(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2005-158043
(P2005-158043A)
(43)公開日　平成17年6月16日(2005.6.16)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 12/14	G06F 12/14	510E	5B017
G06F 12/00	G06F 12/14	540A	5B082
G09C 1/00	G06F 12/00	537H	5J104
	G09C 1/00	660D	

審査請求 未請求　請求項の数 23　ＯＬ　（全 16 頁）

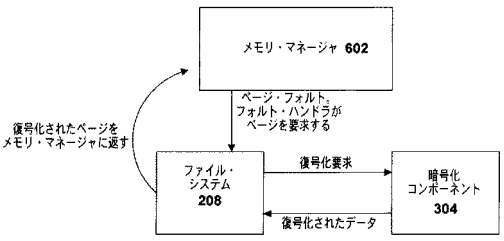
(21)出願番号　特願2004-308911 (P2004-308911)
(22)出願日　平成16年10月22日 (2004.10.22)
(31)優先権主張番号　10/721,562
(32)優先日　平成15年11月25日 (2003.11.25)
(33)優先権主張国　米国(US)

(71)出願人　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　ベンジャミン　エー．リース
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

最終頁に続く

(54)【発明の名称】システム・ページング・ファイルの暗号化

(57)【要約】
【課題】　オペレーティング・システムはメモリ領域を解放するためにメモリ・ページのデータをディスク上のページング・ファイルにコピーするが、この際に、そのデータを暗号化することによって、ページングされたデータを、不正な（あるいは望ましくない）監視から保護するメカニズムを提供すること。
【解決手段】　セッション・キーを使用してページング・ファイルに格納されるデータを暗号化し、セッション・キーはページング・ファイルが存在するマシンが起動した直後に生成される。ページング・ファイルのデータの暗号化と復号化の両方に使用されるセッション・キーは揮発性メモリに格納されるので、マシンが再起動した後にセッション・キーは残されていない。セッション・キーは再起動後には残されていないので、最新の起動に先立って格納された古いページング・ファイルのデータをクリア・テキストに復元できず、これにより、データを監視から保護する。
【選択図】　図６



【特許請求の範囲】
【請求項１】
仮想メモリを含むコンピューティング環境を提供するシステムであって、
揮発性メモリとハードディスクに格納されたページング・ファイルとの間でデータを移動したりまたはコピーしたりすることによって前記仮想メモリを提供する仮想メモリ・マネージャを備え、前記システムは前記ページング・ファイルに格納する前記データを暗号化することによって前記仮想メモリのコンテンツを保護することを特徴とするシステム。
【請求項２】
前記仮想メモリ・マネージャはファイル・システムに前記データを渡し、前記ファイル・システムは、前記データを前記ページング・ファイルに格納する前に前記データが暗号化されるようにすることを特徴とする請求項１に記載のシステム。
【請求項３】
前記ファイル・システムは暗号化するためのマークを前記ページング・ファイルに付け、前記ページング・ファイルは、前記ページング・ファイルに前記データを格納することを求める要求を受け取ったときに、前記ページング・ファイルに暗号化するためのマークが付けられていることを確認し、前記データを暗号化するように暗号化コンポーネントと通信することを特徴とする請求項２に記載のシステム。
【請求項４】
前記データの暗号化に使用され、さらに前記暗号化されたデータを後で復号化する場合に必要になるセッション・キーを生成するキー・ジェネレータをさらに備えることを特徴とする請求項１に記載のシステム。
【請求項５】
前記セッション・キーは、前記セッション・キーの生成後に起動が行われた場合に前記セッション・キーが使用できなくなるような方法で非永続的に格納されることを特徴とする請求項４に記載のシステム。
【請求項６】
前記セッション・キーが永続的には格納されないことを確実にすることによって前記仮想メモリのコンテンツを保護することを特徴とする請求項５に記載のシステム。
【請求項７】
前記データの暗号化は、
ＤＥＳ（Data Encryption Standard）、３ＤＥＳ（Triple-DES）、またはＡＥＳ（Advanced Encryption Standard）のうちの１つまたは複数のアルゴリズムを使用して行われることを特徴とする請求項１に記載のシステム。
【請求項８】
前記仮想メモリに格納されたユーザー・モードのすべてのアプリケーションとデータが前記ページング・ファイルに格納されるときに暗号化されることを確実にすることによって、前記仮想メモリのコンテンツを保護することを特徴とする請求項１に記載のシステム。
【請求項９】
仮想メモリを保護する方法であって、
揮発性メモリの複数のページにデータを格納すること、
前記揮発性メモリの前記複数のページの第１のページのコンテンツをディスクに格納されたページング・ファイルに移動することを決定すること、および
前記コンテンツを、前記コンテンツをページング・ファイルに格納する命令と共にファイル・システムに渡すこと
を備え、
前記ページング・ファイルに暗号化するためのマークが付けられ、
前記ファイル・システムは、前記コンテンツが前記ページング・ファイルに格納される前に、キーを使用して暗号化されるようにし、
前記キーは前記ページング・ファイルに格納された情報を復号化するために必要であり

