(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5489201号
(P5489201)
(45)発行日　平成26年5月14日(2014.5.14)　(24)登録日　平成26年3月7日(2014.3.7)

(51)Int.Cl.　　F I
G06F 3/06 (2006.01)　　G06F 3/06 304H
G06F 12/14 (2006.01)　　G06F 12/14 510D

請求項の数 9　外国語出願　(全 14 頁)

(21)出願番号　特願2009-21400(P2009-21400)
(22)出願日　平成21年2月2日(2009.2.2)
(65)公開番号　特開2009-187547(P2009-187547A)
(43)公開日　平成21年8月20日(2009.8.20)
審査請求日　平成24年2月1日(2012.2.1)
(31)優先権主張番号　12/012,261
(32)優先日　平成20年2月1日(2008.2.1)
(33)優先権主張国　米国(US)

(73)特許権者　500373758
シーゲイト　テクノロジー　エルエルシー
アメリカ合衆国、９５０１４　カリフォルニア州、クパチーノ、サウス・デ・アンザ・ブールバード、１０２００
(74)代理人　100064746
弁理士　深見　久郎
(74)代理人　100085132
弁理士　森田　俊雄
(74)代理人　100083703
弁理士　仲村　義平
(74)代理人　100096781
弁理士　堀井　豊
(74)代理人　100109162
弁理士　酒井　將行

最終頁に続く

(54)【発明の名称】安全な直接プラッタ・アクセス

(57)【特許請求の範囲】
【請求項１】
装置であって、
データ記憶のためのユーザ領域に加えて保護領域を定義するデータ記憶媒体と、
前記保護領域内に定義されるサブ領域とを備え、前記ユーザ領域を読取るかまたは前記ユーザ領域に書込むというコマンドがある場合にデータが前記保護領域内に一時的に記憶され、前記装置はさらに、
コントローラを備え、前記コントローラは、
前記ユーザ領域を読取るかまたは前記ユーザ領域に書込むというコマンドを実行するようにとの要求をホスト・システムから受信し、前記要求は、少なくとも１つの論理ブロック・アドレス（ＬＢＡ）を含み、前記コントローラは、さらに、
前記少なくとも１つのＬＢＡが前記保護領域のサブ領域内にある場合に前記コマンドを実行する、装置。
【請求項２】
前記データ記憶媒体が通信可能に接続されているホスト装置のオペレーティング・システムの動作中、ユーザは前記保護領域にアクセスできない、請求項１に記載の装置。
【請求項３】
前記データ記憶媒体は、磁気記憶媒体を有するディスク・ドライブを含み、前記磁気記憶媒体は、前記ユーザ領域と、ＰＡＲＴＩＥＳ（Protected Area Run Time Interface Extension Services）領域と、ＬＢＡを用いることなくアドレス指定可能な隠れシス

テム領域とを含み、前記ＰＡＲＴＩＥＳ領域の読み取りまたは書き込みは、オペレーティングシステムに依存することなく行なわれ、前記保護領域は、前記磁気記憶媒体上の前記隠れシステム領域と前記ＰＡＲＴＩＥＳ領域との少なくとも１つにある、請求項１に記載の装置。

【請求項４】

前記データ記憶媒体は、磁気記憶媒体を有するディスク・ドライブを含み、前記保護領域は、ソフトウエアまたはファームウエアによりアクセス可能な前記磁気記憶媒体上にホスト保護領域を含む、請求項１に記載の装置。

【請求項５】

前記ユーザ領域に対するデータの読取りおよび書込み操作のために、データおよびコマンドは前記サブ領域内で一時的に記憶される、請求項１に記載の装置。

【請求項６】

前記データ記憶媒体は、前記保護領域をその上に含む磁気記憶媒体を有するディスク・ドライブを備え、また前記サブ領域は前記保護領域内のＬＢＡ値の或る範囲により定義され、また前記サブ領域はＬＢＡ値を用いてアドレス指定することによりアクセスされる、請求項５に記載の装置。

【請求項７】

前記サブ領域は、前記データ記憶媒体のユーザ領域と前記ホスト・システムとの間の一時的なデータ・バッファのために確保され、前記サブ領域の読取りまたは書き込みは、オペレーティングシステムに依存することなく行なわれる、請求項１に記載の装置。

【請求項８】

データ処理システムであって、

請求項１から７のいずれかに記載の装置を含むデータ記憶装置と、

前記データ記憶装置に電気的に接続されたホスト・システムとを備え、前記ホスト・システムは、プロセッサおよびオペレーティング・システムを含み、前記プロセッサは、前記データ記憶装置との間で、読取りおよび書込みのためにデータを転送する、データ処理システム。

【請求項９】

前記ホスト・システムのオペレーティング・システムの動作中、ユーザによる前記保護領域へのアクセスを不能にする、請求項８に記載のデータ処理システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は磁気記憶装置に関するものであって、より詳しくは、磁気ディスク・ドライブへのまた磁気ディスク・ドライブからのデータの安全な大量転送に関するものである。

【背景技術】

【０００２】

従来のディスク・ドライブ内の磁気記憶媒体は複数の記憶領域に分割されることがある。これらの記憶領域の１つはユーザ領域と呼ばれ、コンピュータ・ユーザの通常の記憶用として確保される。通常、高度技術アタッチメント（ＡＴＡ）または小型コンピュータ・システム・インターフェース（ＳＣＳＩ）などの標準インターフェースを介して、また論理ブロック・アドレス（ＬＢＡ）などのアドレス指定方式を用いて、ユーザはホスト装置のオペレーティング・システムによりこのユーザ領域に自由にアクセスすることができる。ユーザのアクセスを制御する必要があるときは、パスワード保護を用いてユーザ領域への読取りおよび／または書込み操作を可能または不能にすることが多い。

【０００３】

しかし、ユーザ領域への読取りおよび／または書込みアクセスの許可だけでは安全保護を十分に行うことはできない。なぜなら、伝送されるデータについては完全性の検証または起点の認証が行われないからである。また、パスワードで可能になる読取り／書込み許可の範囲は広すぎることが多い。なぜなら、許可は全ユーザ領域またはそのパーティショ

ンに対して行うのが普通だからである。個別のデータ・ブロックに適用される特定の許可プロトコルが提案されてはいるが、この方法はブロック転送を行う度に許可または認証をテストするので読取り／書込み操作の速度が遅くなる。特に、この操作が比較的大きなデータ・ファイルを扱う場合に遅くなる。

【０００４】

同じディスク・ドライブの中に、ディスク・ドライブのメーカが作成した、隠れシステム領域と呼ばれる別の記憶領域が含まれることもある。通常の動作中は、この記憶領域はユーザに見えないしまたユーザはアクセスすることができない。通常、隠れシステム領域は１メガバイトより小さな固定のサイズであり、ディスク・ドライブのファームウエアなどのシステム・データを入れるのに用いられる。

