金情報の全てまたはどれかを含む、請求項８に記載の方法。
【請求項１０】
ネットワークにおいて動作可能であり、前記ネットワークの遠隔記憶場所においてデータのアイテムの記憶を管理及び達成するためのコンピュータ装置であって、前記ネットワーク内のネットワークでアクセス可能な記憶手段を識別するための記憶空間識別手段と、前記使用可能記憶手段内のデータ記憶容量の利用可能性に関する情報を収集するための記憶可能性情報収集手段と、分割ポリシーに従って前記データのアイテムを分割するための分割手段と、分散ポリシーに従って、前記特定された使用可能な記憶手段の間で結果として生じるデータのフラグメントを分散するための分散手段とを備える、コンピュータ装置

。
【請求項１１】
前記データの分割ポリシーを決定するための分割ポリシー決定手段を備える、請求項１０に記載のコンピュータ装置。
【請求項１２】
前記分割ポリシー決定手段は、被分割データのタイプを決定するためのデータタイプ決定手段を含み、前記データタイプ決定手段は、データのタイプ及び前記データの所定フラグメントの理解容易性のレベルに基づいて、前記分割手段により前記データが分割されたフラグメントの性質及びサイズを決定するために動作可能である、請求項１１に記載のコンピュータ装置。
【請求項１３】
前記分割手段は、前記データのセグメントを識別するため、及びフラグメント前記セグメントの非近接の複数を前記データのフラグメントとして割り当てるために動作でき、前記データの結果のフラグメントが前記データのインタリーブ部分により構成される、請求項１０から１２のいずれか１項に記載のコンピュータ装置。
【請求項１４】
前記データの分散ポリシーを決定する分散ポリシー決定手段をさらに備える、請求項１０から１３のいずれか１項に記載のコンピュータ装置。
【請求項１５】
前記分散ポリシー決定手段は、前記データを分割する前記ステップで生成されるデータのフラグメントの数、及び使用中の前記ネットワークでアクセス可能な使用可能な記憶手段の数に基づいて分散ポリシーを決定するために動作可能である、請求項１４に記載のコンピュータ装置。
【請求項１６】
前記分散ポリシー決定手段は、前記ステップが実行される前記データのタイプに基づいて分散ポリシーを決定するために動作可能である、請求項１４または１５に記載のコンピュータ装置。
【請求項１７】
前記記憶可用性情報収集手段は、使用中の前記ネットワーク内の前記特定された記憶手段に関する情報を収集するために動作可能であり、次に、これに基づいて分散ポリシーを決定できる、請求項１４から１６のいずれか１項に記載のコンピュータ装置。
【請求項１８】
前記記憶可用性情報収集手段により収集される前記情報は、前記記憶手段に記憶される情報の情報検索速度、物理的な場所及び／または前記汎用コンピュータからの物理的な距離、前記記憶手段のための予定休止時間、及び前記記憶手段の所有者により課される前記記憶手段の料金情報の全てまたはどれかを含む、請求項１７に記載のコンピュータ装置。
【請求項１９】
それぞれが前記ネットワーク内の少なくとも１つの他の装置と通信しているコンピュータ装置のネットワークであって、前記コンピュータ装置の少なくとも１つは請求項１から９のいずれか１項に記載の前記方法を実行するように構成され、前記コンピュータ装置の少なくとも１つの他の装置は別のコンピュータ装置からデータを受信し、最終的な検索のために前記データを記憶することができる記憶手段として構成される、コンピュータ装置のネットワーク。
【請求項２０】
それぞれが前記ネットワーク内の少なくとも１つの他の装置と通信しているコンピュータ装置のネットワークであって、前記コンピュータ装置の少なくとも１つは請求項１０から１８のいずれか１項に記載のコンピュータ装置として構成され、前記コンピュータ装置の少なくとも１つの他の装置が別のコンピュータ装置からデータを受信し、最終的な検索のために前記データを記憶することができる記憶手段として構成される、コンピュータ装置のネットワーク。

【請求項２１】
コンピュータにロードされると、そのコンピュータに請求項１から９のいずれか１項に記載の方法を実行させるコンピュータ実行可能命令を定める情報を運ぶ、コンピュータ読み取り可能プログラムキャリヤ媒体。
【請求項２２】
コンピュータにロードされると、そのコンピュータを請求項１０から１８のいずれか１項に記載の装置として構成させるコンピュータ実行可能命令を定める情報を運ぶ、コンピュータ読み取り可能プログラムキャリヤ媒体。
【請求項２３】
コンピュータにロードされると、そのコンピュータに請求項１から９のいずれか１項に記載の方法を実行させるコンピュータ実行可能命令を定める情報を伝搬する、コンピュータ受信可能情報キャリヤ信号。
【請求項２４】
コンピュータにロードされると、そのコンピュータに、本発明の第１の態様に従って前記方法を実行させるか、あるいは請求項１０から１８のいずれか１項に記載の装置として構成させるかのどちらかであるコンピュータ実行可能命令を定める情報を伝搬する、コンピュータ受信可能情報キャリヤ信号。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、単一の場所でのデータの記憶に関するセキュリティ問題を回避する、安全な方法でのデータの記憶に関する。
【背景技術】
【０００２】
コンピュータをベースにした技術の多くの応用例では、後で使用したり、ユーザへの出力用に検索するためにデータを記憶することが必要である。コンピュータネットワークが個人的な性質であるか、あるいは別の理由から機密であるデータを用いることが増え、その結果、データはそれがアクセス権のないユーザによって検索またはアクセスされるのを防ぐために、あるレベルのセキュリティの適用を受けることを必要とする。
【０００３】
多くのケースでは、情報への未許可のアクセスは、データのブロックの一部だけに対するアクセスを獲得するという点で有益となる可能性がある。例えば、銀行口座と承認パスワードの関係性を設定するルックアップテーブルでは、このような情報の未許可の検索には、表の全内容の検索をすることは必要としない。表のただ１つのエントリが関係する口座の名義人に重大な結果を生じさせることがある。
【０００４】
したがって、データに適用されるセキュリティのレベルが、情報の理解可能な検索を防止するに十分であることを確実にすることは重要である。
【０００５】
実施されると、データへの未許可のアクセスを防止するために使用できる多様なセキュリティ機構が提案されてきた。これらの機構は、通常、データにアクセスする人または装置の証明を確立するための認証、及びデータを理解不能とする暗号化を必要とする。しかしながら、セキュリティ機構が調えられた状態でデータが単一の場所に記憶される場合に、セキュリティ機構が権限なしにデータへのアクセスを求める個人または装置によって破られた場合には、その場所に記憶されているデータ全体にアクセス可能となることがある。
【０００６】
コンピュータシステム内に記憶されるデータのセキュリティの耐性を増すためには、ネットワークのサーバの間でデータを分散することは既知である。この技法の１つの応用例が、インターネット上のサーバの間でコンテンツを分散することによりセキュリティを提

