(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2014-513484
(P2014-513484A)
(43)公表日　平成26年5月29日(2014.5.29)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/08	(2006.01)	H04L	9/00	601C	5J104
H04L	9/10	(2006.01)	H04L	9/00	621A	
			H04L	9/00	601E	

審査請求 未請求　予備審査請求 未請求　（全 44 頁）

(21)出願番号　特願2014-508446 (P2014-508446)
(86)(22)出願日　平成24年4月20日 (2012.4.20)
(85)翻訳文提出日　平成26年1月4日 (2014.1.4)
(86)国際出願番号　PCT/US2012/034452
(87)国際公開番号　WO2012/148812
(87)国際公開日　平成24年11月1日 (2012.11.1)
(31)優先権主張番号　61/480,518
(32)優先日　平成23年4月29日 (2011.4.29)
(33)優先権主張国　米国 (US)

(71)出願人　508243639
エルエスアイ　コーポレーション
アメリカ合衆国カリフォルニア州９５１３１，サンノゼ，リッダー・パーク・ドライヴ　１３２０
(74)代理人　100104411
弁理士　矢口　太郎
(72)発明者　ラーム、ファーボッド　マイケル
アメリカ合衆国、９５０１４　カリフォルニア州、クパティーノ、１０１８８　キャス　プレイス

Fターム(参考)　5J104 AA01　AA16　EA17　NA02　NA37

最終頁に続く

(54)【発明の名称】暗号化トランスポート・ソリッドステート・ディスク・コントローラ

(57)【要約】
【課題】　暗号化トランスポートＳＳＤコントローラは、コマンド、記憶アドレスを受け取り、フラッシュメモリなどの不揮発性メモリ（Ｎｏｎ－Ｖｏｌａｔｉｌｅ　Ｍｅｍｏｒｙ：NVM）に圧縮（および任意選択で暗号化された）形式でデータを記憶する目的でホストとデータを交換するためのインターフェースを有する。前記ホストから受け取られた暗号化データは復号化され、且つ可逆的圧縮を使用して圧縮されてフラッシュメモリ書き込み増幅を有利に低減させる。前記圧縮されたデータは再暗号化され、フラッシュメモリに記憶される。前記記憶されたデータは、ホストに送信される前に読み出され、復号化、展開、および再暗号化される。単一の集積回路などのセキュアな物理境界内で実施されると、前記ＳＳＤコントローラは暗号化データを、ホストへの送出を含むフラッシュメモリ内の記憶を介した受け取りから保護する。具体的実施形態では、コントローラはホストとセッション暗号化鍵および復号化鍵を交換し、かつ／またはＴＣＧ　Ｏｐａｌなどのセキュリティプロトコルを使用して暗号化鍵および復号化鍵を決定する。

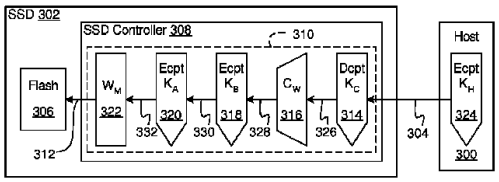

Fig. 3A

【特許請求の範囲】
【請求項１】
システムであって、
ホストから暗号化データおよび記憶アドレスを受け取る手段と、
前記受け取る手段からの結果の少なくとも一部を復号化する手段と、
前記復号化する手段からの結果の少なくとも一部を圧縮して書き込み増幅を有利に低減させる手段と、
前記圧縮する手段からの結果の少なくとも一部を暗号化する手段と、
前記暗号化する手段からの結果の少なくとも一部を書式設定（ｆｏｒｍａｔｔｉｎｇ）する手段と、
前記書式設定する手段からの結果の少なくとも一部を、前記記憶アドレスに従って１若しくはそれ以上の不揮発性メモリ（Ｎｏｎ－Ｖｏｌａｔｉｌｅ　Ｍｅｍｏｒｉｅｓ：ＮＶＭｓ）に記憶する手段と
を有し、
前記受け取る手段、前記復号化する手段、前記圧縮する手段、前記暗号化する手段、および前記書式設定する手段は、各々、少なくとも部分的にソリッドステートディスク（Ｓｏｌｉｄ－Ｓｔａｔｅ　Ｄｉｓｋ：ＳＳＤ）のコントローラに含まれており、前記ソリッドステートディスクは前記不揮発性メモリと前記コントローラとを有するものである
システム。
【請求項２】
請求項１記載のシステムにおいて、さらに、
前記ホストと１若しくはそれ以上の暗号化鍵および復号化鍵を交換する手段
を有するものであり、
前記復号化する手段は、前記交換された鍵の少なくとも一部分を使用して前記受け取られた暗号化データを復号化するものであるシステム。
【請求項３】
請求項２記載のシステムにおいて、前記復号化する手段、前記圧縮する手段、および前記暗号化する手段はセキュアな物理境界内にあるシステム。
【請求項４】
請求項３記載のシステムにおいて、前記セキュアな物理境界は単一の集積回路を含むものであるシステム。
【請求項５】
請求項３記載のシステムにおいて、さらに、
前記交換された鍵の少なくとも一部分を前記セキュアな物理境界内に保存する手段を有するものであるシステム。
【請求項６】
請求項１記載のシステムにおいて、前記圧縮する手段は可逆的圧縮を実施するものであるシステム。
【請求項７】
請求項１記載のシステムにおいて、前記暗号化データはセキュリティプロトコルに従って暗号化されるものであるシステム。
【請求項８】
請求項７記載のシステムにおいて、前記セキュリティプロトコルはメタデータを使用して暗号化鍵および復号化鍵を決定するシステム。
【請求項９】
請求項８記載のシステムにおいて、前記セキュリティプロトコルはトラステッド・コンピューティング・グループ（Ｔｒｕｓｔｅｄ　Ｃｏｍｐｕｔｉｎｇ　Ｇｒｏｕｐ：ＴＣＧ）Ｏｐａｌであるシステム。
【請求項１０】
請求項８記載のシステムにおいて、前記暗号化鍵および復号化鍵は、少なくとも一部は

、前記メタデータの記憶アドレス範囲によって決定されるシステム。
【請求項１１】
請求項１０記載のシステムにおいて、前記暗号化鍵および復号化鍵のうちの１つ１つは、少なくとも一部は、前記メタデータのそれぞれの記憶アドレス範囲によって決定されるシステム。
【請求項１２】
請求項１記載のシステムにおいて、前記暗号化する手段は内部暗号化の手段であり、システムはさらに、前記内部暗号化の手段と前記書式設定する手段との間で動作するバックエンド暗号化の手段を有するものであるシステム。
【請求項１３】
方法であって、
ホストから記憶アドレスを受け取る工程と、
前記記憶アドレスに従って、１若しくはそれ以上の不揮発性メモリ（Ｎｏｎ－Ｖｏｌａｔｉｌｅ　Ｍｅｍｏｒｉｅｓ：ＮＶＭｓ）から、書式付き暗号化圧縮データをインポートする工程と、
前記インポートしたデータの少なくとも一部を書式解除（ｕｎｆｏｒｍａｔｔｉｎｇ）する工程と、
前記書式解除したデータの少なくとも一部を復号化する工程と、
前記復号化したデータの少なくとも一部を展開する工程と、
前記展開したデータの少なくとも一部を暗号化する工程と、
前記暗号化したデータの少なくとも一部を前記ホストにエクスポートする工程と
を有し、
前記インポートする工程、前記書式解除する工程、前記復号化する工程、前記展開する工程、前記暗号化する工程、および前記エクスポートする工程は、各々少なくとも部分的にソリッドステートディスク（Ｓｏｌｉｄ－Ｓｔａｔｅ　Ｄｉｓｋ：ＳＳＤ）のコントローラにより実行され、前記ソリッドステートディスクは前記不揮発性メモリと前記コントローラとを有するものである方法。
【請求項１４】
請求項１３記載の方法において、さらに、
前記ホストと暗号化鍵および復号化鍵を交換する工程
を有するものであり、
前記暗号化する工程は、前記交換した鍵の少なくとも一部分を使用して前記展開したデータを暗号化する方法。
【請求項１５】
請求項１３記載の方法において、さらに、
前記復号化する工程、前記展開する工程、および前記暗号化する工程をセキュアな物理境界内で実行する工程を有するものである方法。
【請求項１６】
システムであって、
ホストから暗号化データを受け取ることができるようになっているホストインターフェースと、
少なくとも一部はセッション復号化鍵を使用して、前記暗号化データの少なくとも一部分を復号化することができるようになっている復号化ハードウェア層と、
前記復号化ハードウェア層の結果の少なくとも一部分を可逆的に圧縮することができるようになっている可逆的圧縮ハードウェア層と、
前記可逆的圧縮ハードウェア層の結果の少なくとも一部分を暗号化することができるようになっている内部暗号化ハードウェア層と、
前記内部暗号化ハードウェア層の結果の少なくとも一部分を暗号化することができるようになっているバックエンド暗号化ハードウェア層と、
前記バックエンド暗号化ハードウェア層の結果の少なくとも一部分を受け取るように結