【発明の概要】

【発明が解決しようとする課題】

【０００５】

磁気記憶媒体に加えて、従来のディスク・ドライブはホスト・システム（例えば、サーバ）内の揮発性ＲＡＭの形の一時データ・バッファを用いる。このＲＡＭバッファを用いて、読取りデータおよび書込みデータをキャッシュしてキャッシュ・データの検証および認証を行う。データを揮発性ＲＡＭバッファにキャッシュすることの欠点は、データ・バッファにとってデータ集合が大きすぎる場合があることである。この方法では正味のデータ・サイズを人為的に制限する。サイズの制限というこの問題を解決する１つの方法は揮発性ＲＡＭバッファのサイズを大きくすることである。しかし揮発性ＲＡＭバッファ・メモリは比較的高価なメモリ・チップを用いることが多い。したがって、バッファ・サイズを大きくするためにメモリ・チップの数を増やすとディスク・ドライブのコストが高くなる。

【０００６】

別の方法は、記憶媒体上に特殊なバッファ記憶領域を作成して、一時的に記憶されたデータにデータ検証および認証を行うことである。残念ながら、特殊なバッファ記憶領域を作成し、管理し、保護するにはオペレーティング・システムのかなりの資源を必要とする。１つの記憶位置からネットワーク結合記憶（ＮＡＳ）装置などの別の記憶位置へのデータの大量転送を処理するときは、従来技術の上述の欠点は更に大きくなる。この場合、高速の広帯域データ転送は宛先ドライブまたは発信ドライブでデータを扱うときに「最終の」ボトルネックに会う。

【０００７】

したがって、オペレーティング・システム資源をできるだけ使わずに高速でデータ検証および認証を行って大量データ転送を可能にする磁気ディスク・ドライブ装置および方法が必要である。

【課題を解決するための手段】

【０００８】

本発明は磁気ディスク・ドライブなどのデータ記憶装置が大量のデータ転送を行なうためのシステムおよびプロセスに関するものである。このシステムは高速の読取り／書込み操作を用いて記憶装置上の永続的な、保護された、すなわち安全な記憶領域にアクセスして、データ記憶装置上の通常のユーザ・データ記憶領域（すなわち、終点記憶用）との間で読取りまたは書込みを行うデータを緩衝しまたは一時的に記憶する。この新しいプロセスはその読取り／書込み操作を行うのにオペレーティング・システムに依存しない。したがってこの新しいプロセスにより、一時記憶領域に関する読取り／書込み操作はコマンド・ペイロードの制限を回避すると共に、データおよびコマンドの検証コストを減らすことができる。

【０００９】

１つの態様では、本発明では磁気ディスク・ドライブ内に定義された保護された、すなわち安全な領域に対して直接プラッタ・アクセスを行う。本発明の１つの実施の形態は保護領域ランタイム・インターフェース拡張サービス（ＰＡＲＴＩＥＳ）技術と呼ばれる既

存の機構を操作して、ＰＡＲＴＩＥＳ領域と呼ばれる安全な記憶領域内に安全な記憶サブ領域を作成して編成する。この新しいプロセスは安全なサブ領域との間の大きなデータ・ファイルの転送を支援しまたデータの正当性および機密性を保証することができるので、本発明はかかる安全なサブ領域を読取り／書込み操作のためのデータ・バッファとして有効に用いることができる。この新しい安全なサブ領域はオペレーティング・システムにより編成および保護が行われないので、ウイルスすなわちトロイの木馬ソフトウエア（オペレーティング・システムを不当に操る能力が大きいほど有害である）による攻撃から本質的に保護される。また本発明のプロセスにより、読取り／書込み操作はコマンド・ペイロードの制限を回避すると共に、データおよびコマンドの検証コストを減らすことができる。なぜなら、読取り／書込み操作を行うのにオペレーティング・システムに依存しないからである。

【図面の簡単な説明】

【００１０】

本発明の性質および利点ならびに好ましい使用モードを完全に理解するため、添付の図面と共に以下の詳細な説明を参照していただきたい。以下の図面では、全図面を通して同じ参照番号は同じまたは同様の部分を指す。

【図１】本発明に係る大量データ転送方式を用いるネットワーク・サーバおよび計算装置の略図である。

【図２】本発明の原理に係る大量データ転送方式を用いることができるディスク・ドライブを示す。

【図３】ＰＡＲＴＩＥＳ技術を用いて作成されまた編成された、安全なＰＡＲＴＩＥＳ領域を有する磁気ディスク・ドライブの記憶領域レイアウトを示す。

【図４】ＰＡＲＴＩＥＳ技術を用いて作成されまた編成された、ＰＡＲＴＩＥＳ領域内に安全なサブ領域を有する磁気ディスク・ドライブの記憶領域レイアウトを示す。

【図５】ＰＡＲＴＩＥＳ技術を用いて作成されまた編成された、隠れシステム領域内に安全なサブ領域を有する磁気ディスク・ドライブの記憶領域レイアウトを示す。

【図６】ＰＡＲＴＩＥＳ技術を用いて作成された磁気ディスク・ドライブ上の安全なサブ領域に読取りコマンドを出すことを可能にする、本発明の１つの実施の形態に係るプロセスを示す流れ図である。

【図７】ＰＡＲＴＩＥＳ技術を用いて作成された磁気ディスク・ドライブ上の安全なサブ領域に書込みコマンドを出すことを可能にする、本発明の１つの実施の形態に係るプロセスを示す流れ図である。

【図８】或る一般コマンドを１つ以上のＬＢＡとしてディスク・ドライブに運びまた或る状態を１つ以上のＬＢＡとして返すことを可能にする、本発明の１つの実施の形態に係るプロセスを示す流れ図である。

【発明を実施するための形態】

【００１１】

ここに説明するのは本発明を実行するのに現在最も良いと考えられるモードである。この説明は本発明の一般原理を示すために行うものであって、制限するものと考えてはならない。本発明の範囲は添付の特許請求の範囲を参照して決めるのが最も良い。ここでは本発明について種々の実施の形態および図面を参照して説明する。当業者が認識するように、本発明の範囲および精神から逸れない限り、かかる教示を参照して種々の変更および改善を行うことができる。

【００１２】

１つの態様では、本発明は磁気ディスク・ドライブなどのデータ記憶装置が大量のデータ転送を行なうためのシステムおよびプロセスに関するものである。このシステムは、高速の読取り／書込み操作を用いて記憶媒体上の永続的で安全な一時記憶領域にアクセスして、記憶媒体上の通常のユーザ・データ記憶領域（すなわち、終点データ記憶用）との間で読取りまたは書込みを行うときにデータを緩衝しまたは一時的に記憶する。この新しいプロセスは一時記憶領域に関して読取り／書込み操作を行うのにオペレーティング・シス

テムに依存しない。したがってこの新しいプロセスにより、読取り／書込み操作はコマンド・ペイロードの制限を回避すると共に、データおよびコマンドの検証コストを減らすことができる。

【００１３】

磁気ディスク・ドライブでは、本発明はＰＡＲＴＩＥＳ技術と呼ばれる既存の機構を操作して、安全な記憶領域を作成して編成する。ＰＡＲＴＩＥＳ技術は、コンピュータ装置のハード・ディスク・ドライブ上の別の保護領域を管理するために設けられるホスト保護領域機能を利用する。この技術は、ＮＣＩＴＳ３４６、ＡＮＳＩ　ＮＣＩＴＳ３０６（ＳＣＳＩ－３ブロック・コマンド）、およびＡＮＳＩ　ＮＣＩＴＳ３４０（ＡＴＡＰＩ－５）などの明細書に記載されている。ＰＡＲＴＩＥＳおよびＡＴＡ／ＡＴＡＰＩ－５標準は、ハード・ドライブの或る領域を編成して通常のシステム運転中にユーザのアクセスを不能にするよう規定する。この記憶領域はＰＡＲＴＩＥＳ領域と呼ばれ、通常、記憶媒体の末端にあり、ブート・エンジニアリング拡張記録（ＢＥＥＲ）を介して複数のサービス領域に分割される。これらの個々のサービス領域を用いて、緊急ブート位置を与えるなどの特定の機能およびその他の診断サービスを支援することができる。