供するプブリウスシステム(Publius system)である。このケースでは、セキュリティは、インターネットを介してデータを検索する機会を高めながら、データの未許可の編集を妨げることを意図としている。これは、インターネットを介しての検索のためにデータを受け入れるサーバをなんらかの方法で動作不能にすることにより、アクセス権のない人がデータへのアクセスを混乱させるのを防止する。

【０００７】

一方ではアクセス権のない人または悪意のある人がサーバ上で動作するデータに変更を加えるのをより困難にすることによって、他方では情報へのアクセスを混乱させる行為をより複雑なプロセスにすることによって、アクセス権のない第三者が情報へのアクセスを混乱させる能力は大幅に抑えられる。

【０００８】

プブリウスシステムでは、発行元コンピュータ装置がコンテンツを暗号化し、それをインターネット上で使用可能なウェブサーバのサブセットの上で立ち上げさせる。該暗号化は、ｎ個のシェアに分割される鍵を使用して実行され、その結果それらの内の任意のｋ個はオリジナルの鍵を再生できるが、ｋ－１個のシェアの検索は該鍵を確定するには不十分である。各サーバは暗号化されたコンテンツ及びシェアの１つを受信する。

【０００９】

この時点では、単に個々のサーバに記憶されているコンテンツを見ることによって、サーバ上に記憶されているデータの性質を決定することは不可能である。データは完全に暗号化され、ランダムに出現する。理解可能な方法でコンテンツをブラウズするためには、インターネットにアクセスするブラウジング装置が、サーバの１つから暗号化されたプブリウスコンテンツ、及びシェアの内のｋ個を検索しなければならない。

【００１０】

このようにしてコンテンツを公開するプロセスにより、暗号化されたデータを回復するために使用される特定のユニフォームリソースロケータ（ＵＲＬ）、及び鍵の構築を可能にする十分なシェアが生成される。公開されたコンテンツは、コンテンツに、又はＵＲＬへの任意の修正によりブラウジング装置が情報を見つけることを不可能にすることになり、あるいは検証失敗となるようにＵＲＬに暗号化により結び付けられている。

【００１１】

この公開機構に加えて、プブリウスシステムは、公開者が自分のプブリウスコンテンツを更新または削除できるようにする一方で、アクセス権のない関係者が同じことを行うのを防止する。プブリウス技術での全体的な意図とは、インターネット上で公開される文書が複数の場所に記憶され、その結果それらの場所の内の１つが攻撃を受けた場合にも、該公開されたコンテンツに他の場所からアクセスできることを確実にすることである。

【００１２】

このシステムは、データの固有のセキュリティへの機能強化を与えることを目的としていないし、それを行うことをしない。それは、第三者がインターネット上で公開されるデータのアクセス許容度を危うくすることを防止することに関連している。基本的には、この処置に関する意図とは、機密データへのアクセスを制限することよりは、むしろデータに対するアクセスを強化し、維持することである。これは、本来、データへのアクセスが厳しく管理されていることを確実にすることに関する本発明とは別の技術的な問題である。

【発明の開示】

【発明が解決しようとする課題】

【００１３】

ネットワーク内でのデータ記憶を改善するため通信網で使用するセキュリティシステムを提供することが本発明の目的である。

【００１４】

装置のユーザがネットワーク上でのデータ記憶の分散性質に実質的に気付かないように、問題のデータ記憶ネットワークにアクセスできる装置を提供することが本発明の他の目

的である。
【００１５】
データへのアクセスがセキュリティ体制を前提とするように、且つ単一の記憶場所の障害が、記憶されているデータのアイテムの理解可能性の障害にならないように、ネットワーク内でデータを記憶する方法を提供することも本発明のさらに他の目的である。
【課題を解決するための手段】
【００１６】
したがって、本発明の第１の局面によると、ネットワークの汎用コンピュータで実行される、データのアイテムを記憶する方法は、ネットワークで使用可能な記憶手段を特定するステップと、使用可能な記憶手段でデータ記憶容量の利用可能性に関して情報を収集するステップと、分割ポリシーに従って前記データのアイテムを分割するステップと、分散ポリシーに従って前記特定された使用可能な記憶手段の間で結果として生じたデータのフラグメント（断片）を分散するステップとを備える。
【００１７】
前記方法は、データを分割する前記ステップに先行して、データの分割ポリシーを決定するステップを備えてよい。
【００１８】
データの分割ポリシーを決定するステップは、データのタイプ及びデータの指定されたフラグメントの理解可能性のレベルに基づいて、分割されるデータのタイプを決定することと、データを分割する前記ステップによりデータが分割されなければならないフラグメントの性質及びサイズを決定することとを含んでよい。
【００１９】
データを分割するステップは、結果として生じるデータのフラグメントがデータの交互配置された部分を含むように、データのセグメントを特定することと、データのフラグメントとして非近接の複数のセグメントを特定することを含んでもよい。
【００２０】
該方法は、データを分散する前記ステップに先行して、データの分散ポリシーを決定するステップを含んでもよい。
【００２１】
データの分散ポリシーを決定するステップは、データを分割する前記ステップで生成されるデータのフラグメントの数、及び使用可能な記憶手段の数に基づいて実行されてもよい。
【００２２】
データのための分散ポリシーを決定するステップは、ステップがその上で実行されるデータのタイプに基づいて実行されてもよい。そのようにして、データを分散する前記ステップでのデータフラグメントの記憶は、データのタイプ、したがって例えば、データに対する緊急の将来のアクセスが予想される範囲を考慮に入れるために制御できる。
【００２３】
使用可能な記憶手段のデータ記憶容量の利用可能性に関する情報を収集するステップは、特定された記憶手段に関する情報を収集することを含んでもよく、それに基づいて分散ポリシーを決定できる。前記情報は、記憶手段に記憶される情報の情報検索速度、物理的な場所及び／または汎用コンピュータからの物理的な距離、記憶手段の予定休止時間、及び記憶手段の所有者により課される記憶手段に対する料金情報の全てまたはどれかを含んでもよい。
【００２４】
本発明の第２の局面によると、ネットワークで動作可能であり、ネットワーク内の遠隔記憶場所でのデータのアイテムの記憶を管理及び達成するためのコンピュータ装置は、ネットワーク内のネットワークでアクセス可能な記憶手段を認識するための記憶空間認識手段と、使用可能記憶手段でのデータ記憶容量の仕様可能性に関する情報を収集するための記憶可能性情報収集手段と、分割ポリシーに従ってデータのアイテムを分割するための分