合された、前記バックエンド暗号化ハードウェアの結果の前記少なくとも一部分を１若しくはそれ以上のフラッシュメモリに書き込むことができるようになっているフラッシュ・メモリ・インターフェースと
を有し、
前記内部暗号化ハードウェア層は選択的にバイパス可能であり、
前記ハードウェア層はソリッドステートディスク（ＳＳＤ）に具備されており、
前記ホストインターフェースはストレージインターフェース規格と適合するシステム。
【請求項１７】
請求項１６記載のシステムにおいて、さらに、
前記フラッシュメモリを有するものであるシステム。
【請求項１８】
請求項１６記載のシステムにおいて、前記ホストは平文を暗号化して前記暗号化データを生成することができるようになっており、さらに、
前記ホストを有するものであるシステム。
【請求項１９】
記憶装置の処理要素によって実行されると、前記処理要素に動作を実行させ、かつ／または制御させる命令のセットが記憶されている有形のコンピュータ可読媒体であって、前記動作は、
コンピューティングホストからデータを受け取る動作と、
複数の動作モードのうちの１つを選択的に使用可能にする動作であって、前記モードは、
暗号化動作モードであって、
前記受け取ったデータの少なくとも一部分を復号化する動作と、
前記復号化したデータの少なくとも一部分を圧縮する動作と、
前記圧縮した復号化データの少なくとも一部分を再暗号化する動作と、
前記再暗号化したデータの少なくとも一部分を暗号化モード書き込みデータとして提供する動作と
を有する前記暗号化動作モードと、
非暗号化動作モードであって、
前記受け取ったデータの少なくとも一部分を圧縮する動作と、
前記圧縮した受け取ったデータの少なくとも一部分を非暗号化モード書き込みデータとして提供する動作と
を有する前記非暗号化動作モードと
を有する、前記選択的に使用可能にする動作と、
前記暗号化動作モードで、前記暗号化モード書き込みデータを選択したモードの書き込みデータとして選択する動作と、
前記非暗号化動作モードで、前記非暗号化モード書き込みデータを前記選択したモードの書き込みデータとして選択する動作と、
前記選択したモードの書き込みデータを、１若しくはそれ以上の不揮発性メモリ（ＮＶＭ）に記憶するために書式設定する動作と
を有し、
有形のコンピュータ可読媒体および前記処理要素はソリッドステートディスク（ＳＳＤ）に具備されている、有形のコンピュータ可読媒体。
【請求項２０】
請求項１９記載の有形のコンピュータ可読媒体において、前記ＮＶＭのうちの少なくとも１つは前記ＳＳＤに具備されている有形のコンピュータ可読媒体。
【請求項２１】
請求項１９記載の有形のコンピュータ可読媒体において、前記書式設定する動作は、前記選択したモードの書き込みデータを選択的に暗号化する動作を有する有形のコンピュータ可読媒体。

【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本出願の優先権利益の主張を、（それがある場合には、適宜）添付の出願データシート、請求、または送達状において行う。本出願の種類によって許容される範囲内で、本出願はこの参照によりあらゆる目的で以下の出願を組み込むものであり、以下の出願はすべて、発明がなされた時点において本出願と所有者を同じくするものである。
【０００２】
２０１１年４月２９日付で出願された、Ｆａｒｂｏｄ Ｍｉｃｈａｅｌ Ｒａａｍを筆頭発明者とする、「Ｅｎｃｒｙｐｔｅｄ－Ｔｒａｎｓｐｏｒｔ Ｓｏｌｉｄ－Ｓｔａｔｅ Ｄｉｓｋ Ｃｏｎｔｒｏｌｌｅｒ」という名称の、米国仮出願（整理番号第ＳＦ－１０－０８号および出願番号第６１／４８０５１８号）。
【背景技術】
【０００３】
分野：不揮発性格納技術の進歩が、使用の性能、効率、及び有用性の改善を提供するために必要とされる。
【０００４】
関連技術：公知である、または周知であるものとして明記されない限り、コンテキスト、定義、または比較を目的とするものを含む本明細書における技法および概念の言及は、そのような技法または概念が以前から公知であり、あるいは先行技術の一部であることの容認と解釈すべきではない。特許、特許出願、および出版物を含む、本明細書で引用されるあらゆる参照文献は（それがある場合には）、具体的に組み込まれているか否かを問わず、あらゆる目的で、この参照によりその全体が本明細書に組み込まれるものである。
【発明の概要】
【課題を解決するための手段】
【０００５】
本発明は多くの仕方で実施されてよく、これには、プロセス、製造品、装置、システム、組成物としての仕方、ならびに、コンピュータ可読記憶媒体（ディスクといった光学的大容量記憶装置および／または磁気的大容量記憶装置、フラッシュストレージといった不揮発性記憶を有する集積回路など）や、プログラム命令が光通信リンクまたは電子通信リンク上で送られるコンピュータネットワークといったコンピュータ可読媒体としての仕方が含まれうる。本明細書では、これらの実施態様、または本発明が取りうる任意の他の形態を、技法と呼ぶ場合もある。詳細な説明では、上記の分野における使用の性能、効率、および有用性の改善を可能にする本発明の１若しくはそれ以上の実施形態の説明を提供する。詳細な説明は、詳細な説明の残りの部分のより迅速な理解を容易にするための導入部を含む。導入部は、本明細書で説明する概念に従うシステム、方法、製造品、およびコンピュータ可読媒体のうちの１若しくはそれ以上の例示的実施形態を含む。結論の項でより詳細に論じるように、本発明は、発行される特許請求の範囲内のあらゆる可能な改変形態および変形形態を包含するものである。
【図面の簡単な説明】
【０００６】
【図１Ａ】図１Ａは、不揮発性メモリ（Ｎｏｎ－Ｖｏｌａｔｉｌｅ Ｍｅｍｏｒｙ：ＮＶＭ）要素（フラッシュメモリなど）によって実施されるような不揮発性記憶を管理するための暗号化トランスポートの技法を使用するＳＳＤコントローラを含むソリッドステートディスク（Ｓｏｌｉｄ－Ｓｔａｔｅ Ｄｉｓｋ：ＳＳＤ）の実施形態の選択された詳細を示す図である。
【図１Ｂ】図１Ｂは、図１ＡのＳＳＤの１つ若しくはそれ以上のインスタンスを含むシステムの様々な実施形態の選択された詳細を示す図である。
【図２】図２は、図１Ａに示すような不揮発性記憶を管理するための暗号化トランスポー

トの技法を使用したＳＳＤの具体的応用の一例を示す図である。
【図３Ａ】図３Ａは、暗号化トランスポートＳＳＤの書き込みデータパス機能であって、２段の圧縮後暗号化を含む書き込みデータパス機能の一実施形態の選択された詳細を示す図である。
【図３Ｂ】図３Ｂは、図３Ａの暗号化トランスポートＳＳＤの読み取りデータパス機能であって、２段の展開前復号化を含む読み取りデータパス機能の一実施形態の選択された詳細を示す図である。
【図４】図４は、例えば暗号化トランスポートＳＳＤのコンテキストで暗号化トランスポートデータ転送を実行するための、ホストとＳＳＤコントローラとの間のセキュアな通信リンクの作成、使用、および放棄の一実施形態を示す流れ図である。
【図５】図５は、暗号化トランスポートＳＳＤコントローラのデータパス制御および／または動作の一実施形態を示す流れ図である。
【０００７】

【表１】

図面の参照符号の一覧

参照符号	要素名
１００	ＳＳＤコントローラ
１０１	ＳＳＤ
１０２	ホスト
１０３	（任意選択の）スイッチ／ファブリック／中間コントローラ
１０４	中間インターフェース
１０５	ＯＳ
１０６	ファームウェア（ＦｉｒｍＷａｒｅ：ＦＷ）
１０７	ドライバ
１０７Ｄ	点線矢印（ホストソフトウェア←→入出力装置通信）
１０９	アプリケーション
１０９Ｄ	点線矢印（ドライバを介したアプリケーション←→入出力装置通信）
１０９Ｖ	点線矢印（ＶＦを介したアプリケーション←→入出力装置通信）
１１０	外部インターフェース
１１１	ホストインターフェース
１１２Ｃ	（任意選択の）カードメモリ
１１３	タグ追跡
１１４	マルチデバイス管理ソフトウェア
１１５	ホストソフトウェア
１１６	入出力カード
１１７	入出力装置／リソースおよび記憶装置／リソース
１１８	サーバ
１１９	ＬＡＮ／ＷＡＮ
１２１	データ処理
１２３	エンジン
１３１	バッファ
１３３	ＤＭＡ
１３５	ＥＣＣ－Ｘ
１３７	メモリ
１４１	マップ
１４３	表
１５１	リサイクラ
１６１	ＥＣＣ
１７１	ＣＰＵ
１７２	ＣＰＵコア
１７３	コマンド管理
１７５	バッファ管理
１７７	変換管理
１７９	コヒーレンシ管理
１８０	メモリインターフェース
１８１	デバイス管理
１８２	識別情報管理
１９０	デバイスインターフェース
１９１	デバイスインターフェース論理
１９２	フラッシュデバイス