【００１４】

ＰＡＲＴＩＥＳ技術は性質の異なる４つのソフトウエア層を含む。第１の層はハード・ドライブ上にＰＡＲＴＩＥＳ領域が存在するのを検出するもので、発見層と呼ばれる。第２の層はフェールセーフ・ブート・サービスを選択するためのもので、ブート選択層と呼ばれる。第３の層はフェールセーフ・ブート・サービスを選択するときにハード・ドライブ上の予約された領域からシミュレートされたドライブＡを与えるもので、シミュレーション層と呼ばれる。第４の層は他のＰＡＲＴＩＥＳサービスを作成し、アクセスし、削除するためのもので、操作層と呼ばれる。これらの層は、ＰＡＲＴＩＥＳサービスを書式化しまた発見するための特定の詳細を与えるＡＮＳＩ　ＰＡＲＴＩＥＳ明細書に規定されている。

【００１５】

通常の操作中にＰＡＲＴＩＥＳサービスを操作してＰＡＲＴＩＥＳ領域へのアクセスを可能にするいくつかの周知の方法がある。第１の方法は、ＰＡＲＴＩＥＳサービスの追加および削除に加えて、ＤＯＳベースのプログラムなどのアプリケーションを用いてホスト保護領域を初期化することである。別の方法は、ＳＥＴＵＰ中またはランタイム中に、ホスト装置の基本入出力システム（ＢＩＯＳ）などのファームウエアを操作することである。例えば、ＢＩＯＳを操作してＰＡＲＴＩＥＳ領域へのアクセスを可能にする１つの方法は、オペレーティング・システムを立ち上げる前にＢＩＯＳがＳＥＴ　ＭＡＸＩＭＵＭロック・コマンドを出さないようにすることである。別の方法は、ＳＥＴ　ＭＡＸＩＭＵＭ　ＵＮＬＯＣＫコマンドを正式に出して、通常はシステム用として確保されている記憶領域へのアクセスを可能にすることである。

【００１６】

制限するためではなく例示として、サーバと磁気ディスク・ドライブ（特に、データの認証および検証のプロセスを扱うオンボード・プロセッサまたはコントローラを有するディスク・ドライブ装置）との間の新しい大量データ転送方法を含むネットワーク記憶サーバに関して本発明を説明する。認識されるように、１台以上の汎用またはアプリケーション専用のプロセッサ、コントローラ・カード、またはコンピュータなどの情報処理装置で本発明のプロセスを支援して、安全なサブ領域の作成および編成を行いまた本発明の原理に係る大量データの転送を容易にすることもできる。

【実施例】

【００１７】

図１は、本発明に係る大量データ転送方式を用いることのできるネットワーク・サーバ４０または計算装置４２の一例のブロック図である。サーバ４０または計算装置４２は、プロセッサ４４、揮発性メモリ・ユニット４６、不揮発性メモリ・ユニット４８、および大容量記憶装置５０を備える。プロセッサ４４は、システム・メモリとして動作する揮発

性メモリ・ユニット４６に結合する。揮発性メモリ・ユニット４６の一例はダイナミック・ランダム・アクセス・メモリ（ＤＲＡＭ）である。プロセッサ４４は、システム・ファームウエアなどの初期の命令セットを保持するのに用いられる不揮発性メモリ・ユニット４８にも結合する。プロセッサ４４は、データ・ファイルおよびオペレーティング・システムなどの命令セットを記憶するのに用いることができる大容量記憶装置５０にも結合する。

【００１８】

大容量記憶装置５０は任意のタイプの、または種々のタイプを組み合わせた、磁気ディスク・ドライブ、コンパクト・ディスク（ＣＤ）ドライブ、ディジタル・ビデオ・ディスク（ＤＶＤ）ドライブ、フロッピー（登録商標）・ディスク・ドライブ、ジップ・ドライブ、ＳｕｐｅｒＤｉｓｋドライブ、光磁気ディスク・ドライブ、ジャズ・ドライブ、高密度フロッピー（登録商標）・ディスク（ＨｉＦＤ）ドライブ、フラッシュ・メモリ、読取り専用メモリ（ＲＯＭ）、プログラム可能読取り専用メモリ（ＰＲＯＭ）、消去可能プログラム可能読取り専用メモリ（ＥＰＲＯＭ）、または電気的消去可能プログラム可能読取り専用メモリ（ＥＥＰＲＯＭ）などでよい。

【００１９】

サーバ４０または計算装置４２は、情報をユーザに表示するフラット・パネル・モニタなどのビデオ出力装置５２と、ユーザからの入力を受けるキーボードまたはタブレットなどの入力装置５４も含んでよい。サーバ４０または計算装置４２は、有線（例えば、銅線または光ファイバ）接続および／または無線接続を用いるネットワーク５６を介して互いに接続してよい。本発明の範囲から逸れない限り、サーバ４０または計算装置４２は、それぞれが異なる物理的位置に常駐してネットワーク５６を介して相互接続される、複数のプロセッサ４４、揮発性メモリ・ユニット４６、不揮発性メモリ・ユニット４８、および大容量記憶装置５０を含んでもよい。当業者が認識するように、本発明のプロセスは、コントローラ・カード（図示せず）または大容量記憶装置５０上に常駐するプロセッサが部分的にまたは全体的に処理して、安全なサブ領域の作成、編成、および／または安全保護を行ってもよい。

【００２０】

図２は本発明に係る大量データ転送方式を実現するのに用いることができるディスク・ドライブ１０の一例である。ディスク・ドライブ１０は、ディスク・ドライブの種々の構成要素が入る大きさおよび構成のハウジング１２（この図では上部を取り除いて下部が見えるようにした）を含む。ディスク・ドライブ１０は、ハウジング内の少なくとも１個の磁気記憶媒体１６を回転させるスピンドル・モータ１４を含む。ハウジング１２内には少なくとも１本のアーム１８を有するサスペンション組立体があり、各アーム１８は、スライダ２２上に支持された記録ヘッドの形の変換器を有する第１の端部２０と、軸受２６により軸上に旋回可能に取り付けられた第２の端部２４とを有する。アクチュエータ・モータ２８はアームの第２の端部２４にあり、アーム１８を旋回させて、記録ヘッド２２をディスク１６の所望のセクタまたはトラック上に位置決めする。アクチュエータ・モータ２８および他の構成要素はコントローラ３０により制御され、これらを以下の開示に係る大量データ転送方式に組み入れてもよい。