割手段と、分散ポリシーに従って特定された使用可能記憶手段の間で結果として生じるデータのフラグメントを分散するための分散手段とを具備する。

【００２５】

コンピュータ装置は、データの分割ポリシーを決定するための分割ポリシー決定手段を含んでもよい。

【００２６】

分割ポリシー決定手段は、分割されるデータのタイプを決定するためのデータタイプ決定手段を含んでもよく、データタイプ決定手段は、データのタイプ及びデータの所定フラグメントの理解容易性のレベルに基づいて、分割手段によりデータが分割されたフラグメントの性質及びサイズを決定するために動作可能である。

【００２７】

分割手段は、データのセグメントを識別するため、及び前記セグメントの非近接の複数を前記データのフラグメントとして割り当てるために動作可能であってもよく、それにより前記データの結果のフラグメントが前記データの交互配置部分により構成される。フラグメント装置は、データの分散ポリシーを決定するための分散ポリシー決定手段をさらに含んでもよい。

【００２８】

分散ポリシー決定手段は、データを分割する前記ステップで生成されるデータのフラグメントの数、及び使用中のネットワークでアクセス可能で使用可能な記憶手段の数に基づいて分散ポリシーを決定するために動作可能であってよい。

【００２９】

分散ポリシー決定手段は、該ステップが実行されるデータのタイプに基づいて分散ポリシーを決定するために動作可能であってもよい。そのようにして、分散手段によるデータフラグメントの記憶は、データのタイプ、したがって例えば、データへの緊急の将来のアクセスが予想される範囲を考慮に入れるために制御できる。

【００３０】

記憶可能性情報収集手段は、使用中の前記ネットワーク内で特定された記憶手段に関する情報を収集するように動作可能であってよく、分散ポリシーをそれに基づいて決定できる。前記情報は、記憶手段に記憶される情報に対する情報検索速度、物理的な場所及び／または前記汎用コンピュータからの物理的な距離、記憶手段の予定休止時間、及び記憶手段の所有者により課される記憶手段の料金情報の全てまたはどれかを含んでもよい。

【００３１】

本発明の第３の局面は、それぞれがネットワーク内の少なくとも１つの他の装置と通信しているコンピュータ装置のネットワークを提供し、コンピュータ装置の少なくとも１つは本発明の第２の態様に従ってコンピュータ装置として構成されるか、あるいは本発明の第１の局面の方法を実行するように構成され、コンピュータ装置の少なくとも１つの他の装置は別のコンピュータ装置からデータを受信し、最終的な検索のために前記データを記憶することができる記憶手段として構成される。

【００３２】

用途に特定となるように構成された、つまり本発明の第１の局面の方法を実行するように設計された独自の装置として、あるいは本発明の第２の局面の装置として構成された装置を提供できるが、本発明の第４の局面は、コンピュータにロードされると、そのコンピュータに本発明の第１の局面による方法を実行させ、あるいは本発明の第２の局面に従った装置として構成されるようになるコンピュータ実行可能命令を定める情報を運ぶコンピュータ読み取り可能プログラムキャリヤ媒体を提供する。

【００３３】

同様に、本発明の第５の局面は、コンピュータにロードされると、そのコンピュータに本発明の第１の局面に従った方法を実行させ、あるいは本発明の第２の局面に従った装置として構成されるようになるコンピュータ実行可能命令を定める情報を伝搬するコンピュータ受信可能情報キャリヤ信号を提供する。

【００３４】
本発明の他の局面及び利点は、添付図面を参照し、一例として、本発明の特定の実施形態の以下の説明から明らかになるであろう。
【発明を実施するための最良の形態】
【００３５】
図１に示されるように、移動通信システム１０は、無線接続によって移動通信網１４とデータ通信している移動通信装置１２を含む。実際問題として、この無線接続は、ＧＰＲＳまたは第三世代モバイルシステム（３Ｇ）などの従来の手段によって実現できる。
【００３６】
このようにして確立された無線データ通信は、移動通信装置１２が、遠隔で配置される記憶装置１８を含む、インターネット１６のデータリソースへのアクセスを獲得できるようにする。図１に描かれている概略図では、３台の記憶装置１８が描かれているが、インターネットが潜在的にさらに多くの記憶装置との通信を可能にすることが理解されるであろう。
【００３７】
移動通信装置１２の構造及び機能をここに説明する。この実施形態での構造及び機能はハードウェアとソフトウェア両方によって実現される。説明を容易にするために、図１に示されているような移動通信装置１２は概略で、つまりハードウェア機能性またはソフトウェア機能性の態様を区別せずに示す。
【００３８】
移動通信装置１２は、アンテナ２４によって他の装置との通信を確立する通信装置２２を含み、通信はＯＳＩモデルを使用するなどの確立された通信プロトコルに従う。使用中、データは移動通信装置１２の他の機能要素によって通信装置２２に渡すことができ、通信装置２２は従来の方法でデータの送信及び受信を処理できる。
【００３９】
実際面ではディスプレイ、キーボード及び／またはポインティングデバイス（マウス、ジョイスティックなど）及び音声出力のようなユーザ作動可能入力手段を含むことができるユーザ入出力装置２６は、ユーザに対する情報の提示用、及びデータ入力として解釈されるユーザ入力アクションを監視するためのユーザインタフェースの確立を可能にする。
【００４０】
オペレーティングシステム３０は、ローカルデータ記憶装置３２の管理などの移動通信装置１２の根本的な動作を実行するために移動通信装置１２で実行される。オペレーティングシステム３０は、ｅメール処理アプリケーション、ブラウザ及びマルチメディアアプリケーションを含んでよいユーザアプリケーション３４によって使用される機能性を提供する。
【００４１】
安全データ記憶装置３６は、ローカルデータ記憶装置３２と対照的に、データを安全に遠隔に、つまり記憶装置１８などの記憶場所内に記憶するための機能をオペレーティングシステム３０に提供するために、移動通信装置１２内で動作可能である。該安全データ記憶装置３６は、ユーザアプリケーション３４によってそれに送信されるようなデータを処理し、通信装置２２を介して記憶装置１８への伝送のためにデータを処理するために、オペレーティングシステム３０と連動して動作する。
【００４２】
安全データ記憶装置３６は、データに適用されるセキュリティのレベルを考慮して必要とされる範囲までデータを分割し、検索の容易さ及びデータの再アセンブリとセキュリティを天秤にかけるようにフラグメントを分散するために動作できる。分割戦略は、データの個々のフラグメントがデータの全体的な性質を明らかにしないことを確実にするように設計される。
【００４３】
例えば、理解可能な１つの情報を、単に該情報を２つのフラグメントに分割するだけで