、前記キーは、前記キーが格納されたマシンを再起動すると前記キーが失われるような方法で格納される
ことを特徴とする方法。
【請求項１０】
前記マシンを起動するときに前記キーを生成すること
をさらに備えることを特徴とする請求項９に記載の方法。
【請求項１１】
前記キーを生成する前に前記揮発性メモリのブロックをワーク・ペースとして使用することを予約することをさらに備え、それによって前記ワーク・スペースを使用することで、前記セッション・キーを生成する前に揮発性メモリのコンテンツをディスクにコピーする必要がなくなることを特徴とする請求項９に記載の方法。
【請求項１２】
前記ファイル・システムは暗号化コンポーネントを通信することによって前記コンテンツが暗号化されるようにし、暗号化コンポーネントは前記ファイル・システムによって暗号化するためのマークを付けられたファイルを暗号化することを特徴とする請求項９に記載の方法。
【請求項１３】
さらに、ファイル・システムと暗号化コンポーネントの間でデータをやりとりするための前記揮発性メモリのブロックを予約することを含むことを特徴とする請求項１２に記載の方法。
【請求項１４】
コンピュータの仮想メモリのデータを格納する暗号化されたページング・ファイルをメンテナンスするシステムであって、
データを受け取り、キーを使用して前記データの暗号化と復号化の操作を実行する暗号化コンポーネントと、
前記キーを生成するメカニズムと、
前記コンピュータを再起動したときに前記キーが保存されていないような方法で前記キーを格納する前記コンピュータ内の記憶場所と、
コピーまたは移動したデータをページング・ファイルにファイル・システムが格納することを要求することによって、揮発性メモリからディスクにデータをコピーまたは移動する仮想メモリ・マネージャと
を備え、
前記ファイル・システムは、キーを使用して前記コピーまたは移動したデータを暗号化するように前記暗号化コンポーネントに対して指示することを特徴とするシステム。
【請求項１５】
前記暗号化コンポーネントは起動時にメモリのブロックを予約することを特徴とする請求項１４に記載のシステム。
【請求項１６】
前記メモリのブロックは前記キーを生成する前に前記暗号化コンポーネントのワーク・ペースとして使用され、それによって前記暗号化コンポーネントがデータを操作するための十分な記憶領域が、前記キーを生成する前に前記揮発性メモリ内に存在することを特徴とする請求項１５に記載のシステム。
【請求項１７】
前記メモリのブロックは、前記ファイル・システムと前記暗号化コンポーネントとの間で情報をやりとりするためのバッファとして使用されることを特徴とする請求項１５に記載のシステム。
【請求項１８】
前記キーは、前記仮想メモリ・マネージャが前記ページング・ファイルにデータを格納するように指示する前に、生成されることを特徴とする請求項１４に記載のシステム。
【請求項１９】

前記キーは前記揮発性メモリに格納され、前記キーのコピーは前記コンピュータの不揮発性のメモリまたは記憶装置のいずれにも格納されないことを特徴とする請求項１４に記載のシステム。

【請求項２０】

コンピュータ起動時に行われる方法を実行するコンピュータで実行可能な命令で符号化されたコンピュータ可読媒体であって、前記方法は、

セッション・キーを生成すること、

前記セッション・キーを、マシンを再起動した後に残さないような非永続的な方法で格納すること、

ディスクに格納された仮想メモリのデータが暗号化されるように指示する情報を取得すること、

ページング・ファイルを暗号化ファイルとしてマーク付けすること、

ディスク上の前記ページング・ファイルに格納すべき揮発性記憶装置のデータをメモリ・マネージャから受け取ること、および

前記受け取ったデータを前記ページング・ファイルに格納する前に、セッション・キーを使用して前記受け取ったデータを暗号化することによって、前記受け取ったデータを監視されないように保護すること

を備えることを特徴とするコンピュータ可読媒体。

【請求項２１】

前記セッション・キーを生成する前にメモリ・ブロックを予約することをさらに備え、前記メモリ・ブロックは、

ページング・ファイルをメンテナンスするファイル・システムと、セッション・キーを使用してデータの暗号化および復号化を実行する暗号化コンポーネントとの間でデータをやりとりするためのバッファと、

前記セッション・キーを生成する前に前記暗号化コンポーネントが使用可能なワーク・スペースと

のいずれかとして使用されることを特徴とする請求項２０に記載のコンピュータ可読媒体。

【請求項２２】

前記セッション・キーは前記揮発性記憶装置に格納され、前記セッション・キーのコピーはディスクに格納されないことを特徴とする請求項２０に記載のコンピュータ可読媒体。

【請求項２３】

仮想メモリを保護する方法であって、

揮発性メモリの複数のページにデータを格納すること、

前記揮発性メモリの前記複数のページの第１のページのコンテンツをディスクに格納されたページング・ファイルに移動することを決定すること、

前記コンテンツを、前記コンテンツをページング・ファイルに格納する命令と共にファイル・システムに提供すること

を備え、

前記ページング・ファイルは暗号化するためのマークが付けられ、

前記ファイル・システムは、前記コンテンツが前記ページング・ファイルに格納される前にキーを使用して前記コンテンツが暗号化されるようにし、

前記キーは前記ページング・ファイルに格納された情報を復号化するのに必要であり、前記キーは、前記キーが格納されたマシンを再起動すると前記キーが失われるような方法で格納される

ことを特徴とする方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、一般にコンピューティングのファイルに関し、特に仮想メモリのページング・ファイルを暗号化および復号化するメカニズムに関する。

【背景技術】

【０００２】

今日のコンピュータ・システムは、物理的なＲＡＭ（random access memory）のサイズを超えるメモリ容量の使用を可能にする仮想メモリの機能を提供するのが一般的である。仮想メモリシステムでは、物理アドレス空間より大きいこともある仮想アドレス空間を使用できる。物理アドレス空間のコンテンツ（contents）がオーバーフローしないように仮想メモリを維持するために、物理メモリより大きな領域が必要な場合は物理メモリからページがコピー・アウト（copy out）され、プログラムでこうしたページへのアクセスが必要な場合は物理メモリにページがコピー・イン（copy into）される。物理メモリからページがコピー・アウトされる場合は、該当するページのコンテンツが「ページング・ファイル」と呼ばれるファイルの形態でディスク上に格納される。

【０００３】

【特許文献１】米国特許第６，２４９，８６６号明細書
【特許文献２】米国特許第５，９２０，８９５号明細書
【特許文献３】米国特許第５，９３１，９４７号明細書
【特許文献４】米国特許第６，３３０，６７０号明細書
【特許文献５】米国特許第６，４０５，３１５号明細書
【特許文献６】米国特許第６，４４２，６５４号明細書

【発明の開示】

【発明が解決しようとする課題】

【０００４】

メモリ・ページのイメージをディスクに格納することによる問題は、たとえその格納が一時的であっても、こうしたページのコンテンツの不正な監視（observation）を防止するのが難しい、ということである。物理メモリは一般的には揮発性メモリであり、システムの電源が切断されるとそのコンテンツが失われる。したがって、システムが電源切断、クラッシュ、あるいは再起動（reboot）した場合に、揮発性メモリに格納された機密のデータは不正な監視者によって復元されないことが確実にされる。しかし、データが揮発性メモリからページング・ファイルにコピーされると、だれでもディスクにアクセスしてデータを監視でき、電源切断イベント、クラッシュ、あるいは再起動の後でもこのデータはディスク上に存在することになる。そのデータが機密の場合あるいはセンシティブな場合は、アタッカーがディスクからデータを入手する恐れがあるので、こうした可能性は、セキュリティ・リスクを示している。