【００２１】

図３は安全なＰＡＲＴＩＥＳ領域を含むディスク・ドライブ内のＬＢＡ範囲を示す。図３はＰＡＲＴＩＥＳ可能ディスク・ドライブの３つの主記憶領域を示す。すなわち、ユーザ領域（通常の、すなわち終点（ｅｎｄｐｏｉｎｔ）のデータ記憶用）、隠れシステム領域、およびＰＡＲＴＩＥＳ領域である。記憶ブロックはそのＬＢＡ値に従って編成してアドレス指定することができる。これらの３つの記憶領域のＬＢＡ範囲は以下の規定を用いてよい。ユーザ領域では、ＬＢＡはゼロからＵＳＥＲ＿ＭＡＸＩＭＵＭと呼ばれる値までの範囲にわたってよい。ただし、ＵＳＥＲ＿ＭＡＸＩＭＵＭはＳＥＴ　ＭＡＸＩＭＵＭコマンドにより設定される値で、この装置がユーザ記憶に利用できる最大ＬＢＡ値である。ＰＡＲＴＩＥＳ領域内では、ＬＢＡはＰＡＲＴＩＥＳ＿ＭＩＮＩＭＵＭと呼ばれる最小値

からＰＡＲＴＩＥＳ＿ＭＡＸＩＭＵＭと呼ばれる最大値までの範囲にわたる。ただし、ＰＡＲＴＩＥＳ＿ＭＩＮＩＭＵＭはＡＴＡを介してホストのオペレーティング・システムに示される指定されたドライブ・サイズより一般に１だけ大きい。

【００２２】

図４は、ＰＡＲＴＩＥＳ機構を用いてＰＡＲＴＩＥＳ領域内のサブ領域を編成して保護する或る実施の形態を示す。ＰＡＲＴＩＥＳ技術を用いてＰＡＲＴＩＥＳ領域内に安全なサブ領域を確保して、ホスト装置とディスク・ドライブとの間の大量データ転送を容易にすることができる。この大量転送プロセスは直接プラッタ・アクセス（ＤＰＡ）と呼ばれており、安全なサブ領域はＤＰＡ領域と呼ばれることがある。ＤＰＡ領域に用いられるＬＢＡはユーザ領域用として確保されたＬＢＡ範囲より上に設定され、ＤＰＡ＿ＭＩＮＩＭＵＭと呼ばれる最小値からＤＰＡ＿ＭＡＸＩＭＵＭと呼ばれる最大値までの範囲にわたる。ＰＡＲＴＩＥＳ技術を用いると、ディスク・ドライブはＤＰＡ＿ＭＩＮＩＭＵＭとＤＰＡ＿ＭＡＸＩＭＵＭとにより設定される範囲内にあるＬＢＡへの問合せに対応することができる。

【００２３】

図５は、ＰＡＲＴＩＥＳ領域外（例えば、隠れシステム領域内）にサブ領域を編成して保護する別の実施の形態を示す。隠れシステム領域は、通常、記憶ブロックをアドレス指定するのにＬＢＡを用いない。しかし、隠れシステム領域内の物理的記憶位置を参照するためにＬＢＡの或る範囲を確保することができる標準機構がある。大量データ転送専用に或るＬＢＡ範囲を確保すると、ドライブはこのＬＢＡアドレスが隠れシステム領域に関するものと解釈しなければならない。またはコマンドおよび／またはコマンド・パラメータは目標領域が隠れシステム領域内にあると指定しなければならない。この安全なサブ領域はＤＰＡ領域と呼ばれ、そのＬＢＡ範囲は、ユーザ領域およびＰＡＲＴＩＥＳ領域の両方のＬＢＡ範囲と矛盾しない。ＤＰＡ領域のＬＢＡは、ＤＰＡ＿ＭＩＮＩＭＵＭと呼ばれる最小値からＤＰＡ＿ＭＡＸＩＭＵＭと呼ばれる最大値までの範囲にわたってよい。ＰＡＲＴＩＥＳ技術を用いると、ディスク・ドライブはＤＰＡ＿ＭＩＮＩＭＵＭとＤＰＡ＿ＭＡＸＩＭＵＭとにより設定される範囲内にあるＬＢＡへの問合せに対応することができる。

【００２４】

本発明は、ＰＡＲＴＩＥＳ領域を開くことまたはＤＰＡ処理のために記憶領域内にサブ領域を作成することをシステム・ファームウエアに要求する、このプロセスにより実現されるプログラミング・インターフェースを提供する。保護されたサブ領域が編成されてアクセスされれば、ユーザは種々のコマンドを出してサブ領域内で種々のタスクを実行することができる。例えばユーザは、安全なサブ領域へのまたサブ領域からの大量のデータ転送を可能にするコマンドを出してよい。また別のコマンドを出してデータに操作を行ってもよいし、またはトランザクション機能性などの追加のセマンティクスを提供してもよい。暗号化が必要な場合はデータを暗号化してよく、その暗号キーはＡＥＳ（高度暗号化標準）ガイドラインに係る周知のプロセスにより選択してよい。

【００２５】

メッセージのデータ完全性は認証アルゴリズムおよび認証キーを用いて保証することができる。この認証アルゴリズムはメッセージおよび認証キーを入力として受けて認証値を計算する。この認証値は短いビット・ストリングであって、その値は認証アルゴリズム、メッセージ、およびキーにより決まる。かかる認証アルゴリズムの一例はキー付きハッシュ関数ＨＭＡＣ－ＳＨＡ１である。その他の暗号化および認証アルゴリズムは当業者に明らかであろう。

【００２６】

ホスト装置とディスク・ドライブとの間で暗号キーおよび認証キーを交換するには、ディフィー・ヘルマン（Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ，ＤＨ）方式などの公開鍵一致方式を用いればよい。ＤＨ方式は元のキー値に基づいて公開参照番号を計算して送信する。公開参照番号を受け取ると、周知のプロセスを用いて元のキーを確実に得ることができる。

【００２７】

図６は、ＰＡＲＴＩＥＳ技術を用いてＰＡＲＴＩＥＳ領域内に作成された保護サブ領域への読取り操作のための流れ図を示す。このプロセスの第１のステップは、ＨＭＡＣ－ＳＨＡ１アルゴリズムなどのキー付きハッシュ関数およびディフィー・ヘルマン（ＤＨ）キー一致方式などの公開鍵暗号化システムを用いる認証方式を実現するよう要求する。ＨＭＡＣ－ＳＨＡ１アルゴリズムを用いて、秘密認証キーＫａおよび読取りコマンドＣＭＤを用いることにより認証値Ｍを計算する。次に、ＡＥＳなどの暗号化方式および秘密暗号キーＫｅを用いてコマンドＣＭＤを暗号化して、暗号化された読取りコマンドＣＭＤｅを作る。暗号キーへの公開参照番号Ｋｅ＿ｒｅｆおよび認証キーへの公開参照番号Ｋａ＿ｒｅｆはディフィー・ヘルマン・キー一致方式に係る周知のプロセスにより計算する。暗号化された読取りコマンドＣＭＤｅ、目標データ・ブロックのＬＢＡ下限値Ｌ（１）、目標データ・ブロックのＬＢＡ上限値Ｌ（ｎ）、認証キーへの公開参照Ｋａ＿ｒｅｆ、暗号キーへの公開参照Ｋｅ＿ｒｅｆ、および認証値Ｍを要求ＲＥＱとしてディスク・ドライブに送る。