理解不能とすることができる場合には、適切なセキュリティが該情報を２つのフラグメントに分割してから、該２つのフラグメントを別々の場所に記憶することにより可能になる可能性がある。テキスト記述がこのカテゴリに該当する―それぞれのファイルが元のテキストファイルの交互に並ぶ文字を受け入れる、２つの別個のファイルにデータを分割することにより、結果として生じるテキスト文字の文字列は一般的には理解できない。

【００４４】

これに対して、１個のデータが、そのそれぞれが悪意のある受取人にとって潜在的に貴重である複数の個々のデータのアイテムを有する場合には、データは、それぞれの個々のフラグメントが理解可能な１つの情報を生じさせないことを確実にするために、より高い程度まで分割する必要があるであろう。クレジットカードの詳細がこのカテゴリに該当する可能性がある。

【００４５】

分割しても多少理解可能性が残るデータのフラグメントが生じる場合でさえ、理解可能性は非常にわずかであり、悪意的に妨害されたフラグメントから意味を抽出するプロセスは、興味を引くには余りにも複雑で、且つ時間を要することになる。類推により、一般的に公開鍵暗号化は大部分の使用に高いレベルのセキュリティを提供すると考えられている。その動作は、公開鍵から秘密鍵を推定するためには、公開鍵がその素因数に分けられなければならないという事実に依存している。公開鍵は非常に多くの素因数だけを有する非常に大きな数であるため、これは計算上非常に困難であり、実際の時間尺度では通常不可能と考えられている。

【００４６】

しかしながら、公開鍵が少なくとも理論的には攻撃に対して弱いという事実は、公開鍵暗号化により暗号化された情報が許可なくしてアクセスできるという可能性を残す。この理論上の可能性は、セキュリティレベルが大部分の使用にとっては十分であり、最も極端なケースを除けば極めて精巧な攻撃も防ぐことになるため、許容できる障害としてユーザによって受け入れられている。

【００４７】

分割ポリシーが、（ユーザ入出力装置２６によって定義されるユーザインタフェースに対するユーザ入力アクションによる入力のような）ユーザによって所望されるセキュリティのレベル、及びデータフラグメントの記憶のために使用可能な図１に描かれている記憶装置１８の数によって影響を受けることがある。このようにして、データの全てを回復しなければならない場合には相当多くの数の攻撃が無事に行われなければならないので、データに適用されるセキュリティの全体的なレベルは、単一の場所にデータを記憶することに比較して強化される。

【００４８】

さらに、分散ポリシー及び分割ポリシーが攻撃者にも既知でない限り、データを再構築することは困難であろう。

【００４９】

安全データ記憶装置３６の構造及び機能性を、ここで図２を参照して説明する。安全データ記憶装置３６は、ユーザ入出力装置２６でユーザインタフェースの定義のためのデータを生成し、ユーザ入力アクションに対応してデータを受け入れるために動作可能であるユーザインタフェースを含む。このようにして、移動通信装置１２のユーザは、必要に応じて安全データ記憶装置３６の設定を管理し、微調整することができる。

【００５０】

安全データ記憶装置３６の管理装置４２は、分割装置４４及び分散装置４６の動作を監視・調整する。該分割装置４４は、安全な記憶のために安全データ記憶装置３６に提示されるデータを分割するために動作可能である。分割装置４４はデータを分析し、分割ポリシーを作成するために動作可能であり、後者がどのようにデータを分割する必要があるのかを決定する。以後、分割装置４４は該分割ポリシーに従ってデータを分割する。分割装置４４は、遠隔場所に安全に記憶されているデータの検索時に、分割されたデータを再組

み立てすることもできる。

【００５１】

分散装置４６は、システムに提示され、分割装置４４により分割されるデータを分散するために動作可能である。分散装置４６は、インターネット１６を介したアクセスに使用可能であり、データフラグメントの記憶を行うことができる記憶装置１８のリストを管理する。記憶装置１８に対する各エントリに対して、リストは、データのフラグメントにとって最も適切な記憶場所を決定するにあたり使用される、記憶装置１８の１つ以上の特徴も記録する。

【００５２】

使用可能な記憶装置１８ごとに記憶される特徴は、分散装置４６がその特定の記憶装置１８を使用する必要があるかどうかを決定する際に、記憶装置１８の利用可能性はいくつかの要因の１つにすぎないという事実を反映している。記憶装置の信頼性も重要である。つまり、記憶装置１８は記憶の時点で使用可能である可能性があるが、該記憶装置の将来の利用可能性も考慮に入れなければならないことを確実にする。データの恒久的なアクセスが必要とされているときに、特定の時間帯でのデータ検索可能データだけに使用可能であることは、使用される記憶装置にとっては望ましくないであろう。さらに、分散ポリシーはより信頼性が低い記憶装置を使用するが、より信頼性が低い記憶装置に記憶されるデータフラグメントのコピーを別の記憶装置でも記憶することにより冗長性を生じさせるため、ある特定の記憶装置の低い信頼性は、安全な記憶手順を用いなければ、信頼性の役割は果たさないかも知れない。

【００５３】

したがって、本発明の本実施形態では、使用される記憶装置は、アップタイム（動作可能時間）、物理場所（移動通信装置１２に対する近接は、それがデータ記憶及び検索時間に影響を及ぼす可能性があるために望ましい）及び使用可能な容量などの多くのパラメータでそれらのサービス利用可能性を通知する。記憶機能が移動通信装置のユーザに課されるコストに基づいて記憶装置によって提供される場合、該特定の記憶装置を使用するコストも公表されてよい。

【００５４】

分散装置４６は、使用可能な記憶装置１８の間でどのようにしてデータフラグメントが分散されなければならないのかを決定する分散ポリシーを作成するために、一覧表示される記憶装置１８の特徴を使用する。次に、分散装置４６は、記憶装置１８の間でデータフラグメントを分散する。分散装置４６は、関係するデータの分散ポリシーに従って記憶装置１８からデータフラグメントを検索することもできる。