【０００５】

以上の観点から、先行技術の弱点を克服するページング・ファイル保護メカニズムを求めるニーズが存在する。

【課題を解決するための手段】

【０００６】

本発明は、ページング・ファイルに格納するデータを暗号化することによってページング・ファイルを保護する。本発明に従って、このページング・ファイルには暗号化するためのマークが付けられる。このページング・ファイルは、ファイル暗号化機能を備えるファイル・システムに格納される。ファイルを暗号化できるファイル・システムについては、特許文献１に記載されており、参考のためここに引用する。このページング・ファイルに格納されるべきデータが仮想メモリ・マネージャからファイル・システムに渡されると、このファイル・システムは、ページング・ファイルが暗号化のためにマーク付けされていることを確認し、そのデータをページング・ファイルに格納する前に、そのデータが暗号化されるようにする。ファイル・システムは、暗号化コンポーネントに対して実際に暗号化を実行するように指示できる。暗号化コンポーネントはファイル・システムからクリア・テキスト（平文：暗号化されていない文）を受け取って、暗号化キーを適用して暗号

文（ciphertext）を作成し、ページング・ファイル内に格納されるように、ファイル・システムに暗号文を返す。

【０００７】

既存のファイル暗号化システムでは、一般にファイルを暗号化し、ファイルの復号化に必要なキーのコピーも永続的に保存する。こうしたファイルについてキーを永続的に保存するのは意味がある、なぜならば、通常のファイルは長期間の保存を意図しており、通常はマシンを起動（boot）した際は、その起動が何回目であってもファイルを復号化するときにキーが必要になる。ページング・ファイルは、コンピューティング環境の唯一のインスタンス（instantiation）というコンテクスト（マシンが１度起動（boot）してから再起動（reboot）するまでの間）でのみ意味があるデータの一時的なリポジトリであるという点で通常のファイルとは異なる。したがって、システムが再起動した後はページング・ファイル・データにはほとんど価値が存在せず、また、このデータを使用可能な形で格納することはセキュリティ・リスクを招くという意味で問題である。したがって、ページング・ファイルの復号化に必要なキーを永続的に保存することは、データ（機密の、あるいはセンシティブなデータを含む）がいくつかの予測できないコンテクスト（たとえば、当該マシンのハードディスクを取り外してハッカーのマシンに取り付けた場合など）で復号化されることを可能にすることがあるので、不都合である。本発明の１つの機能に従って、１回の起動で１つのセッション・キーが生成され、システムの１回の稼働中（run）（起動してから再起動するまでの間）に限り、このセッション・キーを使用してページング・ファイルのコンテンツが暗号化され、復号化される。このセッション・キーは、マシンの１回の起動(boots)が終了した後は保存されない。

【０００８】

物理メモリ・ページのページング・ファイルへのコピーは起動後の任意のタイミングで必要になる可能性があるので、ページング・ファイルへの書き込み要求に対してセッション・キーは確実に対応できるようにするために、セッション・キーは、マシンが起動した直後に作成されるのが好ましい。キーを生成するコンポーネントは、起動の直後に物理メモリのブロックを予約するのが好ましい。こうして予約されたメモリは、暗号化コンポーネントがページング・ファイルに格納するデータを暗号化するときに使用するワーク・スペースとして、および／またはファイル・システムと暗号化コンポーネントとの間でデータを渡すためのバッファとして、使用できる。

【０００９】

本発明の他の機能について以下に説明する。

添付の図面を参照しながら以上の課題を解決するための手段と、好適な実施形態についての後述の詳細な説明を読むことにより、本発明をより深く理解できる。本発明を説明するために本発明の例示的な構成を図示するが、本発明は開示されたこの特定の方法および手段には限定されない。

【発明を実施するための最良の形態】

【００１０】

概要

仮想メモリ・マネージャは、マシンの揮発性の物理メモリより大きな仮想アドレス空間を提供する。仮想メモリ・マネージャは、必要に応じて揮発性メモリにデータをコピー・インしたり、揮発性メモリからコピー・アウトしたりすることによってこの作業を実行する。揮発性メモリからデータがコピー・アウトされる場合、このデータは、ディスク上に、ページング・ファイルの形態で格納される。本発明は、ページング・ファイル・データを暗号形式で保存することによって、ページング・ファイルに格納されたデータが不正な監視から保護されるメカニズムを提供する。

【００１１】

コンピューティング環境の例

図１は、本発明の機能を実現できる例示的なコンピューティング環境を示している。コンピューティング・システム環境１００は適切なコンピューティング環境の１つの例にす

ぎず、本発明の使い方または機能の範囲に関するいかなる制限も示さない。また、コンピューティング環境１００は、例示的なオペレーティング環境１００に示すコンポーネントの１つまたは組合わせに関して依存性も要件もないものとする。

【００１２】

本発明は、他のさまざまな汎用または専用のコンピューティング・システム環境または構成にも適用できる。本発明の使用に適した周知のコンピューティング・システム、環境、および／または構成の例には、パーソナル・コンピュータ、サーバー・コンピュータ、ハンドヘルドまたはラップトップ・デバイス、マルチ・プロセッサ・システム、マイクロ・プロセッサ・ベースのシステム、セットトップボックス、プログラム可能な家庭用電子機器、ネットワークＰＣ、ミニ・コンピュータ、メインフレーム・コンピュータ、埋め込みのシステム、前述の任意のシステムまたはデバイスを含む分散コンピューティング環境などが含まれるが、これらに限定はされない。

【００１３】

本発明は、プログラム・モジュールのようにコンピュータで実行可能な命令をコンピュータで実行する一般的なコンテクストで説明できる。一般に、プログラム・モジュールには、ルーチン、プログラム、オブジェクト、コンポーネント、データ構造などがあり、特定のタスクを実行したり、特定の抽象データ型を実装したりする。本発明は、通信ネットワークなどのデータ送信媒体を介してリンクするリモート処理装置でタスクを実行する分散コンピューティング環境でも実施できる。分散コンピューティング環境では、メモリ記憶装置を含むローカルとリモートの両方のコンピュータ記憶媒体にプログラム・モジュールとそれ以外のデータを格納できる。