【００２８】

ディスク・ドライブは未検証の要求ＲＥＱを受け取る。ディスク・ドライブはまず、Ｌ（１）およびＬ（ｎ）がＤＰＡ＿ＭＩＮＩＭＵＭおよびＤＰＡ＿ＭＡＸＩＭＵＭにより指定された範囲内にあるかどうかチェックすることにより、送信されたデータを認証しまた検証しなければならない。Ｌ（１）およびＬ（ｎ）がＤＰＡ　ＬＢＡ範囲内にない場合は、プロセスは誤りメッセージを出して読取りプロセスは停止する。Ｌ（１）およびＬ（ｎ）がＤＰＡ　ＬＢＡ範囲内にある場合は、ディスク・ドライブはディフィー・ヘルマン・キー交換方式に従う周知のプロセスを用いて公開参照番号Ｋｅ＿ｒｅｆおよびＫａ＿ｒｅｆからＫｅおよびＫａをそれぞれ得る。次に、プロセスはＡＥＳ解読アルゴリズムおよびＫｅを用いてコマンドＣＭＤを解読する。

【００２９】

次に、ディスク・ドライブは解読されたコマンドＣＭＤおよび認証キーＫａから認証値を計算し、この値と送信された認証値Ｍとを比較して、要求ＲＥＱの正当性を決定する。この２つの値が等しくなくてコマンドの正当性が確認されない場合は、誤りメッセージを出してプロセスは停止する。この２つの値が等しくてコマンドの正当性が確立された場合は、プロセスはコマンドＣＭＤが許容されるコマンドかどうかチェックする。コマンドＣＭＤが許容されない場合は、プロセスは誤りメッセージを出してプロセスは停止する。コマンドＣＭＤが許容される場合は、プロセスはコマンドＣＭＤを実行して、結果をＸ１，．．．，Ｘｎとして出力する。秘密暗号キーＫｅを用いて結果Ｘ１，．．．，Ｘｎを暗号化し、暗号化された結果Ｙ１，．．．，ＹｎをＬＢＡ　Ｌ（１），．．．，Ｌ（ｎ）に書き込む。

【００３０】

プロセスは読取りプロセスの結果をディスク・ドライブからホスト装置に送信する準備をするため、まず、秘密認証キーＫａおよび暗号化されていない結果Ｘ１，．．．，Ｘｎを用いて別の認証値ＭＭを計算する。プロセスは、ディフィー・ヘルマン・キー一致方式に係る周知のプロセスを用いて、公開参照番号Ｋｅ＿ｒｅｆおよびＫａ＿ｒｅｆの新しい集合を生成してよい。次に、プロセスはＬＢＡ下限値Ｌ（１）、ＬＢＡ上限値Ｌ（ｎ）、認証キーへの公開参照Ｋａ＿ｒｅｆ、暗号化キーへの公開参照Ｋｅ＿ｒｅｆ、および認証値ＭＭをホスト装置に送信する。

【００３１】

ホスト装置は未検証の応答ＲＥＳＰを受け取る。　次にプロセスは、Ｌ（１）およびＬ（ｎ）がＤＰＡ　ＬＢＡ範囲内の有効なＬＢＡかどうかチェックする。Ｌ（１）またはＬ（ｎ）が有効なＬＢＡ範囲内にない場合は、誤りメッセージを出してプロセスは停止する。Ｌ（１）およびＬ（ｎ）が共にＤＰＡ　ＬＢＡ範囲内にある場合は、プロセスは先に進んで、ＫｅおよびＫａをＫｅ＿ｒｅｆおよびＫａ＿ｒｅｆからそれぞれ得る。次にホスト装置は暗号化された結果Ｙ１，．．．，ＹｎをＬＢＡ　Ｌ（１），．．．，Ｌ（ｎ）から読み取り、これらを解読して結果Ｘ１，．．．，Ｘｎを作る。次に、ホスト装置は解読さ

れた結果Ｘ１，．．．，Ｘｎおよび秘密認証キーＫａを用いて認証値を計算し、この認証値と送信された認証値ＭＭとを比較する。この２つの値が一致しない場合は正当性が確認されず、プロセスは誤りメッセージを出して読取りプロセスは停止する。正当性が確立された場合は、結果Ｘ１，．．．，Ｘｎをホストに与えて必要に応じて更に処理する。

【００３２】

図７は、ＰＡＲＴＩＥＳ技術により作成された保護サブ領域への書込み操作のための流れ図を示す。このプロセスの第１のステップは、ＨＭＡＣ－ＳＨＡ１アルゴリズムを用いて、秘密認証キーＫａ、書込みコマンドＣＭＤ、およびデータＸ１，．．．，Ｘｎを用いることにより認証値Ｍを計算するよう要求する。ＡＥＳ暗号化および秘密暗号キーＫｅを用いてデータＸ１，．．．，Ｘｎおよび書込みコマンドＣＭＤを暗号化して、暗号文Ｙ１，．．．，Ｙｎおよび暗号化されたコマンドＣＭＤｅをそれぞれ作る。またホスト装置は、ＫｅおよびＫａへの公開参照として用いるために、周知のプロセスを用いてディフィー・ヘルマン番号を生成する。次にプロセスは暗号文Ｙ１，．．．，ＹｎをＬＢＡ　Ｌ（１），．．．，Ｌ（ｎ）に書き込む。暗号化された読取りコマンドＣＭＤｅ、ＬＢＡ下限値Ｌ（１）、ＬＢＡ上限値Ｌ（ｎ）、認証キーへの公開参照Ｋａ＿ｒｅｆ、暗号キーへの公開参照Ｋｅ＿ｒｅｆ、および認証値Ｍを要求ＲＥＱとしてディスク・ドライブに送る。

【００３３】

ディスク・ドライブは未検証の要求ＲＥＱを受け取る。Ｌ（１）およびＬ（ｎ）がＤＰＡ＿ＭＩＮＩＭＵＭおよびＤＰＡ＿ＭＡＸＩＭＵＭにより指定された範囲内にあるかどうかまずチェックすることにより、送信されたデータを認証しまた検証する。それらがＤＰＡ　ＬＢＡ範囲内にない場合は、誤りメッセージを出して読取りプロセスは停止する。それらがＤＰＡ　ＬＢＡ範囲内にある場合は、ディスク・ドライブはＡＥＳ解読アルゴリズムと、Ｋｅ＿ｒｅｆ内のディフィー・ヘルマン番号から得られる該当するＫｅとを用いて、ＣＭＤｅおよびＹ１，．．．，ＹｎからＣＭＤおよびＸ１，．．．，Ｘｎを解読する。

【００３４】

次に、ディスク・ドライブはＣＤＭ、Ｘ１，．．．，Ｘｎ、および認証キーＫａ（これはＫａ＿ｒｅｆ内のディフィー・ヘルマン番号から得られる）を用いて認証値を計算し、この値と送信された認証値Ｍとを比較して、ＣＤＭおよびＸ１，．．．，Ｘｎの正当性を決定する。この２つの値が等しくなくてＣＤＭおよびＸ１，．．．，Ｘｎの正当性が確認されない場合は、誤りメッセージを出してプロセスは停止する。この２つの値が等しくてコマンドおよびＸ１，．．．，Ｘｎの正当性が確立される場合は、プロセスはコマンドＣＭＤが許可されるコマンドであるかどうかチェックする。コマンドＣＭＤが許容されない場合は、プロセスは誤りメッセージを出して書込みプロセスは停止する。コマンドＣＭＤが許容される場合は、プロセスはＸ１，．．．，ＸｎをＬ（１），．．．，Ｌ（ｎ）に書き込む。随意であるが、プロセスはＣＭＤの該当する状態をホスト装置に返す。