参照符号	要素名
１９３	スケジューリング
１９４	フラッシュダイ
１９９	ＮＶＭ
２００	暗号化トランスポートＳＳＤ
２０２	コンピュータ
２０４	リモートサーバ
２０６	ＶＧＡディスプレイ
２０８	ＶＧＡビデオ信号
２１０	ＶＧＡコントローラ
２１２	セキュアな通信リンク（ＳＳＤ－リモートサーバ）
２１４	フラッシュメモリ
２１６	セキュアな物理境界（ＳＳＤコントローラ）
２１８	セキュアな通信リンク（ＳＳＤ－ＶＧＡコントローラ）
２２０	セキュアな物理境界（ＶＧＡコントローラ）
２２２	（リモートサーバとコンピュータとの間の）結合
２２４	（コンピュータとＳＳＤコントローラとの間の）結合
３００	ホスト
３０２	暗号化トランスポートＳＳＤ
３０４	暗号化データ
３０６	フラッシュメモリ
３０８	ＳＳＤコントローラ
３１０	書き込みデータパス
３１２	暗号化－書式設定データ
３１４	セッション復号化層
３１６	可逆的圧縮層
３１８	内部暗号化層
３２０	バックエンド暗号化層
３２２	書き込み－書式設定層
３２６	復号化データ
３２８	圧縮データ
３３０	暗号化－圧縮データ
３３２	バックエンド暗号化データ
３３６	読み取り書式設定解除層
３３８	バックエンド復号化層
３４０	内部復号化層
３４２	読み取り伸張層
３４４	セッション暗号化層
３４６	読み取りデータパス
４０１	開始
４０２	「チャネルを開く」要求
４０３	ホスト側の認証
４０４	ホスト側の鍵交換
４０５	ホスト側のセキュアなトラフィック交換
４０５Ｘ	ホスト側のＴＣＧ　Ｏｐｓ／ストレージアクセス
４０６	「チャネルを閉じる」要求
４０９	ホスト動作
４１２	「チャネルを開く」受諾

参照符号	要素名
４１３	コントローラ側の認証
４１４	コントローラ側の鍵交換
４１５	コントローラ側のセキュアなトラフィック交換
４１５Ｘ	コントローラ側のＴＣＧ　Ｏｐｓ／ストレージアクセス
４１６	「チャネルを閉じる」受諾
４１７	鍵を破壊する
４１９	コントローラ動作
５０１	書き込みデータを受け取る
５０２	書き込みデータを復号化する
５０３	復号化したデータを圧縮する
５０４	圧縮したデータを暗号化する
５０５	暗号化したデータを（再）暗号化する
５０６	（再）暗号化したデータを変調する
５０７	変調したデータを記憶する
５０８	ホスト側のコントローラ側へのセキュアなトラフィック
５１０	コントローラ側のホスト側へのセキュアなトラフィック
５１１	暗号化したデータを提供する
５１２	伸張したデータを暗号化する
５１３	（再）復号化したデータを伸張する
５１４	復号化したデータを復号化する
５１５	復調したデータを復号化する
５１６	読み取ったデータを復調する
５１７	データを読み取る
５２２Ｋ	鍵＝K_H
５２４Ｋ	鍵＝K_B
５２５Ｋ	鍵＝K_A

【発明を実施するための形態】

【０００８】

本発明の１つ若しくはそれ以上の実施形態の詳細な説明を、以下で、本発明の選択された詳細を図示する添付の図を併用して行う。本発明を実施形態との関連で説明する。実施形態は、本明細書では、単なる例示であると理解されるものであり、本発明は、明確に、本明細書中の実施形態のいずれか若しくは全部に、またはいずれか若しくは全部によって限定されるものではなく、本発明は、多数の代替形態、改変形態、および均等物を包含するものである。説明が単調にならないように、様々な言葉によるラベル（これに限定されるものではないが、最初の、最後の、ある一定の、様々な、別の、他の、特定の、選択の、いくつかの、目立ったなど）が実施形態のセットを区別するために適用される場合がある。本明細書で使用する場合、そのようなラベルは、明確に、質を伝えるためのものでも、いかなる形の好みや先入観を伝えるためのものでもなく、単に、別々のセットを都合よく区別するためのものにすぎない。開示するプロセスのいくつかの動作の順序は本発明の範囲内で変更可能である。多様な実施形態がプロセス、方法、および／またはプログラム命令の各特徴の差異を説明するのに使用される場合は常に、所定の、または動的に決定される基準に従って、複数の多様な実施形態にそれぞれ対応する複数の動作モードの１つの静的選択および／または動的選択を行う他の実施形態が企図されている。以下の説明では、本発明の十分な理解を提供するために、多数の具体的詳細を示す。それらの詳細は例として示すものであり、本発明は、それらの詳細の一部または全部がなくても、特許請求の範囲に従って実施されうる。わかりやすくするために、本発明に関連した技術分野で公知の技術資料は、本発明が不必要に曖昧になることのないように詳細に説明していない。

【０００９】

概説

この概説は、詳細な説明のより迅速な理解を助けるために含まれるにすぎず、本発明は、（それがある場合には、明示的な例を含む）この概説で提示される概念だけに限定されるものではなく、どんな概説の段落も、必然的に、主題全体の縮約された見方であり、網羅的な、または限定的な記述であることを意味するものではない。例えば、以下の概説は

、スペースおよび編成によりある一定の実施形態だけに限定される概要情報を提供するものである。特許請求の範囲が究極的にそこに導かれることになる実施形態を含む多くの他の実施形態があり、それらを本明細書の残りの部分にわたって論じる。