【００１４】

図１を参照すると、本発明を実施する例示的なシステムに、コンピュータ１１０の形で汎用のコンピューティング・デバイスが配置されている。コンピュータ１１０のコンポーネントには、処理装置１２０、システム・メモリ１３０、さまざまなシステム・コンポーネント（システム・メモリと処理装置１２０など）を接続するシステム・バス１２１が含まれるが、それらに限定はされない。処理装置１２０は、マルチ・スレッド・プロセッサでサポートする処理装置など、複数の論理処理装置を表すことができる。システム・バス１２１は、さまざまなバス・アーキテクチャの任意の１つを使用したメモリ・バスまたはメモリ・コントローラ、周辺バス、ローカル・バスを含む各種バス構造のいずれでもよい。こうしたアーキテクチャには、例として、ＩＳＡ（Industry Standard Architecture）バス、ＭＣＡ（Micro Channel Architecture）バス、ＥＩＳＡ（Enhanced ISA）バス、ＶＥＳＡ（Video Electronics Standards Association）ローカル・バス、ＰＣＩ（Peripheral Component Interconnect）バス（メザニン（Mezzanine）バスとも呼ばれる）が含まれるが、これらに限定はされない。システム・バス１２１は、ポイント・ツー・ポイント接続、スイッチング・ファブリック、あるいは通信装置間の同様の機能としても実現できる。

【００１５】

コンピュータ１１０は、通常はさまざまなコンピュータ可読媒体を備えている。コンピュータ可読媒体は、コンピュータ１１０からアクセスできる任意の使用可能な媒体を含むことができるが、揮発性と不揮発性の両方、および取り外し可能と不可能の両方の媒体を含むことができる。例として、コンピュータ可読媒体にはコンピュータ記憶媒体および通信媒体を含めることができるが、これらに限定はされない。コンピュータ記憶媒体には、コンピュータ可読の命令、データ構造、プログラム・モジュール、またはその他のデータなどの情報を記憶する任意の方法または技術で組み込まれた、揮発性と不揮発性の両方、および取り外し可能と不可能の両方の媒体が含まれる。コンピュータ記憶媒体には、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュ・メモリなどのメモリ技術、ＣＤ　ＲＯＭ、デジタル多用途ディスク（ＤＶＤ：digital versatile disk）などの光ディスク記憶装置、磁気カセット、磁気テープ、磁気ディスクなどの磁気記憶装置、または必要な情報を格納でき、コンピュータ１１０からアクセスできる他の任意の媒体が含まれるが、これらに限定

はされない。通信媒体は、搬送波やその他の搬送メカニズムのような変調データ信号の形態で、コンピュータ可読の命令、データ構造、プログラム・モジュール、またはその他のデータなどを具現化しており、この通信媒体は任意の情報伝配信媒体を含む。「変調データ信号」という用語は、信号内で情報を符号化する方法で、１つまたは複数の特性を設定された、または変更された信号を意味する。例として、通信媒体には、有線ネットワーク、直接ワイヤ接続などの有線媒体と、音、ＲＦ、赤外線などの無線媒体が含まれるが、これらに限定はされない。上記の任意の組合わせも、コンピュータ可読媒体の範囲内に含まれるものとする。

【００１６】

システム・メモリ１３０には、読み取り専用メモリ（ＲＯＭ：read only memory）１３１やランダム・アクセス・メモリ（ＲＡＭ：random access memory）１３２のように揮発性および／または不揮発性メモリという形をとるコンピュータ記憶媒体が含まれる。起動時などにコンピュータ１１０内のエレメント間の情報転送を支援する基本ルーチンを含む基本入出力システム１３３（ＢＩＯＳ：basic input/output system）は、通常はＲＯＭ１３１に格納される。ＲＡＭ　１３２には、通常は処理装置１２０から、ダイレクトにアクセス可能であり、かつ／または処理装置１２０で現在操作しているデータおよび／またはプログラム・モジュールが格納される。例として、図１にはオペレーティング・システム１３４、アプリケーション・プログラム１３５、その他のプログラム・モジュール１３６、およびプログラム・データ１３７が示されているが、これらに限定はされない。

【００１７】

コンピュータ１１０には、その他の取り外し可能／不可能、揮発性／不揮発性のコンピュータ記憶媒体を含めることができる。単に例として、図１に取り外し不可能な不揮発性の磁気媒体の読み出しまたは書き込みを行うハードディスク・ドライブ１４０、取り外し可能な不揮発性の磁気ディスク１５２の読み出しまたは書き込みを行う磁気ディスク・ドライブ１５１、ＣＤ　ＲＯＭや他の光媒体のような取り外し可能な不揮発性の光ディスク１５６の読み出しまたは書き込みを行う光ディスク・ドライブ１５５を示す。例示的なオペレーティング環境で使用できる上記以外の取り外し可能／不可能、揮発性／不揮発性のコンピュータ記憶媒体には、磁気テープ・カセット、フラッシュ・メモリ・カード、ＤＶＤ、デジタル・ビデオ・テープ、ソリッド・ステートＲＡＭ、ソリッド・ステートＲＯＭなどが含まれるが、それらに限定はされない。ハードディスク・ドライブ１４１は、通常はインターフェース１４０などの取り外し不可能なメモリ・インターフェースを介してシステム・バス１２１に接続し、磁気ディスク・ドライブ１５１と光ディスク・ドライブ１５５は、通常はインターフェース１５０などの取り外し可能なメモリ・インターフェースを介してシステム・バス１２１に接続する。

【００１８】

図１に示す前述のドライブとこれに対応するコンピュータ記憶媒体には、コンピュータ可読の命令、データ構造、プログラム・モジュールなど、コンピュータ１１０のデータを格納できる。たとえば、図１を参照すると、ハードディスク・ドライブ１４１にオペレーティング・システム１４４、アプリケーション・プログラム１４５、その他のプログラム・モジュール１４６、およびプログラム・データ１４７が格納されている。ただし、こうしたコンポーネントは、オペレーティング・システム１３４、アプリケーション・プログラム１３５、その他のプログラム・モジュール１３６、およびプログラム・データ１３７と同じとすることも、または異なるものとすることができる。ここでは、オペレーティング・システム１４４、アプリケーション・プログラム１４５、その他のプログラム・モジュール１４６、およびプログラム・データ１４７には異なる番号を付けて、少なくとも別の複製であることを示している。ユーザーは、キーボード１６２やポインティング・デバイス１６１（一般に、マウス、トラック・ボール、またはタッチ・パッドと呼ばれる）などの入力装置を使用してコンピュータ２０にコマンドや情報を入力できる。他の入力装置（図示せず）には、マイクロフォン、ジョイスティック、ゲーム・パッド、サテライト・ディッシュ、スキャナなどを含めることができる。これらの入力装置および他の入力装置