【００５５】

管理装置４２が動作する方法を、ここに図４を参照して説明する。図４に示されているプロセスは、オペレーティングシステム３０によって、つまり暗黙に且つユーザが知ることなく、あるいはユーザの制御下で、ユーザ入出力装置から受信されるユーザ入力アクションを介してユーザアプリケーション３４によって明示的に、安全な記憶のためのデータが安全データ記憶装置に渡されるときに開始する。該プロセスは、管理装置４２が記憶されるデータの制御を分割装置４４に渡すと、ステップＳ１－２で開始する。基本的に、この制御の通路は、分割装置４４に対するデータ自体の論理的な通路と見なすことができる。

【００５６】

事実上、データは、データの記憶時まで処理動作全体の間、ローカルデータ記憶装置３２に物理的に記憶されてよいが、データの制御は分割装置４４に渡される。

【００５７】

次に、処理はステップＳ１－４で、分割装置４４による分割が無事に終了したかどうかを設定することによって続行する。無事に終了しなかった場合には、プロセスはステップＳ１－２に戻り、データの制御を分割装置４４に渡してデータの分割を再度試行することによって続行する。

【００５８】
分割装置４４によるデータの分割が無事に行われた場合、次に管理装置４２は、ステップＳ１－６において結果として生じるデータのための分割ポリシーデータを記憶する。。この分割ポリシーは、データの検索時に分割装置４４によって生成されるデータフラグメントから元のデータを再組み立てするために使用される。
【００５９】
これに続き管理装置４２は、ステップＳ１－８で分散装置４６にデータの制御を渡す。ステップＳ１－１０では、管理装置４２は、分散が無事に行われたかどうかを確認する。前記のように、分散が無事に行われず、したがって管理装置４２が分散装置４６から分散ポリシーを受信しない結果となった場合には、ステップＳ１－８が繰り返され、分割されたデータの分散が再度試行される。
【００６０】
データフラグメントの分散が無事に行われた場合には、管理装置４２におけるプロセスは、結果として生じるデータのための分散ポリシーを記憶することによりステップＳ１－１２で続行する。この後者のポリシーは、データの検索の要求時に、分散装置４６がデータの分散されたフラグメントを検索できるようにし、その結果それらが分割装置４４により記憶されている分割ポリシーに従って再アセンブリできるようにする情報を提供する。そしてプロセスは終了する。
【００６１】
分割装置４４は図３にさらに詳しく示されており、安全に記憶されるデータを受信し、データを分析してどの分割アルゴリズムがどのような条件で適用されなければならないのかを確認するために動作可能であるデータアナライザ５０を有する。この命令の組み合わせが分割ポリシーとして知られている。この分割ポリシーは、分割ポリシーとともに安全に記憶されるデータを受信し、データを相応して分割するために動作可能であるデータ分割器５２に渡される。分割ポリシーは、万一データが後に検索される必要がある場合の記憶のために、管理装置４２にも戻される。その動作を実行するデータ分割器５２から生じるデータフラグメントは、分散ポリシーに従った分散のために分散装置４６に渡される。
【００６２】
ここで、データアナライザ５０の動作を、図５を参照して説明する。ステップＳ２－２では、安全に記憶されるデータに含まれるデータのタイプが決定される。テキストファイルあるいはビデオファイルまたは音声ファイルなどの多様な種類のデータが考えられる。使用される分割ポリシーはデータのタイプに依存するであろう。
【００６３】
例えば、テキストファイル（読み取り可能テキストの大部分を含む全てのファイル）は、好ましくは相対的に高い度合いで分割されなければならず、各フラグメントは文書全体を通して拡散される複数セクションから構成する。これは、１つまたは２つのフラグメントが危い場合にも、文書全体の完全な意味が既知とならないことを確実になると考えられる。これに対して、いくつかのビデオ及び音声コーデックは、失われるフレームを隔離するのには十分に耐性があり、したがってファイル構造がコンテンツの少なくとも一部の回復を可能にするので、交互配置されたフラグメントを特定することは不適切になり、したがってファイルを大きく連続的なパートに簡単に分割するのがより適切と考えられる。他の符号化された画像またはビデオのフォーマットは、ファイルがマルチメディアプレーヤで再生できるようにするためにファイル全体を使用できるようにする必要があり、したがってこのケースでは任意の分割ポリシーが適切となると思われる。
【００６４】
このようにして、ステップＳ２－４では、前記ステップで決定されたデータのタイプに適切な分割アルゴリズムが選択される。次にステップＳ２－６では、分割アルゴリズムが追加の使用のためにデータの分割ポリシーとして指定される。そして手順が終了する。
【００６５】
図６は、分割ポリシー及び分割されるデータの受信時に、分割装置４４のデータ分割器

５２で実行される分割のプロセスを示す。図６のプロセスの使用の特定の例が図７に示され、データ６０のパケットが処理ステップを通して渡される。該例はテキストファイルから構成され、データアナライザ５０により実行されるように図５のプロセスで確認されたデータのアイテムに基づいており、したがって分割ポリシーはデータのセクションへの高い度合いの分割から構成され、それぞれのフラグメントはテキストファイル全体を通して拡散されるセクションから構成されている。

【００６６】

このようにして、ステップＳ３－２では、データ６０は分割ポリシーに基づき、選択されたアルゴリズムを使用して分割される。図７に図示されるように、データは、フラグメントＡまたはＢに向かうことになるようにデータのさまざまなセクションを特定することにより分割される。次に、セクションはフラグメントの中に組み入れられる。

【００６７】

次にステップＳ３－４では、図７に図示されるようにフラグメントが名付けられ、それぞれのフラグメントは一意のフラグメント識別子（この例ではＡまたはＢ）及びデータ識別子（この例ではＸＸ）で名付けられる。これらの識別子により、該データの検索が必要とされるその後でのデータのトレーシングが可能になる。

【００６８】

ステップＳ３－６では、標識付データフラグメントがフラグメントの分散のために分散装置４６に渡される。

【００６９】

分散装置４６の動作を、ここで、分散装置４６がデータのフラグメントを分散できるプロセスを示す図８を参照して説明する。いつでも可能な分散の範囲は、使用可能な記憶装置１８の数、使用可能な記憶装置１８の信頼性、使用可能な装置１８の非有用性の任意の予想時間（動作不能時間(down time)）、移動通信装置１２のユーザが使用するための使用可能記憶装置１８の特性により課されるあらゆるコスト、及び（高速アクセス速度及び信頼性がある接続を促進する）記憶装置１８の物理的な接近に依存している。