【００３５】

別の実施の形態では、一般コマンドＣＭＤおよび／またはその状態を１つ以上のＬＢＡとして運んでよい。図８は、ＰＡＲＴＩＥＳ技術を用いて記憶媒体上に作成された保護サブ領域に一般コマンドを出すことに関する一般的な操作の流れ図を示す。このプロセスの第１のステップは、秘密認証キーＫａ、一般コマンドＣＭＤ、およびクリアテキストＸ１，．．．，Ｘｎを用いて認証値Ｍを計算するようホスト装置に要求する。次に、ＡＥＳ暗号化方式および秘密暗号キーＫｅを用いてクリアテキストＸ１，．．．，ＸｎおよびＣＭＤを暗号化して、暗号化されたデータＹ１，．．．，Ｙｎおよび暗号化された一般コマンドＣＭＤｅを作る。プロセスはＣＭＤｅおよびＹ１，．．．，ＹｎをＬＢＡ　Ｌ（１），．．．，Ｌ（Ｎ）に書き込む。ただし、ＣＭＤｅを記憶するのに追加のデータ・ブロックを用いるので、Ｎはｎに等しいかまたはｎより大きい。次に、プロセスは暗号キーへの公開参照Ｋｅ＿ｒｅｆおよび認証キーへの公開参照Ｋａ＿ｒｅｆとして用いるために公開ディフィー・ヘルマン番号を生成する。ＬＢＡ下限値Ｌ（１）、ＬＢＡ上限値Ｌ（Ｎ）、認証キーへの公開参照Ｋａ＿ｒｅｆ、暗号キーへの公開参照Ｋｅ＿ｒｅｆ、および認証値Ｍを要求ＲＥＱとしてディスク・ドライブに送る。

【００３６】
ディスク・ドライブは未検証の要求ＲＥＱを受け取り、Ｌ（１），．．．，Ｌ（Ｎ）の外部からの変更を防ぐ。次に、Ｌ（１）およびＬ（Ｎ）がＤＰＡ＿ＭＩＮＩＭＵＭおよびＤＰＡ＿ＭＡＸＩＭＵＭにより指定された範囲内にあるかどうかチェックする。それらがＤＰＡ　ＬＢＡ範囲内にない場合は、誤りメッセージを出して読取りプロセスは停止する。それらがＤＰＡ　ＬＢＡ範囲内にある場合は、プロセスはＡＥＳ解読アルゴリズムと、周知のプロセスを用いてＫｅ＿ｒｅｆから得られる暗号キーＫｅとを用いて、Ｌ（１），．．．，Ｌ（Ｎ）からデータＸ１，．．．，ＸｎおよびＣＭＤを探し出して解読する。解読された結果と、周知のプロセスを用いてＫａ＿ｒｅｆから得られる認証キーＫａとを用いて、認証値を計算する。

【００３７】
この認証値と送信された認証値Ｍとを比較して、要求ＲＥＱの正当性を決定する。この２つの値が等しくなくてコマンドの正当性が確認されない場合は、誤りメッセージを出してプロセスは停止する。この２つの値が等しくてコマンドの正当性が確立される場合は、プロセスはコマンドＣＭＤが許容されるコマンドかどうかチェックする。コマンドＣＭＤが許容されない場合は、プロセスは誤りメッセージを出してプロセスは停止する。コマンドＣＭＤが許容される場合は、プロセスはコマンドＣＭＤを実行して、その結果をＸＸ１，．．．，ＸＸｎとして、状態値ＳＴＡＴＵＳと共に出力する。秘密暗号キーＫｅを用いて結果ＸＸ１，．．．，ＸＸｎおよびＳＴＡＴＵＳを暗号化して、暗号化された結果ＹＹ１，．．．，ＹＹｎおよびＳＴＡＴＵＳｅを作り、ＬＢＡ　Ｌ（１），．．．，Ｌ（Ｎ）に書き込む。

【００３８】
このプロセスは一般操作の結果をホスト装置に送る準備をするため、秘密認証キーＫａ、ＸＸ１，．．．，ＸＸｎ、およびＳＴＡＴＵＳを用いて別の認証値ＭＭをまず計算する。次に、ディスク・ドライブはＳＴＡＴＵＳｅ、ＬＢＡ下限値Ｌ（１）、ＬＢＡ上限値Ｌ（Ｎ）、Ｋａ＿ｒｅｆ、Ｋｅ＿ｒｅｆ、およびＭＭをホスト装置に送る。

【００３９】
ホスト装置は未検証の応答ＲＥＳＰを受け取る。次にホスト装置は、Ｌ（１）およびＬ（Ｎ）がＤＰＡ　ＬＢＡ範囲内の有効なＬＢＡかどうかチェックする。Ｌ（１）またはＬ（Ｎ）が有効なＬＢＡ範囲外にある場合は、誤りメッセージを出してプロセスは停止する。Ｌ（１）およびＬ（Ｎ）が共にＤＰＡ　ＬＢＡ範囲内にある場合は、プロセスはＬＢＡ　Ｌ（１），．．．，Ｌ（Ｎ）から暗号化された結果ＹＹ１，．．．，ＹＹｎおよびＳＴＡＴＵＳｅを探し出して解読する。暗号キーへの公開参照Ｋｅ＿ｒｅｆから得られる秘密暗号キーＫｅを用いて、ＹＹ１，．．．，ＹＹｎおよびＳＴＡＴＵＳｅから結果ＸＸ１，．．．，ＸＸｎおよびＳＴＡＴＵＳをそれぞれ解読する。次に、プロセスは解読された結果ＸＸ１，．．．，ＸＸｎ、ＳＴＡＴＵＳ値、およびＫａを用いて認証値を計算する。この認証値とＭＭとを比較して結果を認証する。正当性が確認されない場合は、プロセスは誤りメッセージを出して読取りプロセスは停止する。正当が確立される場合は、ＳＴＡＴＵＳを登録し、ホスト装置は結果ＸＸ１，．．．，ＸＸｎを用いて更にデータ処理を行ってよい。

【００４０】
或る実施の形態では暗号化アルゴリズムと解読アルゴリズムとに同じキーを用いる対称キー・システムを用いるが、当業者が認識するように、本発明は非対称キー・システムを用いてもよいし、秘密キーのファミリを用いてもよいし、または秘密キーのファミリを１個以上のマスタ・キーから得てもよい。また本発明はデータ暗号化標準（ＤＥＳ）またはトリプルＤＥＳなどのＡＥＳ以外の暗号化方式を用いて、暗号文に不確実性を追加してよい。またＨＭＡＣ－ＳＨＡ１以外の、ＨＭＡＣ－ＳＨＡ２５６およびＨＭＡＣ－ＭＤ５などの方式を用いて、完全性を検証しまたデータの起点を認証するのに用いられる認証値を計算してよい。したがって、ディフィー・ヘルマン・キー一致方式以外の公開キー一致方式を用いて、ホストとディスク・ドライブの間で暗号化キーを交換しまたは生成してよい