は、多くの場合にシステム・バスに接続されたユーザー入力インターフェース１６０を介して処理装置１２０に接続するが、パラレル・ポート、ゲーム・ポート、ＵＳＢ（universal serial bus）のような他のインターフェースやバス構造によって接続することもできる。モニタ１９１または他のタイプの表示装置も、ビデオ・インターフェース１９０のようなインターフェースを介してシステム・バス１２１に接続される。さらに、コンピュータには出力周辺インターフェース１９５を介してスピーカ１９７やプリンタ１９６など、モニタ以外の出力周辺装置を接続できる。

【００１９】

コンピュータ１１０は、リモート・コンピュータ１８０のような１台または複数台のリモート・コンピュータへの論理接続を使用してネットワーク環境で動作できる。リモート・コンピュータ１８０は、パーソナル・コンピュータ、サーバー、ルータ、ネットワークＰＣ、ピア・デバイス、または他の一般のネットワーク・ノードでよい。通常は、コンピュータ１１０に関連して上で説明したエレメントの多くまたはすべてが含まれるが、図１にはメモリ記憶装置１８１のみを示す。図１に示す論理接続には、ローカル・エリア・ネットワーク（ＬＡＮ：local area network）１７１とワイド・エリア・ネットワーク（ＷＡＮ：wide area network）１７３が含まれるが、他のネットワークを含めてもよい。このようなネットワーキング環境は、職場、企業規模のコンピュータ・ネットワーク、イントラ・ネット、およびインターネットではごく一般的である。

【００２０】

ＬＡＮネットワーキング環境で使用した場合、コンピュータ１１０はＬＡＮ １７１にネットワーク・インターフェースまたはアダプタ１７０を介して接続する。ＷＡＮネットワーキング環境で使用した場合、コンピュータ１１０は一般にインターネットなどのＷＡＮ １７３を介して通信を確立するためのモデム１７２またはその他の手段を備えている。モデム１７２（内蔵または外付け）は、ユーザー入力インターフェース１６０または他の適切なメカニズムを使用してシステム・バス１２１に接続できる。ネットワーク環境では、コンピュータ１１０またはその一部に関連して記述したプログラム・モジュールは、リモート・メモリ記憶装置に格納できる。例として、図１にメモリ・デバイス１８１に格納されたリモート・アプリケーション・プログラム１８５を示すが、これには限定されない。図示されたネットワーク接続が例示的であり、コンピュータ間の通信リンクを確立する他の手段を使用することができることは言うまでもない。

【００２１】

メモリ・ページをページング・ファイルに格納する

図２は、コンピュータ・メモリ、およびメモリのページを格納できるファイル・システムを示している。コンピュータ・システムは、ＲＡＭ １３２のようなメモリを備えている。ＲＡＭ １３２は、複数のページに体系化できるメモリの複数のバイトを備えている。各ページは、隣接する特定のサイズのメモリ・ブロックであり、一般的なシステムでは、４ＫＢ（キロバイト）、または４ＭＢ（メガバイト）、あるいは同時に両方のページ・サイズをサポートする。図２の例で、ＲＡＭ １３２にはページ２０２（１）、２０２（２）、２０２（３）、２０２（４）、２０２（５）…２０２（ｎ）が含まれる。

【００２２】

ファイル・システム２０８は、ディスク上にファイル形式でデータを格納し、また、ファイルを体系化（たとえば、ファイルのディレクトリをメンテナンスすることによる）したり、ファイルの格納と取得を実行したり、ファイルのメンテナンスに関連するその他のタスクを実行したりするのに必要なソフトウェアおよび／またはハードウェアも備えている。図２の例では、ファイル・システム２０８は、ファイル２０４（１）、２０４（２）…２０４（ｍ）を格納する。さらに、ファイル・システム２０８は、ページング・ファイル２０６のような１つまたは複数のページング・ファイルを格納できる。ページング・ファイル２０６は、ページのコピーをディスクで格納するために使用するファイルである。任意のプログラムがページング・ファイルをメンテナンスできるが、オペレーティング・システム（たとえば、図１に示すオペレーティング・システム１３４）がページング・

ファイルをメンテナンスし、すべてのアプリケーションやプロセスがこれを共有するのがきわめて一般的である。この例では、ページング・ファイル２０６はオペレーティング・システム１３４でメンテナンスするページング・ファイルである。ＭＩＣＲＯＳＯＦＴ ＷＩＮＤＯＷＳ（登録商標）オペレーティング・システムは、こうしたページング・ファイルをメンテナンスするオペレーティング・システムの例である。オペレーティング・システム１３４は、メモリ領域の解放が必要な場合に、メモリのページをページング・ファイル２０６にコピーする。たとえば、オペレーティング・システム１３４はページ２０２（４）のコンテンツをページング・ファイル２０６にコピーし、ページ２０２（４）の物理メモリを再割当てして他のデータを格納できるようにすることによってＲＡＭ １３２の領域を解放することを決定できる。これとは逆に、オペレーティング・システム１３４がデータへのアクセス要求を受け取ったが、このデータはすでにページング・ファイル２０６にコピーされたページにあるためにＲＡＭ １３２には格納されていない場合（すなわち、仮想アドレス変換テーブルで”ｎｏｔ ｐｒｅｓｅｎｔ（存在しない）”とマーク付けされたページにアクセスしようとしたためにページ・フォルト例外が発生した場合）、オペレーティング・システム１３４は要求されたページのコンテンツをページング・ファイル２０６からコピーしてＲＡＭ １３２の物理ページフレームに配置する（アドレス変換テーブルが新しいページの位置を指し示すように調整も行う）。