【００７０】

したがって、図８に示されているプロセスのステップＳ４－２では、記憶装置１８の利用可能性及び信頼性が決定される。これは、使用可能記憶装置により利用できる情報に基づいて実行される。この情報は、放送によって、インターネットを介して情報を供給することによって、あるいは任意の他の従来の手段によって利用できてもよい。

【００７１】

次にステップＳ４－４では、分散ポリシーは、使用可能記憶装置１８の信頼性に基づき、及び前述されたような記憶されている特徴に基づいて決定される。この例では、全ての利用できる情報を考慮に入れるために全ての特徴が使用される。ステップＳ４－６では、分割装置４４によって生じたデータフラグメントが、決定された分割ポリシーに従って、分散装置４６によって分散される。最後に、ステップＳ４－８では、確立された分散ポリシーは記憶のために管理装置４２に渡され、その結果安全に記憶されるデータが検索されなければならないときには、分散ポリシーはアクセスを可能にするために分散装置４６に戻すことができる。

【００７２】

実際には、設計者は、アプリケーションに特定のハードウェアの動作により機能のどの態様が送達される必要があるのか、及びコンピュータ上でのソフトウェアの実行によりどれが送達される必要があるのかに関し、かなりの設計の自由を有することが理解されるであろう。

【００７３】

多様な異なる分割アルゴリズムを使用できるであろうことが理解される一方、図５に説明されるプロセスはある特定のデータにとって適切な分割アルゴリズムを決定する最も有効な方法を提供する。

【００７４】

本発明に従ってデータの安全な記憶を可能とするために、必ずしも記憶されるフラグメント数と同一程度の記憶装置台数がある必要はない。単一の記憶装置１８でデータの同じアイテムのいくつかの明らかに切断されたフラグメントを、他の記憶装置１８で他のこのようなフラグメントを記憶することにより、使用可能記憶装置１８の数が記憶されるフラグメントの数より少ない場合にも、分散の効果は少なくとも部分的に維持できることが理解できる。

【００７５】

分散ポリシーの決定においては、分散装置４６は記憶されている特徴のどれかまたは全てを考慮に入れてよいか、あるいは単に使用可能な記憶装置１８に基づいて分散ポリシーを決定してよいことが理解できる。

【００７６】

分割されたデータを再組み立てするプロセス同様に、データを分割するプロセスが固有の処理オーバヘッドを有することを認識しなければならない。したがって、データを分割するとき、及び検索時にデータを再組み立てするときの両方において、システムに不必要な処理要求を出すことになるので、分割の使いすぎはシステム性能に否定的な影響を及ぼす可能性がある。本発明の実施形態に従ってデータの分割及び分散に関連する処理要件を考慮する必要がある。

【００７７】

さらに、比較的遠隔のサーバ場所、または低いデータ検索率で接続を介してのみアクセス可能な場所が使用される場合には特に、分割されたデータを分散するプロセスはデータ検索率を高めることができる。本発明の好ましい実施形態では、分散ポリシーの決定はこの要因を考慮に入れる必要がある。

【００７８】

遠隔に記憶されているデータを利用することにより、移動通信装置自体の記憶情報より多くの情報の記憶を可能にする。しかしながら、いずれ、分割及び分散ポリシーのデータの蓄積が扱いにくくなり、本発明の実施形態はこの情報の遠隔且つ安全な記憶のための機能も含むことができた。好ましくは、頻繁にアクセスされるデータに関係する分割データ及び分散データは、高速検索を主として考慮しないで記憶できる、アクセス頻度の低いデータとは別に（できるだけ局所的に）記憶される。

【００７９】

データの分散がデータのセキュリティを維持するために適切なレベルでありつづけることを確実にするために、分割され、分散されたデータ上で分散アルゴリズム及び分割アルゴリズムは、周期的に実行される。さらに、これにより（記憶料金の増加または非利用可能性時間の改変などの）記憶装置１８の特徴のあらゆる変更を考慮に入れることができる。

【００８０】

図９は、管理装置４２が分割及び分散の効果を周期的にチェックする方法を示している。ステップＳ５－２では、管理装置４２は、チェックされる分割装置４４及び分散装置４６を使用して過去に遠隔に記憶されたデータアイテムを選択する。ステップＳ５－４では、データアイテムは、それがいつ最後にチェックされたのか、あるいはいつ最後に記憶されたのかを確認する。これが相対的に最近に発生した場合（移動通信装置自体の動作性能に関連して決定される基準）には、ステップＳ５－６で、管理装置４２は検討のために次のデータ装置を選択し、検索及び再記憶を正当化するために過去において十分な時間で記憶されたデータアイテムが検出されるまで、ステップＳ５－４で問い合わせを繰り返す。

【００８１】

ステップＳ５－８では、手順は続行し、管理装置４２は、分割装置４４及び分散装置４６を使用して選択されたデータアイテムの検索を命令する。これが達成されるプロセスは図１０に示され、さらに詳しく後述される。

【００８２】

前記に注記したように、分割装置４４がデータを分割し、分散装置４６がデータの分割

を分散するプロセスは、それらがそれぞれ分割ポリシー及び分散ポリシーの中で定められる一式のリバーシブル規則に従うため逆にできる。

【００８３】

ステップＳ５－８でデータの検索が無事に行われたのに続き、ステップＳ５－１０で、データは再記憶され、図４に示されている管理装置４２内のプロセスを利用する。次に、プロセスは、安全データ記憶装置４２により過去に記憶されたデータアイテムを追加検討するためにステップＳ５－６に戻ることによって続行する。

【００８４】

図９に示されているプロセスに図示されるように再記憶のため、あるいは移動通信装置１２の別のプロセスにおける使用のために問題のデータが必要とされているためなどの、データの検索のプロセスは図１０に示されている。ステップＳ６－２では、管理装置４２は、分散情報により特定されるデータが検索用であるという命令とともに、分散装置４６に分散情報（つまり分散ポリシー及び他の特定情報）を送信する。次に、分散装置４６は、情報を検索し、情報が検索された旨の信号を管理装置に送り返すように構成される。検索時、分散装置４６は、検索されたデータフラグメントに対する操作上の制御を管理装置４２に移す。