【００１０】

頭字語

ここで定義される様々な縮めた表現の略語（例えば、頭字語）の少なくとも一部が本明細書において使用される特定の要素を指す。

【００１１】

【表２】

頭字語	説明
ＡＥＳ	Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ（高度暗号化規格）
ＡＨＣＩ	Ａｄｖａｎｃｅｄ Ｈｏｓｔ Ｃｏｎｔｒｏｌｌｅｒ Ｉｎｔｅｒｆａｃｅ（アドバンスド・ホスト・コントローラ・インターフェース）
ＡＰＩ	Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｇｒａｍ Ｉｎｔｅｒｆａｃｅ（アプリケーション・プログラム・インターフェース）
ＡＳＣＩＩ	Ａｍｅｒｉｃａｎ Ｓｔａｎｄａｒｄ Ｃｏｄｅ ｆｏｒ Ｉｎｆｏｒｍａｔｉｏｎ Ｉｎｔｅｒｃｈａｎｇｅ（情報交換用米国標準コード）
ＢＣＨ	Ｂｏｓｅ Ｃｈａｕｄｈｕｒｉ Ｈｏｃｑｕｅｎｇｈｅｍ（ボーズ・チョドーリ・オッケンジェム）
ＡＴＡ	Ａｄｖａｎｃｅｄ Ｔｅｃｈｎｏｌｏｇｙ Ａｔｔａｃｈｍｅｎｔ（ＡＴ Ａｔｔａｃｈｍｅｎｔ）（アドバンスド・テクノロジ・アタッチメント（ＡＴアタッチメント））
ＣＤ	Ｃｏｍｐａｃｔ Ｄｉｓｋ（コンパクトディスク）
ＣＦ	Ｃｏｍｐａｃｔ Ｆｌａｓｈ（コンパクトフラッシュ）
ＣＭＯＳ	Ｃｏｍｐｌｅｍｅｎｔａｒｙ Ｍｅｔａｌ Ｏｘｉｄｅ Ｓｅｍｉｃｏｎｄｕｃｔｏｒ（相補型金属酸化膜半導体）
ＣＰＵ	Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ（中央処理装置）
ＣＲＣ	Ｃｙｃｌｉｃ Ｒｅｄｕｎｄａｎｃｙ Ｃｈｅｃｋ（巡回冗長検査）
ＤＡＳ	Ｄｉｒｅｃｔ Ａｔｔａｃｈｅｄ Ｓｔｏｒａｇｅ（ダイレクト・アタッチト・ストレージ）
ＤＤＲ	Ｄｏｕｂｌｅ－Ｄａｔａ－Ｒａｔｅ（ダブルデータレート）
ＤＥＳ	Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ（データ暗号化規格）
ＤＭＡ	Ｄｉｒｅｃｔ Ｍｅｍｏｒｙ Ａｃｃｅｓｓ（直接メモリアクセス）
ＤＮＡ	Ｄｉｒｅｃｔ ＮＡＮＤ Ａｃｃｅｓｓ（直接ＮＡＮＤアクセス）
ＤＲＡＭ	Ｄｙｎａｍｉｃ Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ（ダイナミック・ランダム・アクセス・メモリ）
ＤＶＤ	Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ／Ｖｉｄｅｏ Ｄｉｓｋ（ディジタル多用途／ビデオディスク）
ＤＶＲ	Ｄｉｇｉｔａｌ Ｖｉｄｅｏ Ｒｅｃｏｒｄｅｒ（ディジタル・ビデオ・レコーダ）
ＥＣＣ	Ｅｒｒｏｒ－Ｃｏｒｒｅｃｔｉｎｇ Ｃｏｄｅ（誤り訂正符号）
ｅＭＭＣ	Ｅｍｂｅｄｄｅｄ ＭｕｌｔｉＭｅｄｉａＣａｒｄ（組み込みマルチメディアカード）
ｅＳＡＴＡ	ｅｘｔｅｒｎａｌ Ｓｅｒｉａｌ Ａｄｖａｎｃｅｄ Ｔｅｃｈｎｏｌｏｇｙ Ａｔｔａｃｈｍｅｎｔ（外部シリアル・アドバンスド・テクノロジ・アタッチメント）
ＧＰＳ	Ｇｌｏｂａｌ Ｐｏｓｉｔｉｏｎｉｎｇ Ｓｙｓｔｅｍ（全地球測位システム）
ＨＤＤ	Ｈａｒｄ Ｄｉｓｋ Ｄｒｉｖｅ（ハード・ディスク・ドライブ）
Ｉ／Ｏ	Ｉｎｐｕｔ／Ｏｕｔｐｕｔ（入出力）
ＩＣ	Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ（集積回路）
ＩＤＥ	Ｉｎｔｅｇｒａｔｅｄ Ｄｒｉｖｅ Ｅｌｅｃｔｒｏｎｉｃｓ（統合ドライブエレクトロニクス）

頭字語	説明
ＪＰＥＧ	Ｊｏｉｎｔ Ｐｈｏｔｏｇｒａｐｈｉｃ Ｅｘｐｅｒｔｓ Ｇｒｏｕｐ（ジョイント・フォトグラフィック・エキスパーツ・グループ）
ＬＡＮ	Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ（ローカル・エリア・ネットワーク）
ＬＢ	Ｌｏｇｉｃａｌ Ｂｌｏｃｋ（論理ブロック）
ＬＢＡ	Ｌｏｇｉｃａｌ Ｂｌｏｃｋ Ａｄｄｒｅｓｓ（論理ブロックアドレス）
ＬＤＰＣ	Ｌｏｗ－Ｄｅｎｓｉｔｙ Ｐａｒｉｔｙ－Ｃｈｅｃｋ（低密度パリティ検査）
ＬＰＮ	Ｌｏｇｉｃａｌ Ｐａｇｅ Ｎｕｍｂｅｒ（論理ページ番号）
ＬＺ	Ｌｅｍｐｅｌ－Ｚｉｖ（ラムペルージブ）
ＭＬＣ	Ｍｕｌｔｉ－Ｌｅｖｅｌ Ｃｅｌｌ（マルチレベルセル）
ＭＭＣ	ＭｕｌｔｉＭｅｄｉａＣａｒｄ（マルチメディアカード）
ＭＰＥＧ	Ｍｏｖｉｎｇ Ｐｉｃｔｕｒｅ Ｅｘｐｅｒｔｓ Ｇｒｏｕｐ（ムービング・ピクチャ・エキスパーツ・グループ）
ＮＡＳ	Ｎｅｔｗｏｒｋ Ａｔｔａｃｈｅｄ Ｓｔｏｒａｇｅ（ネットワーク・アタッチト・ストレージ）
ＮＣＱ	Ｎａｔｉｖｅ Ｃｏｍｍａｎｄ Ｑｕｅｕｉｎｇ（ネイティブ・コマンド・キューイング）
ＮＶＭ	Ｎｏｎ－Ｖｏｌａｔｉｌｅ Ｍｅｍｏｒｙ（不揮発性メモリ）
ＯＮＡ	Ｏｐｔｉｍｉｚｅｄ ＮＡＮＤ Ａｃｃｅｓｓ（最適化ＮＡＮＤアクセス）
ＯＮＦＩ	Ｏｐｅｎ ＮＡＮＤ Ｆｌａｓｈ Ｉｎｔｅｒｆａｃｅ（オープンＮＡＮＤフラッシュインターフェース）
ＯＳ	Ｏｐｅｒａｔｉｎｇ Ｓｙｓｔｅｍ（オペレーティングシステム）
ＰＣ	Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ（パーソナルコンピュータ）
ＰＣＩｅ	Ｐｅｒｉｐｈｅｒａｌ Ｃｏｍｐｏｎｅｎｔ Ｉｎｔｅｒｃｏｎｎｅｃｔ ｅｘｐｒｅｓｓ （ＰＣＩ ｅｘｐｒｅｓｓ）（周辺装置相互接続エクスプレス（ＰＣＩエクスプレス））
ＰＤＡ	Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｔ（携帯情報端末）
ＰＯＳ	Ｐｏｉｎｔ Ｏｆ Ｓａｌｅ（販売時点）
ＲＡＩＤ	Ｒｅｄｕｎｄａｎｔ Ａｒｒａｙ ｏｆ Ｉｎｅｘｐｅｎｓｉｖｅ／Ｉｎｄｅｐｅｎｄｅｎｔ Ｄｉｓｋｓ（安価なディスク／独立ディスクの冗長アレイ）
ＲＳ	Ｒｅｅｄ－Ｓｏｌｏｍｏｎ（リード－ソロモン）
ＲＳＡ	Ｒｉｖｅｓｔ，Ｓｈａｍｉｒ ＆ Ａｄｌｅｍａｎ（リベスト、シャミアおよびエーデルマン）
ＳＡＮ	Ｓｔｏｒａｇｅ Ａｔｔａｃｈｅｄ Ｎｅｔｗｏｒｋ（ストレージ・アタッチト・ネットワーク）
ＳＡＳ	Ｓｅｒｉａｌ Ａｔｔａｃｈｅｄ Ｓｍａｌｌ Ｃｏｍｐｕｔｅｒ Ｓｙｓｔｅｍ Ｉｎｔｅｒｆａｃｅ （Ｓｅｒｉａｌ ＳＣＳＩ）（シリアル小型コンピュータ・システム・インターフェース（シリアルＳＣＳＩ））
ＳＡＴＡ	Ｓｅｒｉａｌ Ａｄｖａｎｃｅｄ Ｔｅｃｈｎｏｌｏｇｙ Ａｔｔａｃｈｍｅｎｔ （Ｓｅｒｉａｌ ＡＴＡ）（シリアル・アドバンスド・テクノロジ・アタッチメント（シリアルＡＴＡ））
ＳＣＳＩ	Ｓｍａｌｌ Ｃｏｍｐｕｔｅｒ Ｓｙｓｔｅｍ Ｉｎｔｅｒｆａｃｅ

頭字語	説明
	（小型コンピュータ・システム・インターフェース）
ＳＤ	Ｓｅｃｕｒｅ Ｄｉｇｉｔａｌ（セキュアディジタル）
ＳＤＲ	Ｓｉｎｇｌｅ－Ｄａｔａ－Ｒａｔｅ（シングルデータレート）
ＳＬＣ	Ｓｉｎｇｌｅ－Ｌｅｖｅｌ Ｃｅｌｌ（シングルレベルセル）
ＳＭＡＲＴ	Ｓｅｌｆ－Ｍｏｎｉｔｏｒｉｎｇ Ａｎａｌｙｓｉｓ ａｎｄ Ｒｅｐｏｒｔｉｎｇ Ｔｅｃｈｎｏｌｏｇｙ（自己モニタリング分析報告技術）
ＳＳＤ	Ｓｏｌｉｄ－Ｓｔａｔｅ Ｄｉｓｋ／Ｄｒｉｖｅ（ソリッドステートディスク／ドライブ）
ＴＣＧ	Ｔｒｕｓｔｅｄ Ｃｏｍｐｕｔｉｎｇ Ｇｒｏｕｐ（トラステッド・コンピューティング・グループ）
ＵＦＳ	Ｕｎｉｆｉｅｄ Ｆｌａｓｈ Ｓｔｏｒａｇｅ（ユニファイド・フラッシュ・ストレージ）
ＵＳＢ	Ｕｎｉｖｅｒｓａｌ Ｓｅｒｉａｌ Ｂｕｓ（ユニバーサル・シリアル・バス）
ＶＦ	Ｖｉｒｔｕａｌ Ｆｕｎｃｔｉｏｎ（仮想関数）
ＷＡＮ	Ｗｉｄｅ Ａｒｅａ Ｎｅｔｗｏｒｋ（広域ネットワーク）