【００２３】

ファイル・システム２０８が提供する１つの機能は、図３に示すファイル暗号化コンポーネントである。すでに図２に関連して示し、説明したように、ファイル・システム２０８は、複数のファイル（ファイル２０４（１）、２０４（２）、２０４（３）など）を格納している。暗号化コンポーネント３０４は、キー３０２を使用してファイルを暗号化および復号化する機能を提供する。ファイル・システム２０８には、暗号形式とクリア形式のいずれのファイルでも格納できるのが好ましい。この場合は、ファイル・システム２０８に格納された各ファイルにフラグが関連付けられており、ファイルを暗号形式でメンテナンスするかどうかによってフラグをセットまたは解除できる。図３の例では、（ファイル２０４（２）に関連付けられた）フラグ３１０がセットされており、ファイル２０４（２）が暗号化されることを示している。

【００２４】

暗号化コンポーネント３０４は、ファイルを暗号化および復号化する機能を提供する。したがって、ファイル・システム２０８がファイル２０４（２）（あるいはフラグによって暗号化するためのマークが付けられた他の任意のファイル）にデータを格納するようにという要求を受け取ると、ファイル・システム２０８は暗号化コンポーネント３０４を呼出し、格納するクリア・テキスト３０６を暗号化コンポーネント３０４に渡す。次に、暗号化コンポーネント３０４はキー３０２を使用してクリア・テキスト３０６を暗号化し、暗号文３０８をファイル・システム２０８に返す。これで、暗号文がファイル２０４（２）に格納される。ファイル・システム２０８がファイル２０４（２）の情報を取得するようにという要求を受け取ると、ファイル・システム２０８はその時点でファイル２０４（２）に暗号化するためのマークが付けられていることを確認し、このファイルの暗号化された暗号文を暗号化コンポーネント３０４に渡す。次に、暗号化コンポーネント３０４がキー３０２を使用して暗号文を復号化してクリア・テキストを返し、さらにファイル・システム２０８がこのクリア・テキストを要求元に渡す。好ましい実施形態において、暗号化コンポーネント３０４は、ＤＥＳ（Data Encryption Standard）、３ＤＥＳ（Triple-DES）、ＡＥＳ（Advanced Encryption Standard）のような対称のキー・アルゴリズムを使用して、暗号化と復号化を実行する。

【００２５】

好ましい実施形態において、暗号化コンポーネント３０４はキー３０２を生成する機能を備えており、暗号化コンポーネント３０４はファイル・システム２０８を管理するソフトウェアにキー３０２を提供する。図４に関連して後述するように、キー３０２はシステム起動直後に生成され、不揮発性のストレージには保存されない。

【００２６】
システムは、暗号化フラグをセット状態で、あるいは解除状態でページング・ファイル作成すべきかどうかを決定するセキュリティ・ポリシーをローカルまたは中央に備えているのが好ましい。たとえば、ページング・ファイルの暗号化を実行するかどうかを示すレジストリ・エントリがあってもよい。起動時、つまりシステムが特定のセッションのページング・ファイルを作成するときに、システムはレジストリを調べてページング・ファイルの暗号化フラグをセットすべきかどうかを確認できる。
【００２７】
システム・ページング・ファイルを暗号化するためのシステムの準備
図４は、ページング・ファイルを暗号化するようにシステムを準備するプロセスを示す流れ図である。まず、暗号化されたページング・ファイルを使用するシステムが起動する（４０２）。起動に続いて、特定の目的で使用するメモリのブロックが予約される（４０４）。具体的には、予約されたメモリ・ブロックは以下の目的で利用できる。第一に、予約されたメモリの一部は、ファイル・システムと暗号化コンポーネントの間でデータの両方向の書き込みを行うためのバッファとして利用できる（ファイル・システムと暗号化コンポーネントの間でデータの書き込みを実行しようとしたときに、予約されたメモリが不十分な場合は、書き込みを複数のステージに分割するか、またはより多くのメモリを割り当てようとすることができる）。第二に、予約されたメモリの一部は、暗号化コンポーネント用のワーク・スペースとして使用できる。
【００２８】
次に、ページング・ファイルの暗号化に使用することになるセッション・キーが作成され、ディスクなどにページングされない揮発性メモリに格納される（４０６）。セッション・キーは、次回の起動時には残されていない方法で格納されるのが好ましい。こうすれば、１回の起動中に生成され、暗号化されたページング・ファイルのデータを、現在のセッションが終了した後に復号化することはできない。このことによって、このデータのセキュリティが保護される（たとえば、コンピュータからハードディスクを取り外したり盗んだりして、そのディスクを別のマシンに取り付けても、ページング・ファイルのデータの復号化を可能にすることになるセッション・キーのコピーを、そのディスクは格納していないはずである）。セッション・キーは、最終的にディスクにはページングされることがないように、ページングされないメモリに格納されることが好ましい（セッション・キーをディスクにページングすると、セキュリティ上の問題の可能性が発生するだけでなく、キーが格納されたページング・ファイルを復号化するためにキーが必要になるのでデッドロックが発生する可能性もある）。図４ではメモリ・ブロックが予約された後にセッション・キーが作成されているが、この順序は本発明において必須ではない。
【００２９】
これで、ファイルの暗号化フラグがセットされた状態で、ページング・ファイルが作成される（４０８）。この時点で、システムはページング・ファイルを暗号化する準備が完了する。メモリ・マネージャがメモリとページング・ファイルの間でデータをやりとりする際に、データはセッション・キーを使用して暗号化／復号化される（４１０）。メモリと暗号化されたページング・ファイルの間でデータを移動するプロセスについては、図５に関連して詳述する。
【００３０】
図５は、暗号化されたデータをページング・ファイルに格納するプロセスを示している。システム稼働中の特定の時点で、メモリに格納されたデータをディスクに移動する必要があると（たとえば、メモリ領域を解放するために）メモリ・マネージャが決断する。次に、メモリ・マネージャはメモリ・ページのコンテンツをファイル・システムに渡し、このコンテンツをページング・ファイルに書き込むように命令する（５０２）。ここで、ファイル・システムはページング・ファイルの暗号化フラグがセットされているかどうかを確認する（５０４）。暗号化フラグがセットされていない場合は、メモリ・マネージャが提供するデータはクリア・テキストとしてページング・ファイルに書き込まれる（５０６