【００８５】

情報の検索、及び管理装置４２によるその旨のメッセージの対応する受信に続き、管理装置４２は、対応する分割ポリシー、及び分割装置４４がフラグメントからデータアイテムを再組み立てしなければならない旨の命令とともに、データフラグメントの操作上の制御を分割装置４４に渡す。分割装置４４は、データを分割するために使用される場合と同じ手順を、逆方向に適用する。データの再組み立ての完了時、分割装置４４は管理装置４２にメッセージを送り返し、再組み立てされたデータに対する操作上の制御を管理装置４２に移す。

【００８６】

次に、フラグメントの再組み立ての完了及びフラグメント装置４４からのメッセージの受信時、管理装置４２は、移動通信装置１０で実行される別のプロセスからの要求、または図９に示されているプロセスに再記憶されるデータとして、該再組み立てされたフラグメントを出力する。

【００８７】

本発明は、前述された特定の実施形態に示されているように、典型的な移動通信装置は局所的な記憶容量に対する制限を有するため、移動通信装置の動作に重要な利点を提供する。相対的に静的な装置を用いて非常に大量のメモリを提供できるのに対して、移動通信装置はある程度までその物理的なサイズによって制約を受ける。したがって、使いすぎ及びその結果生じる装置の故障を回避するために、メモリリソースを管理する必要がある。

【００８８】

したがって、移動通信装置に遠隔記憶を提供するための動機付けは高い。しかしながら、これは遠隔に記憶されるデータに固有の危険性につながる場合があり、本発明は、移動通信装置がユーザにより要求されるようにデータを検索できるようにデータを分割・分散することにより、この問題を解決する。

【００８９】

本発明は、一例として、本発明がハードウェアまたはソフトウェアに関して、あるいは該２つの組み合わせに関して装置の所定の機能性において具現化される移動通信装置に関連して説明されてきたが、本発明が、その上にロードされるソフトウェアによって構成される、汎用コンピュータまたはプログラマブル通信装置で提供でき、該ソフトウェアがコンピュータのための１つ以上のプログラムを備え、該プログラムまたは各プログラムがコンピュータプログラム製品からコンピュータの中にロードできることが理解できる。このようなコンピュータプログラム製品の例は、（光ディスクまたは磁気ディスクなどの）コンピュータ読み取り可能キャリヤ媒体、またはフラッシュメモリなどの電子記憶媒体、あるいはコンピュータで受信可能であり、コンピュータにロードされるときにコンピュータ

内でコンピュータプログラム製品を構築するための対応するコンピュータ実行可能命令を含むファイルを構成するデータを持つ信号を含む。

【００９０】

さらに、汎用コンピューティング装置の構成は、任意の使用可能な方法によりソフトウェアまたはハードウェアプラグインを既存の機能性に導入し、該コンピューティング装置を本発明の特定の実施形態に従って動作するように再構成することを含めることも考えられる。

【図面の簡単な説明】

【００９１】

【図１】移動通信網と通信している移動通信装置を含む、インターネットによって実現される通信システムの概略図である。

【図２】本発明の特定の実施形態に従って図１に示されている移動通信装置の安全データ記憶装置を描く概略図である。

【図３】図２に示されている安全データ記憶装置の分割装置４４を描く図である。

【図４】図２に示されている安全データ記憶装置の管理装置４２で実行される安全データ記憶管理プロセスを定めるフロー図である。

【図５】本発明の特定の実施形態に従ってデータが安全に記憶されるための分割ポリシーを決定するために、分割装置４４で実行されるデータ分析プロセスを定めるフロー図である。

【図６】図５に示されているプロセスで決定される分割ポリシーに従って実行されるデータ分割プロセスを定めるフロー図である。

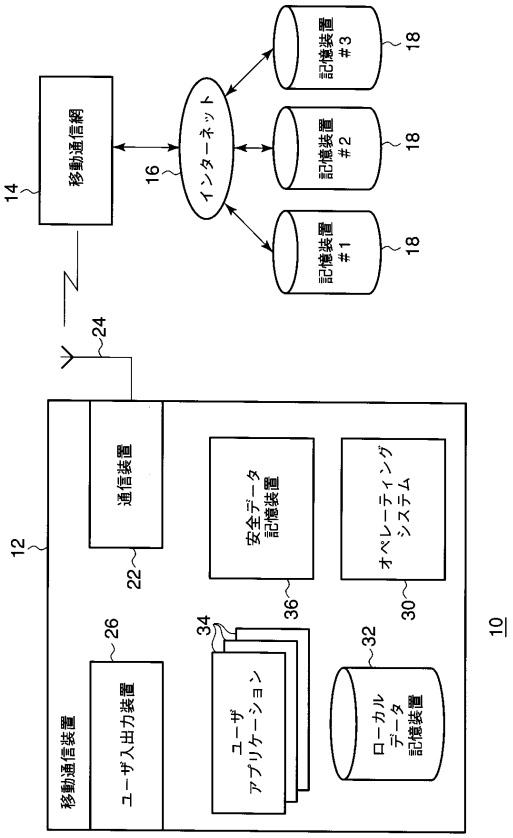
【図７】図５に示されているデータ分析プロセス、及び図６に示されているデータ分割プロセスの実行によるデータパケットの構造の概略図である。

【図８】図２に示されている安全データ記憶装置の分散装置によって実行されるデータ分散プロセスを定めるフロー図である。

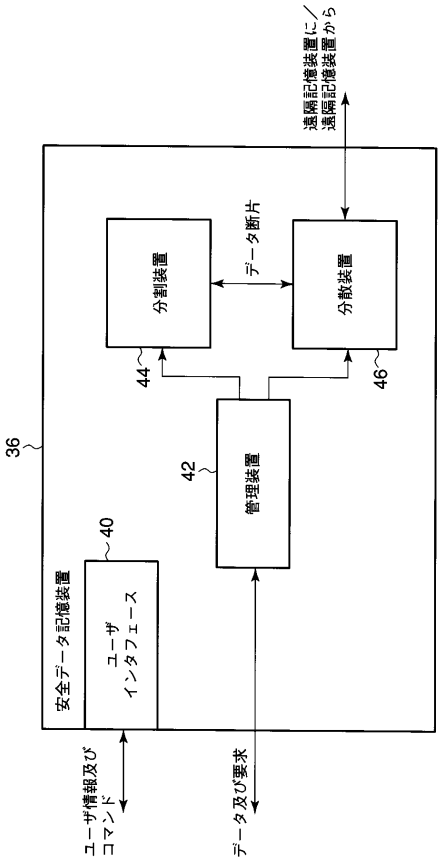
【図９】図４に示されているプロセスに従ってデータの記憶に関して管理装置により実行される分散データ管理プロセスを定めるフロー図である。