ストレージ周辺装置の中には、トランスポート暗号化層を使用して、ホストからストレージ周辺装置に送られるデータを保護することができるようになっているものがある。ホストは、記憶媒体（ＮＶＭなど）に記憶されるべきストレージ周辺装置へのデータを送る前に、内部でデータを暗号化する。同様に、ストレージ周辺装置から読み取られ、ホストに送られるデータも、そのデータが書き込まれたときに同じ暗号化を有するものと想定され、ホストは使用するためにデータを復号化する。ホストから見ると、データは記憶媒体との間の全経路上で暗号化されている。

【００１２】

ある実施形態では、ＳＳＤといったストレージ周辺装置は、（ＮＡＮＤフラッシュチップのアレイといった）記憶媒体にデータを記憶する前に、いわゆる「バックエンド」暗号化により、データを内部で暗号化し、記憶媒体から暗号化データを読み取った後でデータを復号化する。ＳＳＤにおいて、バックエンド暗号化は、データを保護し、あるシナリオではＮＡＮＤフラッシュチップの耐久性を向上させるスクランブリング特性を提供するように働く。例えば、バックエンド暗号化は、ホストデータに使用されるあらゆる他の形の暗号化から独立して、記憶媒体に記憶されたＳＳＤのファームウェアを保護するのに使用される。

【００１３】

あるストレージ周辺装置は、ストレージ・セキュリティ・サブシステム・クラス（ＴＣＧ Ｏｐａｌなど）といったセキュリティプロトコルに従って動作し、ホストから受け取られる、記憶媒体に書き込まれるべきデータを暗号化することができるようになっており、さらに、記憶媒体から読み取られるデータを復号化することができるようになっている。ある実施形態では、セキュリティプロトコル暗号化／復号化は、記憶アドレス範囲といったメタデータを使用して、暗号化鍵および復号化鍵を一部決定する。別の実施形態では、１若しくはそれ以上のアドレス範囲があり、各範囲はそれぞれの鍵と関連付けられている。別の実施形態では、アドレス範囲のうちのどれも一致しない場合には、グローバルな「上記のどれでもない」鍵がある。様々な実施形態によれば、セキュリティプロトコル暗号化／復号化は、トランスポート暗号化／復号化と同じ、トランスポート暗号化／復号化と異なる、バックエンド暗号化／復号化と同じ、およびバックエンド暗号化／復号化と異なる、のうちの１若しくはそれ以上である。

【００１４】

ある実施形態では、ＳＳＤといったストレージ周辺装置は、ホストから受け取ったデータを、（ＮＡＮＤフラッシュチップのアレイといった）記憶媒体にデータを記憶する前に圧縮する。圧縮は、データの種類（例えばＪＰＥＧデータおよび／またはＭＰＥＧデータ

）に基づく不可逆的圧縮、局所的なやり方（ＬＺ圧縮など）で行われる可逆的圧縮、データ重複排除、および圧縮されるデータを表すのに必要とされる記憶を低減させる任意選択の可逆変換のうちの１若しくはそれ以上を含む。記憶の前のデータの圧縮は、有利には、書き込み増幅を低減させ、かつ／または様々なシナリオにおける見かけの記憶容量を増加させる。しかし、（例えばトランスポート暗号化のために）暗号化されているデータは、シナリオによっては、圧縮することができない。

【００１５】

ある実施形態では、ＳＳＤといったストレージ周辺装置は、ホストと鍵交換を行ってトランスポート暗号化層に使用される（１若しくはそれ以上の）鍵を決定し、任意選択で、かつ／または選択的に、各鍵がどの条件の下で使用されるか決定する。ストレージ周辺装置がホストからトランスポート暗号化データを受け取ると、ストレージ周辺装置は、任意選択で、かつ／または選択的に、（１若しくはそれ以上の）鍵のうちの選択された１つを使用して、トランスポート暗号化に従ってデータを復号化する。復号化されたデータは次いで圧縮される。ＴＣＧ　Ｏｐａｌといったセキュリティプロトコルが使用される別の実施形態では、圧縮されたデータは、任意選択で、かつ／または選択的に、セキュリティプロトコルに従って暗号化される。セキュリティプロトコルと異なるバックエンド暗号化が行われるさらに別の実施形態では、圧縮され、任意選択で、かつ／または選択的に、暗号化されたデータは、データが記憶媒体への書き込みのために変調される前に、バックエンド暗号化によってさらに暗号化される。

【００１６】

他の実施形態では、ＴＣＧ　Ｏｐａｌではなく、トランスポート暗号化が再利用される。すなわち、圧縮後に、圧縮されたデータは、（１若しくはそれ以上の）トランスポート暗号化鍵／トランスポート暗号化アルゴリズムを使用して再暗号化される。

【００１７】

データが記憶媒体から読み戻され、ホストに返されるときには、元の暗号化データがホストに返されるように、データを記憶するための前述の動作は事実上反転される。

【００１８】

暗号化アルゴリズムの例は、ＤＥＳ、トリプルＤＥＳ、ＡＥＳ－１２８、ＡＥＳ－２５６、ＲＳＡ、および他の公開鍵暗号化アルゴリズムである。

【００１９】

ある状況では、特定のサイズのホストストレージ書き込みがＳＳＤのフラッシュメモリへの（各々が、例えば、その特定のサイズの倍数などのサイズを有する）複数の書き込みを生じるときに、書き込み増幅が生じる。複数の書き込みは、例えば、フラッシュメモリのある部分を書き込む（例えばプログラムする）前の当該部分の消去、ウェアレベリング、不要部分の整理、およびシステムデータ書き込みを生じるフラッシュメモリ管理操作などから生じる。書き込み増幅の計算の一例は、（例えば、ホスト書き込みと関連付けられたホストデータの書き込みを完了するためのシステム書き込みなどを含む）ホスト書き込みの特定の集合の代わりにフラッシュメモリに書き込まれたデータの量を、ホスト書き込みのその特定の集合によって書き込まれたデータの量で割ったものである。ある使用シナリオでは、ホスト書き込みの特定の集合によって書き込まれたデータの圧縮は、ホスト書き込みのその特定の集合の代わりにフラッシュメモリに書き込まれるデータの量を低減させることを可能にする。ホスト書き込みのその特定の集合の代わりにフラッシュメモリに書き込まれるデータの量が低減されるため、書き込み増幅はそれによって低減される。

【００２０】

一部の実施形態では、ＮＶＭ内の様々なサイズの量の圧縮データにアクセスすることにより、ある使用シナリオでは記憶効率が改善される。例えば、ＳＳＤコントローラは、コンピューティングホストから（例えばディスク書き込みコマンドに関連した）（圧縮されていない）データを受け取り、データを圧縮し、データをフラッシュメモリへ記憶する。コンピューティングホストからの（例えばディスク読み出しコマンドに関連した）その後の要求に応答して、ＳＳＤコントローラはフラッシュメモリから圧縮データを読み出し、

圧縮データを解凍し、解凍されたデータをコンピューティングホストに提供する。圧縮データは、様々なサイズの量に従ってフラッシュメモリに記憶され、各量のサイズは、例えば、圧縮アルゴリズム、動作モード、様々なデータに関する圧縮有効性により変動する。ＳＳＤコントローラは、一部は、含まれるマップ表を調べて（１つまたは複数の）ヘッダがフラッシュメモリのどこに記憶されているか確認することによってデータを解凍する。ＳＳＤコントローラは、適切な（圧縮）データがフラッシュメモリのどこに記憶されているか確認するためにフラッシュメモリから得た（１つまたは複数の）ヘッダをパースする。ＳＳＤコントローラは、コンピューティングホストに提供すべき解凍データを生成するために、フラッシュメモリからの適切なデータを解凍する。

【００２１】

様々な実施形態では、ＳＳＤコントローラは、コンピューティングホストとインターフェースするためのホストインターフェースと、フラッシュメモリといったＮＶＭとインターフェースするためのインターフェースと、各インターフェースを制御し、圧縮および解凍と共に、低レベル誤り訂正、高レベル誤り訂正、ならびに独立シリコン素子を用いた動的高レベル冗長性モード管理を行う（かつ／または行うことの様々な態様を制御する）ための回路とを含む。