）。

【００３１】

ページング・ファイルの暗号化フラグがセットされている場合は、ファイル・システムが暗号化コンポーネントを呼び出してデータを暗号化する（５０８）。ここで、暗号化コンポーネントはセッション・キーを使用してデータを暗号化し（５１０）、暗号文を生成する。さらに、暗号文がファイル・システムに返され（５１２）、ファイル・システムはこの暗号文をページング・ファイルに格納する（５１４）。使用可能な対称の暗号化アルゴリズム（たとえば、ＤＥＳ、３ＤＥＳ、ＡＥＳなど）は通常は特定のサイズのブロックとしてデータを暗号化するブロック暗号なので、生成される（ページング・ファイルに書き込まれる）暗号文のサイズは、暗号化アルゴリズムで使用するブロックのサイズ以上である。

【００３２】

暗号化されたページング・ファイルからデータを取得するプロセスは、図５で説明した格納のプロセスに類似している。ページング・ファイルからデータを取得するようにというメモリ・マネージャからの要求を受け取った場合に、ページング・ファイルに暗号化するためのマークが付けられていると、ファイル・システムはページング・ファイルに格納された暗号文を暗号化コンポーネントに渡し、暗号化コンポーネントはセッション・キーを使用してこれを復号化し、クリア・テキストを返す。このプロセス実行するシステムの例を図６に示す。メモリ内の特定のページにアクセスするようにという要求を受け取ると、メモリ・マネージャは要求されたページがメモリ内に存在しないことを（ページ・マップに基づいて）確認する。ページが存在しないとページ・フォルトが発生する。フォルト・ハンドラは、要求されたページをページング・ファイルから取得するためにファイル・アクセス要求を作成する。ファイル・システム２０８はこのアクセス要求を受取、ページング・ファイルに暗号化するためのマークが付けられていることを確認する。こうして、ファイル・システム２０８は暗号化コンポーネント３０４に対してセッション・キーを使用して要求されたページを復号化するように指示する。ここで、暗号化コンポーネント３０４は復号化されたページをファイル・システムに渡し、ファイル・システムは復号化されたページをメモリ・マネージャ６０２に返す。ここで、メモリ・マネージャ６０２は取得したページのコンテンツを物理メモリ・ページのフレームに書き込み、さらに物理メモリ内にこのページが存在すること（および新しいロケーション）を反映するようにページ・マップを調整する。ページング・ファイルのデータを暗号化および復号化するプロセスは、メモリ・マネージャには透過的（transparent）であり、メモリ・マネージャは、データが暗号化されるかどうかに関係なく、データの格納および取得の要求を作成できるのが好ましい。

【００３３】

以上の例は単に説明のためだけに示されており、本発明に関する限定と理解してはならないことに留意されたい。本発明をさまざまな実施形態に関連して説明してきたが、ここに記載したコンテンツは説明を目的としており、限定を意図しないことは言うまでもない。さらに、本発明を特定の手段、機材（materials）、および実施形態に関連して説明してきたが、本発明をここに開示する仕様に限定する意図はない。本発明は、特許請求の範囲に示す、機能上同等のあらゆる構造、方法、使い方に拡張される。この明細書に記載する技術を利用する当業者は、これにさまざまな変更を加えることができる。こうした変更は、本発明の機能において本発明の範囲と精神を逸脱することなく実施できる。

【図面の簡単な説明】

【００３４】

【図１】本発明の機能を実現できる例示的なコンピューティング環境を示すブロック図である。

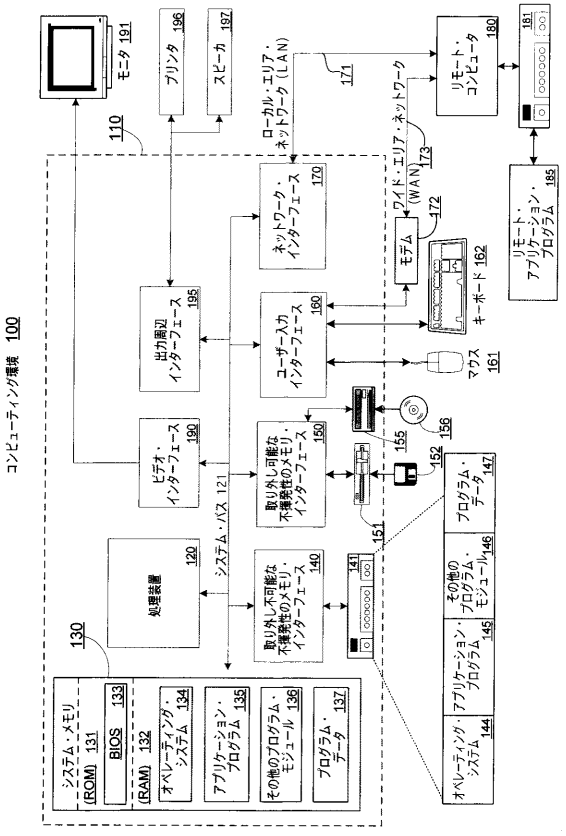
【図２】コンピュータのメモリとそのファイル・システムとの関係を示すブロック図である。