【図１０】図４に示されているプロセスに従って記憶されるデータで実行されるデータ検索プロセスを定めるフロー図である。

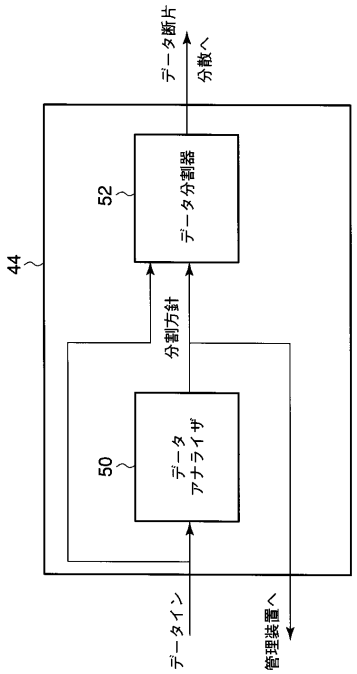
【図１】
図１



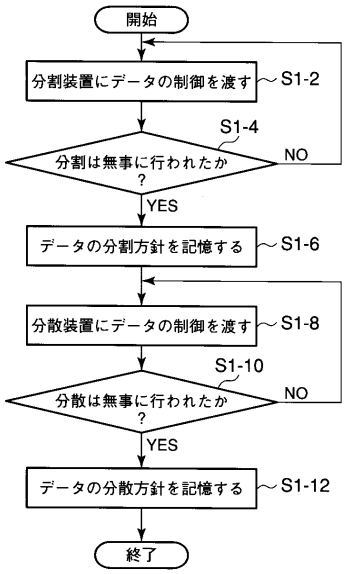
【図２】
図２



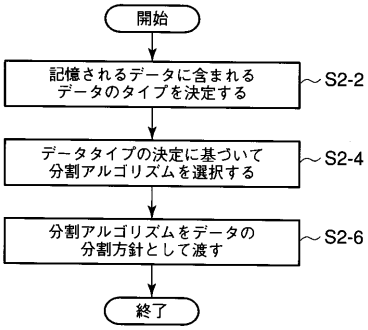
【図３】
図３



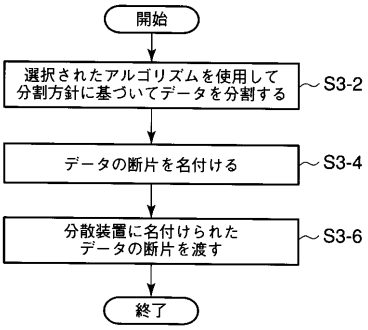
【図４】
図４



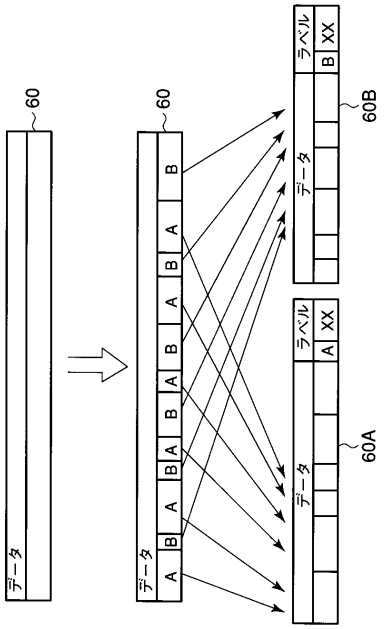
【図５】
図５



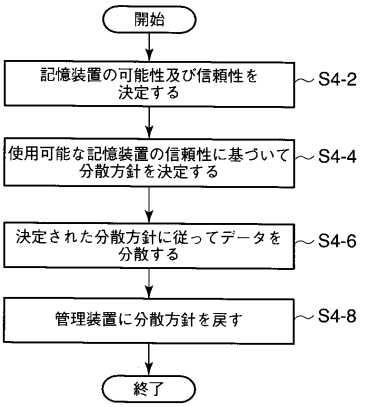
【図６】
図６



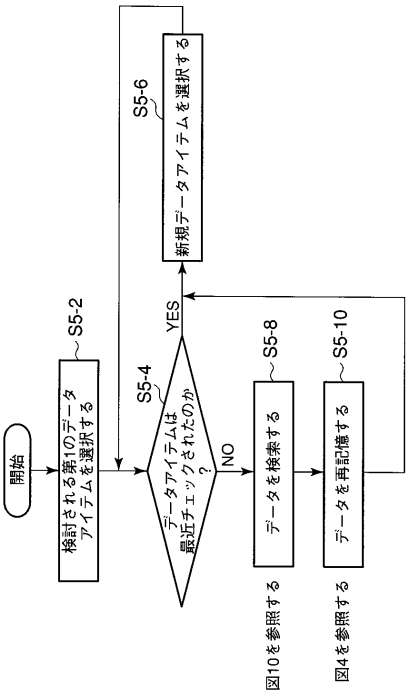
【図７】
図７



【図８】
図８

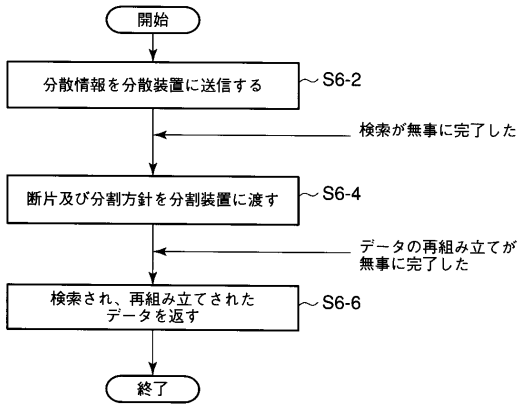


【図９】
図９



【図１０】

図10


開始
分散情報を分散装置に送信する
S6-2
検索が無事に完了した
断片及び分割方針を分割装置に渡す
S6-4
データの再組み立てが
無事に完了した
検索され、再組み立てされた
データを返す
S6-6
終了

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 グレイ・クレモ
イギリス国、 ビーエス１・４エヌデー、 ブリストル、 クウィーンスクエア ３２
(72)発明者 ラッセル・ジョン・ヘイネス
イギリス国、 ビーエス１・４エヌデー、 ブリストル、 クウィーンスクエア ３２
(72)発明者 ティモシー・アドリアン・ルウイス
イギリス国、 ビーエス１・４エヌデー、 ブリストル、 クウィーンスクエア ３２

Ｆターム(参考) 5B017 AA07 BA10 CA07
5B082 CA18

【外国語明細書】
2005293592000001.pdf