【００２２】

様々な実施形態によれば、あるホストインターフェースは、ＵＳＢインターフェース規格、ＣＦインターフェース規格、ＭＭＣインターフェース規格、ｅＭＭＣインターフェース規格、サンダーボルトインターフェース規格、ＵＦＳインターフェース規格、ＳＤインターフェース規格、メモリ・スティック・インターフェース規格、ｘＤピクチャ・カード・インターフェース規格、ＩＤＥインターフェース規格、ＳＡＴＡインターフェース規格、ＳＣＳＩインターフェース規格、ＳＡＳインターフェース規格、およびＰＣＩｅインターフェース規格のうちの１つ若しくはそれ以上と適合する。様々な実施形態によれば、コンピューティングホストは、コンピュータ、ワークステーションコンピュータ、サーバコンピュータ、ストレージサーバ、ＳＡＮ、ＮＡＳデバイス、ＤＡＳデバイス、ストレージアプライアンス、ＰＣ、ラップトップコンピュータ、ノートブックコンピュータ、ネットブックコンピュータ、タブレット機器またはタブレットコンピュータ、ウルトラブックコンピュータ、電子読み出し装置（ｅ－ｒｅａｄｅｒなど）、ＰＤＡ、ナビゲーションシステム、（ハンドヘルド型）ＧＰＳ機器、自動通信路制御システム、自動車媒体制御システムまたはコンピュータ、プリンタ、コピー機またはファックス機またはオールインワン機器、ＰＯＳ機器、金銭登録機、メディアプレーヤ、テレビ、メディアレコーダ、ＤＶＲ、ディジタルカメラ、セルラハンドセット、コードレス電話機ハンドセット、および電子ゲームのうちの全部または任意の部分である。一部の実施形態では、インターフェースホスト（ＳＡＳ／ＳＡＴＡブリッジなど）は、コンピューティングホストおよび／またはコンピューティングホストへのブリッジとして動作する。

【００２３】

様々な実施形態では、ＳＳＤコントローラは、１つ若しくはそれ以上のプロセッサを含む。プロセッサは、ＳＳＤコントローラの動作を制御し、かつ／または行うためにファームウェアを実行する。ＳＳＤコントローラは、コマンドおよび／または状況ならびにデータを送り、受け取るためにコンピューティングホストと通信する。コンピューティングホストは、オペレーティングシステム、ドライバ、およびアプリケーションのうちの１つ若しくはそれ以上を実行する。コンピューティングホストによるＳＳＤコントローラとの通信は、任意選択で、かつ／または選択的に、ドライバおよび／またはアプリケーションによるものである。第１の例では、ＳＳＤコントローラへのすべての通信がドライバによるものであり、アプリケーションは、ドライバに高レベルコマンドを提供し、ドライバがそれをＳＳＤコントローラのための特定のコマンドに変換する。第２の例では、ドライバはバイパスモードを実施し、アプリケーションは、ドライバを介してＳＳＤコントローラに特定のコマンドを送ることができるようになっている。第３の例では、ＰＣＩｅ　ＳＳＤコントローラが１つ若しくはそれ以上の仮想機能（Ｖｉｒｔｕａｌ　Ｆｕｎｃｔｉｏｎｓ

：ＶＦｓ）をサポートし、アプリケーションが、一度構成されると、ドライバをバイパスしてＳＳＤコントローラを直接通信することを可能にする。

【００２４】

様々な実施形態によれば、あるＳＳＤは、ＨＤＤ、ＣＤドライブ、ＤＶＤドライブといった磁気的不揮発性記憶および／または光学的不揮発性記憶によって使用されるフォームファクタ、電気的インターフェース、および／またはプロトコルと適合する。様々な実施形態では、ＳＳＤは、０以上のパリティ符号、０以上のＲＳ符号、０以上のＢＣＨ符号、０以上のビタビ符号または他のトレリス符号、および０以上のＬＤＰＣ符号の様々な組み合わせを使用する。

【００２５】

例示的実施形態

詳細な説明の概説を終えるにあたり、以下に、例示的実施形態をまとめて示す。これらの例示的実施形態は、少なくとも一部は「ＥＣ」（Ｅｘａｍｐｌｅ Ｃｏｍｂｉｎａｔｉｏｎｓ：ＥＣｓ）として明示的に列挙されたものを有し、本明細書で説明する概念に従った様々な種類の実施形態の詳細な説明を提供するものである。これらの例は、相互排他的であることも、網羅的であることも、限定的であることも意図されておらず、本発明は、これらの例示的実施形態だけに限定されるものではなく、発行される特許請求の範囲およびその均等物の範囲内のすべての可能な改変形態および変形形態を包含するものである。

【００２６】

ＥＣ１）方法であって、

１若しくはそれ以上の不揮発性メモリ（Ｎｏｎ－Ｖｏｌａｔｉｌｅ Ｍｅｍｏｒｉｅｓ：ＮＶＭｓ）からデータを受け取る工程と、

前記受け取ったデータを調整する工程と、

一連の動作に従って前記調整したデータを処理する工程と、

前記処理の結果をコンピューティングホストに提供する工程と

を有し、

前記一連の動作は、

前記調整したデータを復号化する工程と、

前記復号化したデータを展開する工程と、

前記展開したデータを再暗号化する工程と、

前記再暗号化したデータを前記結果として提供する工程と

を有し、

前記展開する工程は可逆的圧縮と対称をなす工程である

方法。

【００２７】

ＥＣ２）ＥＣ１記載の方法において、前記復号化する工程は第１の復号化する工程であり、前記調整する工程は第２の復号化する工程を有するものである方法。

【００２８】

ＥＣ３）ＥＣ１記載の方法において、前記処理する工程は複数のモードのうち選択された１つのモードに従って選択され、前記一連の動作は、前記複数のモードのうち第１のモードに対応する第１の一連の動作である方法。

【００２９】

ＥＣ４）ＥＣ３記載の方法において、

第２の一連の動作は前記複数のモードのうち第２のモードに対応し、

前記第２の一連の動作は、前記展開したデータを前記結果として提供する工程を有するものである方法。

【００３０】

ＥＣ５）方法であって、

コンピューティングホストからデータを受け取る工程と、

一連の動作に従って受け取ったデータを処理する工程と、

前記処理の結果を調整して、１若しくはそれ以上の不揮発性メモリ（ＮＶＭ）に記憶することを可能にする工程と
を有し、
前記一連の動作は、
前記受け取ったデータを復号化する工程と、
前記復号化したデータを圧縮する工程と、
前記圧縮したデータを再暗号化する工程と、
前記再暗号化したデータを結果として提供する工程と
を有し、
前記圧縮する工程は可逆的である
方法。
【００３１】
ＥＣ６）ＥＣ５記載の方法において、前記調整する工程は暗号化する工程を有するものである方法。
【００３２】
ＥＣ７）ＥＣ５記載の方法において、前記処理する工程は複数のモードのうち選択された１つのモードに従って選択され、前記一連の動作は、前記複数のモードのうちの第１のモードに対応する第１の一連の動作である方法。
【００３３】
ＥＣ８）ＥＣ７記載の方法において、
第２の一連の動作は前記複数のモードのうち第２のモードに対応し、
前記第２の一連の動作は、前記圧縮したデータを前記結果として提供する工程を有する方法。
【００３４】
ＥＣ９）方法であって、
１若しくはそれ以上の不揮発性メモリ（ＮＶＭ）からデータを受け取る工程と、
前記受け取ったデータを調整する工程と、
複数のモードのうち選択された１つのモードに従って前記調整したデータを処理する工程と、
前記処理の結果をコンピューティングホストに提供する工程と
を有し、
前記複数のモードのうち第１のモードは、
前記調整したデータを復号化する工程と、
前記復号化したデータを第１の展開データとして展開する工程と、
前記第１の展開データを第１の再暗号化データとして再暗号化する工程と、
前記第１の再暗号化したデータを結果として提供する工程と
を有し、
前記複数のモードのうち第２のモードは、
前記調整したデータを第２の展開データとして展開する工程と、
前記第２の展開データを第２の再暗号化データとして再暗号化する工程と、
前記第２の再暗号化データを結果として提供する工程と
を有する方法。
【００３５】
ＥＣ１０）ＥＣ９記載の方法において、前記調整する工程は復号化する工程を有するものである方法。
【００３６】
ＥＣ１１）ＥＣ９記載の方法において、前記展開する工程は可逆的圧縮と対称をなす工程である方法。
【００３７】
ＥＣ１２）ＥＣ９記載の方法において、