。例えば、暗号化キーに基づく参照番号を生成して送信するのではなく、このシステムは、ホストおよびディスク・ドライブだけが知っているキー／ＩＤ表に従って正しい暗号化キーを探索するのに用いることができる厳密なリテラル参照（すなわち、キー・ラベル、キーＩＤ）を送信するようにしてよい。

【００４１】

或る実施の形態では認証方式を用いてＤＰＡ領域への問合せの許可または正当性をチェックするが、本発明は保護されないマスタリング・モードのＤＰＡ空間を用いてもよい。この場合ディスク・ドライブは、ＤＰＡ空間が使用中か使用中でないかに関するＬＢＡの範囲についての問合わせに応答する。これらの要求については許可または正当性をチェックするのではなく、使用／不使用フラグをヒントとして用いて、正しく行動したクライアントの間の衝突を防ぐ。この方法は認証なしのマスタリングの形と考えてよい。

【００４２】

コマンドＣＭＤが読取りコマンドまたは書込みコマンドである方式の実施の形態について述べたが、本発明はＩＳＯ－７８１６または他のスマートカードに基づくＡＰＤＵに準拠するコマンドなどの他のコマンドをドライブ終点に出してもよい。ＡＴＡコマンドなどの代替的なコマンドまたは記憶内に常駐する終点で実行するための他の指定された操作を用いる代替的な実施の形態は当業者に明であろう。

【００４３】

認識されるように、本発明を理解するのに、プロセスを構成する各ステップを実際に具体化するための詳細な説明は必要ない。システムの属性、機能性、およびシステム内の種々のソフトウエアおよびハードウエア構成要素の相互関係を開示したので、実際の具体化はプログラマおよびコンピュータ技術者の通常の技術の範囲内にある。当業者が普通の技術を適用すれば、不適当な実験を行わなくても本発明を実行することができる。

【００４４】

本発明を制限するためではなく例示する目的で本発明の特定の実施の形態を説明したが、当業者が認識するように、本発明の範囲および精神から逸れない限り、種々の変更および改善を行ってよい。例えば、暗号化、検証、および／または認証を用いずにディスク・ドライブが大量のデータを転送する場合に適応するように大量データ転送方式を変更して、データおよびコマンド検証のコストを減らすと共に、簡単なマスタリング機能を可能にするのは容易なことである。

【００４５】

本発明のプロセスおよびシステムについて、流れ図の形の機能的ステップを用いて上に説明した。理解されるように、別段の指定がない限り、また本発明の範囲および精神から逸れない限り、複数の機能を１つの物理的装置内またはソフトウエア製品の中のソフトウエア・モジュール内に統合してよいし、或る機能を別個の物理的装置またはソフトウエア・モジュール内で実現してもよい。また認識されるように、ハードウエアとソフトウエアとの境界は必ずしもはっきりしない。

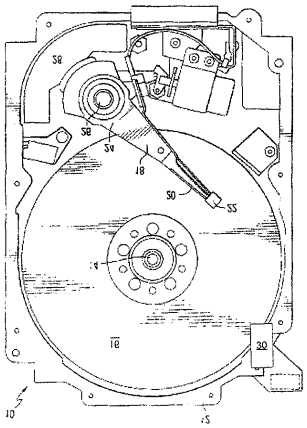
したがって、本発明が制約されるのは特定の例示の実施の形態ではなく、特許請求の範囲だけであることを理解していただきたい。