【図３】ファイルを暗号化するメカニズムを示すブロック図である。

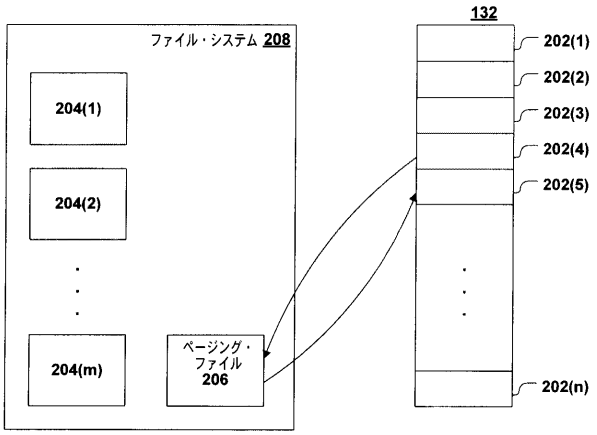
【図４】ページング・ファイルを暗号化するようにシステムを準備するプロセスを示す流れ図である。
【図５】ページング・ファイルに格納するメモリ・データを暗号化するプロセスを示す流れ図である。
【図６】暗号化されたページング・ファイルからページを取得するメモリ・マネージャを示すブロック図である。
【符号の説明】
【００３５】
１００　コンピューティング環境
１２０　処理装置
１２１　システム・バス
１３０　システム・メモリ
１３１　ＲＯＭ
１３２　ＲＡＭ
１３３　ＢＩＯＳ
１３４　オペレーティング・システム
１３５　アプリケーション・プログラム
１３６　その他のプログラム・モジュール
１３７　プログラム・データ
１４０　取り外し不可能な不揮発性のメモリ・インターフェース
１４１　ハードディスク・ドライブ
１４４　オペレーティング・システム
１４５　アプリケーション・プログラム
１４６　その他のプログラム・モジュール
１４７　プログラム・データ
１５０　取り外し可能な不揮発性のメモリ・インターフェース
１５１　磁気ディスク・ドライブ
１５２　取り外し可能な不揮発性の磁気ディスク
１５５　光ディスク・ドライブ
１５６　取り外し可能な不揮発性の光ディスク
１６０　ユーザー入力インターフェース
１６１　マウス
１６２　キーボード１７０　ネットワーク・インターフェース
１７１　ローカル・エリア・ネットワーク（ＬＡＮ）
１７２　モデム
１７３　ワイド・エリア・ネットワーク（ＷＡＮ）
１８０　リモート・コンピュータ
１８１　メモリ・デバイス
１８５　リモート・アプリケーション・プログラム
１９０　ビデオ・インターフェース
１９１　モニタ
１９５　出力周辺インターフェース
１９６　プリンタ
１９７　スピーカ
２０６　ページング・ファイル
２０８　ファイル・システム
３０２　キー
３０４　暗号化コンポーネント
３０６　クリア・テキスト（平文）
３０８　暗号文

６０２　メモリ・マネージャ

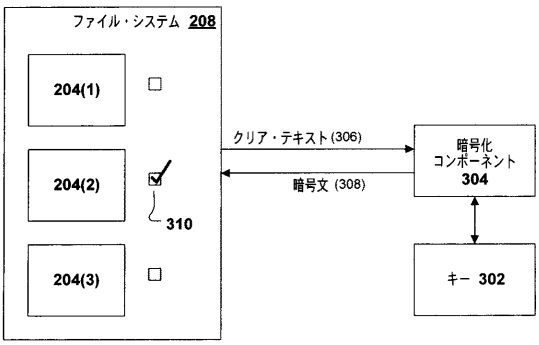
【図１】



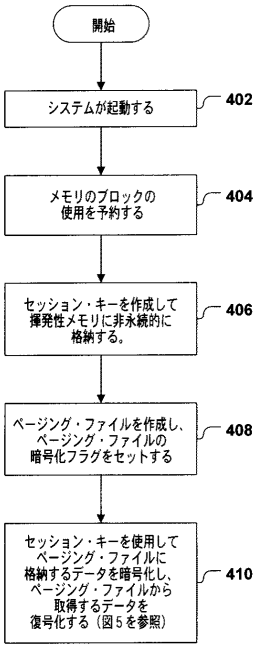
【図２】



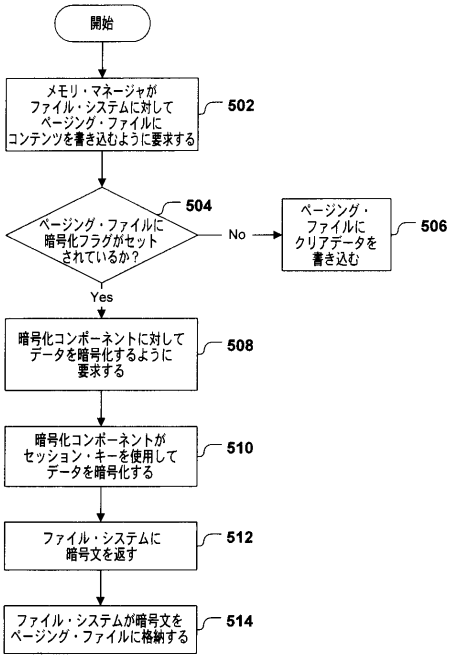
【図３】



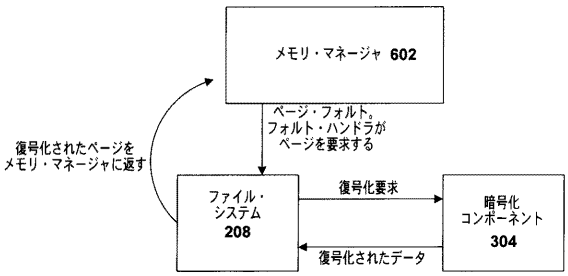
【図４】


開始
システムが起動する
402
メモリのブロックの
使用を予約する
404
セッション・キーを作成して
揮発性メモリに非永続的に
格納する。
406
ページング・ファイルを作成し、
ページング・ファイルの
暗号化フラグをセットする
408
セッション・キーを使用して
ページング・ファイルに
格納するデータを暗号化し、
ページング・ファイルから
取得するデータを
復号化する（図５を参照）
410

【図５】


開始
メモリ・マネージャが
ファイル・システムに対して
ページング・ファイルに
コンテンツを書き込むように要求する
502
ページング・ファイルに
暗号化フラグがセット
されているか？
504
No
ページング・
ファイルに
クリアデータを
書き込む
506
Yes
暗号化コンポーネントに対して
データを暗号化するように
要求する
508
暗号化コンポーネントが
セッション・キーを使用して
データを暗号化する
510
ファイル・システムに
暗号文を返す
512
ファイル・システムが暗号文を
ページング・ファイルに格納する
514

【図６】


メモリ・マネージャ 602
ページ・フォルト、
フォルト・ハンドラが
ページを要求する
復号化されたページを
メモリ・マネージャに返す
ファイル・
システム
208
復号化要求
復号化されたデータ
暗号化
コンポーネント
304

フロントページの続き

(72)発明者　デビッド　ビー．クロス
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　ダンカン　ジー．ブライス
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　ジャンロン　グ
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　ラジーブ　ワイ．ナガル
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　スコット　エー．フィールド
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

Ｆターム(参考) 5B017 AA03 BA02 BA07 BB08 CA07
5B082 EA11 GA11
5J104 AA12 AA16 AA34 EA04 EA15 JA03 NA02 NA27 NA37 PA14