前記複数のモードのうち第３のモードは、
前記第１の展開データを結果として提供する工程
を有する方法。
【００３８】
ＥＣ１３）方法であって、
コンピューティングホストからデータを受け取る工程と、
複数のモードのうち選択された１つのモードに従って、前記受け取ったデータを処理する工程と、
前記処理の結果を調整して、１若しくはそれ以上の不揮発性メモリ（ＮＶＭ）に記憶することを可能にする工程と
を有し、
前記複数のモードのうち第１のモードは、
前記受け取ったデータを復号化する工程と、
前記復号化したデータを圧縮する工程と、
前記圧縮した復号化データを再暗号化する工程と、
前記再暗号化したデータを結果として提供する工程と
を有し、
前記複数のモードのうちの第２のモードは、
前記圧縮した復号化データを結果として提供する工程
を有する方法。
【００３９】
ＥＣ１４）ＥＣ１３記載の方法において、前記調整する工程は暗号化する工程を有する方法。
【００４０】
ＥＣ１５）ＥＣ１３記載の方法において、前記再暗号化する工程は前記復号化する工程と対称をなす工程である方法。
【００４１】
ＥＣ１６）ＥＣ１３記載の方法において、前記再暗号化する工程はセキュリティプロトコルに準拠するものであり、前記復号化する工程はトランスポートプロトコルに準拠するものである方法。
【００４２】
ＥＣ１７）ＥＣ１３記載の方法において、さらに、
コンピューティングホストとトランスポートセッション暗号化鍵を安全に交換する工程と、
前記復号化する工程において前記トランスポートセッション暗号化鍵の少なくとも一部分を使用する工程と
を有するものである方法。
【００４３】
ＥＣ１８）ＥＣ１７記載の方法において、前記トランスポートセッション暗号化鍵を安全に交換する工程は、
非対称鍵交換を使用してコンピューティングホストとソリッドステートディスク（ＳＳＤ）との間でセキュアなリンクを確立する工程と、
前記セキュアなリンク内でトランスポートセッション暗号化鍵を交換する工程と
を有する方法。
【００４４】
ＥＣ１９）ＥＣ１３記載の方法において、
前記複数のモードのうち第３のモードは、
前記受け取ったデータを圧縮する工程と、
前記圧縮したデータを暗号化する工程と、
前記圧縮した暗号化データを結果として提供する工程と

を有する方法。
【００４５】
ＥＣ２０）ＥＣ１９記載の方法において、前記暗号化する工程はセキュリティプロトコルに準拠するものである方法。
【００４６】
ＥＣ２１）ＥＣ１９記載の方法において、
前記複数のモードのうち第４のモードは、
前記圧縮したデータを結果として提供する工程
を有する方法。
【００４７】
ＥＣ２２）ＥＣ１３記載の方法において、前記調整する工程は、前記結果をスクランブリングする工程、および／または前記結果を変調する工程を有する方法。
【００４８】
ＥＣ２３）ＥＣ１３記載の方法において、前記調整する工程は暗号化する工程を有する方法。
【００４９】
ＥＣ２４）ＥＣ１３記載の方法において、さらに、
記憶する工程を有するものである方法。
【００５０】
ＥＣ２５）ＥＣ２４記載の方法において、前記記憶する工程は、フラッシュ・メモリ・インターフェースを介したものである方法。
【００５１】
ＥＣ２６）ＥＣ１３記載の方法において、前記受け取る工程は、ストレージインターフェース規格と適合するストレージインターフェースを介したものである方法。
【００５２】
ＥＣ２７）ＥＣ１３記載の方法において、さらに、
コンピューティングホストにより、データを暗号化したデータとして提供する工程を有するものである方法。
【００５３】
ＥＣ２８）ＥＣ１３記載の方法において、前記復号化する工程、前記圧縮する工程、および前記再暗号化する工程は、少なくとも部分的に、ソリッドステートディスク（ＳＳＤ）のコントローラによって実施される方法。
【００５４】
ＥＣ２９）システムであって、
コンピューティングホストからデータを受け取る手段と、
複数の動作モードのうちの１つを選択的に使用可能にする手段であって、当該モードは、
暗号化動作モードであって、少なくとも部分的に、
前記受け取られたデータを復号化する手段と、
前記復号化されたデータを圧縮する手段と、
前記圧縮、且つ復号化されたデータを再暗号化する手段と、
前記再暗号化されたデータを暗号化モード書き込みデータとして提供する手段と
によって実施されるものである、前記暗号化動作モードと、
非暗号化動作モードであって、少なくと部分的に、
前記受け取られたデータを圧縮する手段と、
前記圧縮、且つ受け取られたデータを非暗号化モード書き込みデータとして提供する手段と
によって実施されるものである、前記非暗号化動作モードと
を有するものである、前記選択的に使用可能にする手段と、
前記使用可能にされたモードの書き込みデータを選択する手段と、

前記選択されたモードの書き込みデータを暗号化する手段と、
前記暗号化、且つ選択されたモードの書き込みデータを書式設定して、１若しくはそれ以上の不揮発性メモリ（ＮＶＭ）に記憶する手段と
を有するシステム。
【００５５】
ＥＣ３０）ＥＣ２９記載のシステムにおいて、さらに、
トランスポートセッション暗号化鍵を安全に交換し、トランスポートセッション暗号化鍵の少なくとも一部分を使用して前記受け取られたデータを受け取られた暗号化データとして復号化する手段を有するものであるシステム。
【００５６】
ＥＣ３１）ＥＣ２９記載のシステムにおいて、前記圧縮する手段のうちの１若しくはそれ以上は、可逆的圧縮を実行して書き込み増幅を有利に低減させることが可能であるシステム。
【００５７】
ＥＣ３２）ＥＣ２９記載のシステムにおいて、前記復号化されたデータを圧縮する手段および前記受け取られたデータを圧縮する手段は、少なくとも共通の一部分を有するものであるシステム。
【００５８】
ＥＣ３３）ＥＣ２９記載のシステムにおいて、前述の手段はソリッドステートディスク（ＳＳＤ）のコントローラを介した手段であり、前記不揮発性メモリはソリッドステートディスクに含まれるフラッシュメモリであるシステム。
【００５９】
ＥＣ３４）ＥＣ３３記載のシステムにおいて、さらに、
前記コントローラを前記コンピューティングホストとインターフェースさせる手段を有するものであるシステム。
【００６０】
ＥＣ３５）ＥＣ３４記載のシステムにおいて、前記インターフェースさせる手段は、ストレージインターフェース規格と適合するものであるシステム。
【００６１】
ＥＣ３６）ＥＣ３４記載のシステムにおいて、さらに、
前記コンピューティングホストの全部または任意選択の部分を有するものであるシステム。
【００６２】
ＥＣ３７）ＥＣ２９記載のシステムにおいて、さらに、
前記不揮発性メモリとインターフェースする手段を有するものであるシステム。
【００６３】
ＥＣ３８）ＥＣ３７記載のシステムにおいて、前記インターフェースする手段はフラッシュ・メモリ・インターフェースを有するものであるシステム。
【００６４】
ＥＣ３９）ＥＣ２９記載のシステムにおいて、さらに、
前記不揮発性メモリのうちの少なくとも１つを有するものであるシステム。
【００６５】
ＥＣ４０）ＥＣ２９記載のシステムにおいて、さらに、
前記コンピューティングホストからの要求をインターフェースする手段であって、当該要求は前記不揮発性メモリに記憶された情報に関するものである、前記要求をインターフェースする手段と、
前記不揮発性メモリとインターフェースする手段と
を有するものであるシステム。
【００６６】
ＥＣ４１）ＥＣ４０記載のシステムにおいて、前述の手段は単一の集積回路（ＩＣ）に