【符号の説明】

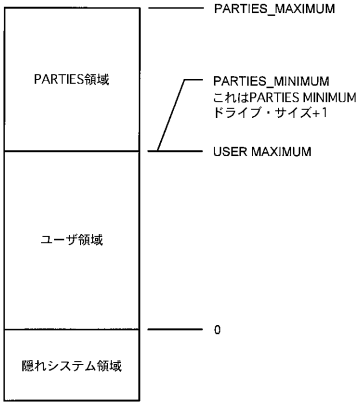
【００４６】

４０　ネットワーク・サーバ
４２　計算装置
４４　プロセッサ
４６　揮発性メモリ・ユニット
４８　不揮発性メモリ・ユニット
５０　大容量記憶装置

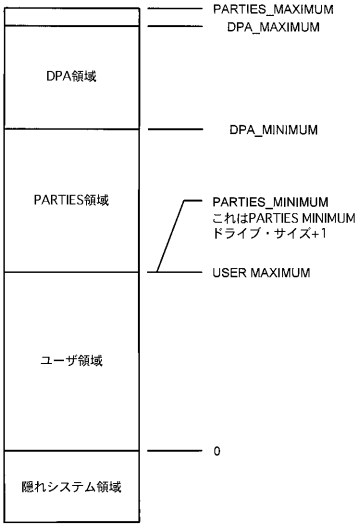
【図２】



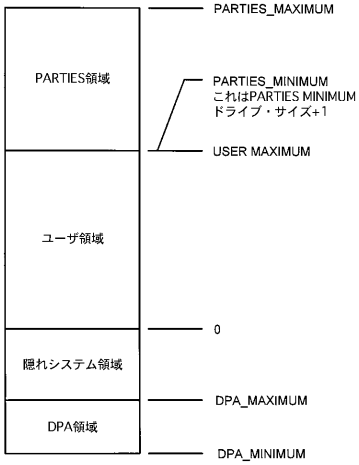
【図３】



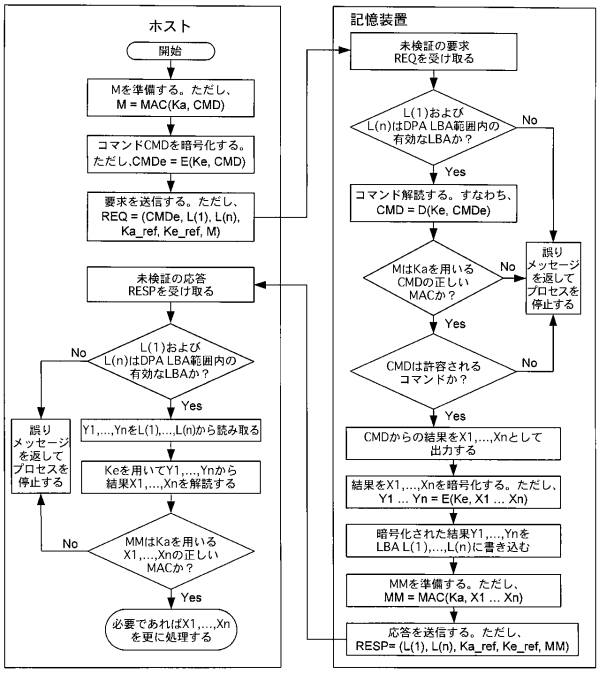
【図４】



【図５】

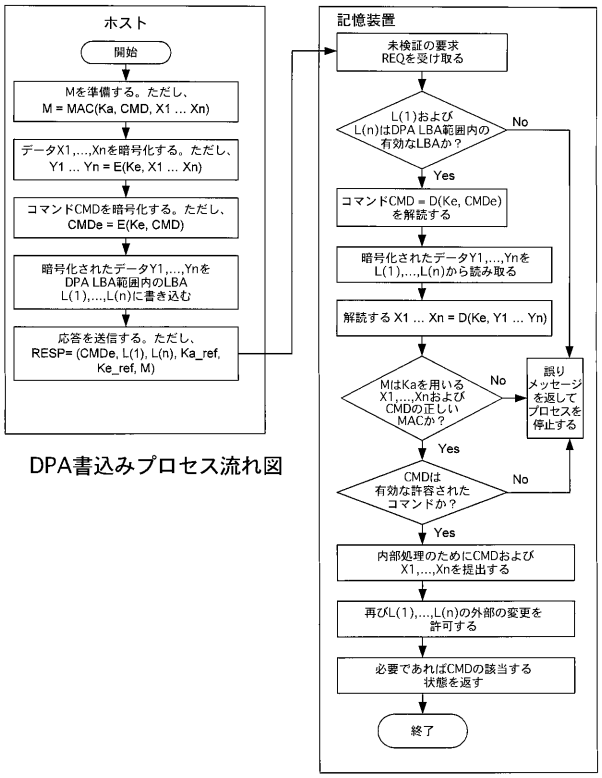


【図６】



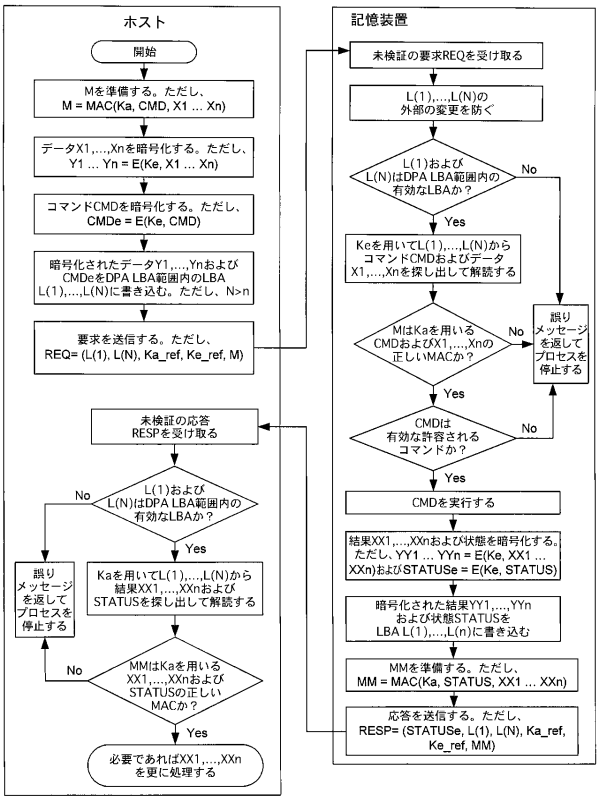
DPA読取りプロセス流れ図

【図７】



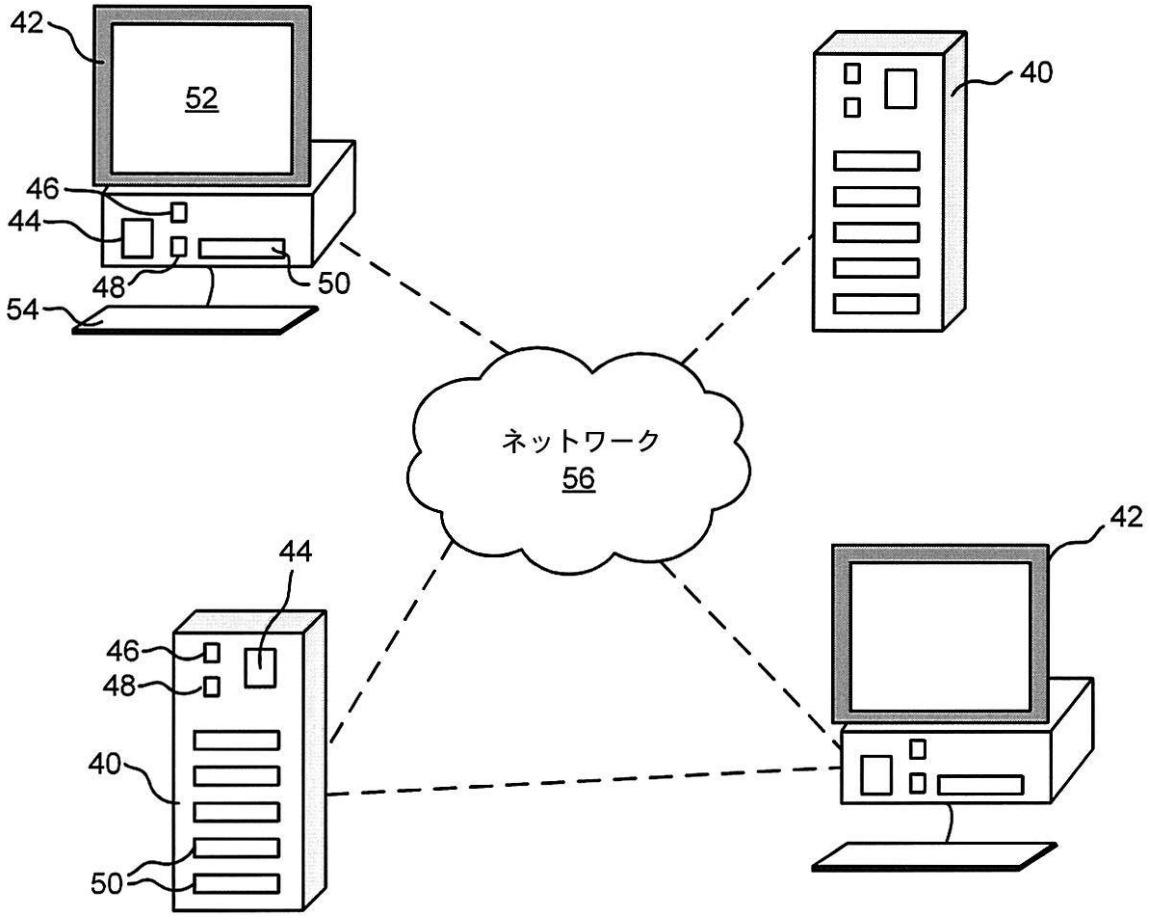
DPA書込みプロセス流れ図

【図８】



一般操作プロセス流れ図

【図１】



フロントページの続き

(74)代理人 100111246
弁理士 荒川 伸夫
(74)代理人 100124523
弁理士 佐々木 眞人
(74)代理人 110000855
特許業務法人浅村特許事務所
(74)代理人 100066692
弁理士 浅村 皓
(74)代理人 100072040
弁理士 浅村 肇
(74)代理人 100091339
弁理士 清水 邦明
(74)代理人 100094673
弁理士 林 鈺三
(74)代理人 100159525
弁理士 大日方 和幸
(74)代理人 100138346
弁理士 畑中 孝之
(74)代理人 100147658
弁理士 岩見 晶啓
(72)発明者 ドナルド ロジナック ビーバー
アメリカ合衆国、ペンシルヴァニア、ピッツバーグ、 オークリーフ レーン １６５３

審査官 坂東 博司

(56)参考文献 特開２００４－０１３５６３（ＪＰ，Ａ）
特開２００４－２３４０５３（ＪＰ，Ａ）
特開２００７－３１６７３６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ 3／０６
Ｇ０６Ｆ １２／１４