一括して実装されるものであるシステム。
【００６７】
ＥＣ４２）ＥＣ４０記載のシステムにおいて、前述の手段はソリッドステートディスク（ＳＳＤ）に含まれているものであるシステム。
【００６８】
ＥＣ４３）ＥＣ３０記載のシステムにおいて、前記トランスポートセッション暗号化鍵を安全に交換する手段は、
非対称鍵交換を使用してホストとソリッドステートディスク（ＳＳＤ）との間でセキュアなリンクを確立する手段と、
前記セキュアなリンク内でトランスポートセッション暗号化鍵を交換する手段と
を有するシステム。
【００６９】
ＥＣ４４）命令のセットを格納する有形のコンピュータ可読媒体であって、当該命令セットは記憶装置の処理要素によって実行されると、当該処理要素に、
コンピューティングホストからデータを受け取る工程と、
複数の動作モードのうちの１つを選択的に使用可能にする工程であって、当該モードは、
暗号化動作モードであって、少なくとも部分的に、
前記受け取ったデータを復号化する工程と、
前記復号化したデータを圧縮する工程と、
前記圧縮した復号化データを再暗号化する工程と、
前記再暗号化したデータを暗号化モード書き込みデータとして提供する工程と
によって実施されるものである、前記暗号化動作モードと、
非暗号化動作モードであって、少なくとも部分的に、
前記受け取ったデータを圧縮する工程と、
前記圧縮、且つ受け取ったデータを非暗号化モード書き込みデータとして提供する工程と
によって実施されるものである、前記非暗号化動作モードと
を有するものである、前記選択的に使用可能にする工程と、
前記使用可能となったモードの書き込みデータを選択する工程と、
前記選択したモードの書き込みデータを暗号化する工程と、
前記暗号化した選択モードの書き込みデータを書式設定して、１若しくはそれ以上の不揮発性メモリ（ＮＶＭ）に記憶する工程と
を有する動作を実行させ、および／または制御させるものである、
有形のコンピュータ可読媒体。
【００７０】
ＥＣ４５）ＥＣ４４記載の有形のコンピュータ可読媒体において、当該コンピュータ可読媒体および前記処理要素はソリッドステートディスク（ＳＳＤ）に含まれるものである有形のコンピュータ可読媒体。
【００７１】
ＥＣ４６）ＥＣ４５記載の有形のコンピュータ可読媒体において、前記不揮発性メモリのうちの少なくとも１つはソリッドステートディスクに含まれるものである有形のコンピュータ可読媒体。
【００７２】
ＥＣ４７）前記復号化する工程と、前記再暗号化する工程とを有するか、または当該工程に言及している前述のＥＣのいずれか１つにおいて、前記復号化する工程および前記再暗号化する工程のうちのいずれか１つ若しくはそれ以上はセキュアな物理境界内で実行されるものであるＥＣ。
【００７３】
ＥＣ４８）前記復号化する工程と、前記再暗号化する工程と、前記圧縮する工程と、前

記展開する工程とを有するか、または当該工程に言及している前述のＥＣのいずれか１つにおいて、前記復号化する工程、前記再暗号化する工程、前記圧縮する工程、および前記展開する工程のうちのいずれか１つ若しくはそれ以上は、セキュアな物理境界内で実行されるものであるＥＣ。

【００７４】

ＥＣ４９）セキュアな物理境界を有するか、または当該物理境界に言及している前述のＥＣのいずれか１つにおいて、前記セキュアな物理境界は単一の集積回路（ＩＣ）によって実装されるＥＣ。

【００７５】

ＥＣ５０）前記トランスポートセッション暗号化鍵を有するか、または当該暗号化鍵に言及している前述のＥＣのいずれか１つにおいて、前記トランスポートセッション暗号化鍵は、対称鍵暗号化／復号化と適合するものであるＥＣ。

【００７６】

ＥＣ５１）対称鍵暗号化／復号化を有し、またはこれに言及している前述のＥＣのいずれか１つにおいて、対称鍵暗号化／復号化は、

ＡＥＳ１２８、

ＡＥＳ１９２、および

ＡＥＳ２５６

のうちの１若しくはそれ以上と適合するものであるＥＣ。

【００７７】

ＥＣ５２）可逆的圧縮を有するか、または当該可逆的圧縮に言及している前述のＥＣのいずれか１つにおいて、当該可逆的圧縮はラムペルージフ（Ｌｅｍｐｅｌ－Ｚｉｖ：ＬＺ）圧縮を有するＥＣ。

【００７８】

ＥＣ５３）可逆的圧縮を有するか、または当該可逆的圧縮に言及している前述のＥＣのいずれか１つにおいて、当該可逆的圧縮は辞書コーダＬＺ７７圧縮を有するＥＣ。

【００７９】

ＥＣ５４）ソリッドステートディスクコントローラを有するか、または当該コントローラに言及している前述のＥＣのいずれか１つにおいて、当該ソリッドステートディスクコントローラは単一の集積回路（ＩＣ）に実装されるものであるＥＣ。

【００８０】

ＥＣ５５）ソリッドステートディスクコントローラと不揮発性メモリとを有するか、またはこれらに言及している前述のＥＣのいずれか１つにおいて、当該ソリッドステートディスクコントローラおよび不揮発性メモリはソリッドステートディスクに含まれるＥＣ。

【００８１】

ＥＣ５６）不揮発性メモリを有するか、または当該メモリに言及している前述のＥＣのいずれか１つにおいて、当該不揮発性メモリのうちの少なくとも１つは１若しくはそれ以上のフラッシュメモリを有するＥＣ。

【００８２】

ＥＣ５７）ストレージインターフェース規格を有し、またはこれに言及している前述のＥＣのいずれかにおいて、ストレージインターフェース規格は、

ユニバーサル・シリアル・バス（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ：ＵＳＢ）インターフェース規格と、

コンパクトフラッシュ（登録商標）（Ｃｏｍｐａｃｔ　Ｆｌａｓｈ：ＣＦ）インターフェース規格と、

マルチメディアカード（ＭｕｌｔｉＭｅｄｉａＣａｒｄ：ＭＭＣ）インターフェース規格と、

組み込み型ＭＭＣ（ｅＭＭＣ）インターフェース規格と、

サンダーボルトインターフェース規格と、

ＵＦＳインターフェース規格と、

セキュアデジタル（Ｓｅｃｕｒｅ　Ｄｉｇｉｔａｌ：ＳＤ）インターフェース規格と、
メモリ・スティック・インターフェース規格と、
ｘＤピクチャ・カード・インターフェース規格と、
内蔵ドライブエレクトロニクス（Ｉｎｔｅｇｒａｔｅｄ　Ｄｒｉｖｅ　Ｅｌｅｃｔｒｏｎｉｃｓ：ＩＤＥ）インターフェース規格と、
シリアル・アドバンスト・テクノロジー・アタッチメント（Ｓｅｒｉａｌ　Ａｄｖａｎｃｅｄ　Ｔｅｃｈｎｏｌｏｇｙ　Ａｔｔａｃｈｍｅｎｔ：ＳＡＴＡ）インターフェース規格と、
エクスターナルＳＡＴＡ（ｅＳＡＴＡ）インターフェース規格と、
スモール・コンピュータ・システム・インターフェース（ＳＣＳＩ）インターフェース規格と、
シリアル接続スモール・コンピュータ・システム・インターフェース（ＳＡＳ）インターフェース規格と、
ファイバー・チャンネル・インターフェース規格と、
イーサネット（登録商標）インターフェース規格と、
ペリフェラル・コンポーネント・インターコネクト・エキスプレス（Ｐｅｒｉｐｈｅｒａｌ　Ｃｏｍｐｏｎｅｎｔ　Ｉｎｔｅｒｃｏｎｎｅｃｔ　ｅｘｐｒｅｓｓ：ＰＣＩｅ）インターフェース規格と
のうちの１若しくはそれ以上のものを有するものであるＥＣ。

【００８３】

ＥＣ５８）フラッシュ・メモリ・インターフェースを有するか、または当該インターフェースに言及している前述のＥＣのいずれか１つにおいて、当該フラッシュ・メモリ・インターフェースは、
オープンＮＡＮＤフラッシュインターフェース（ＯＮＦＩ）、
トグルモードインターフェース、
ダブルデータレート（ＤＤＲ）同期インターフェース、
ＤＤＲ２同期インターフェース、
同期インターフェース、および
非同期インターフェース
のうちの１若しくはそれ以上と適合するものであるＥＣ。

【００８４】

ＥＣ５９）コンピューティングホストを有し、またはこれに言及している前述のＥＣのいずれかにおいて、コンピューティングホストは、
コンピュータと、
ワークステーションコンピュータと、
サーバコンピュータと、
ストレージサーバと、
ストレージ・アタッチト・ネットワーク（Ｓｔｏｒａｇｅ　Ａｔｔａｃｈｅｄ　Ｎｅｔｗｏｒｋ：ＳＡＮ）と、
ネットワーク・アタッチト・ストレージ（Ｎｅｔｗｏｒｋ　Ａｔｔａｃｈｅｄ　Ｓｔｏｒａｇｅ：ＮＡＳ）デバイスと、
ダイレクト・アタッチト・ストレージ（Ｄｉｒｅｃｔ　Ａｔｔａｃｈｅｄ　Ｓｔｏｒａｇｅ：ＤＡＳ）デバイスと、
ストレージアプライアンスと、
パーソナルコンピュータ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ：ＰＣ）と、
ラップトップコンピュータと、
ノートブックコンピュータと、
ネットブックコンピュータと、
タブレットデバイス又はタブレットコンピュータと、
ウルトラブックコンピュータと、

電子書籍端末（電子読み出し機）と、
携帯端末（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ：ＰＤＡ）と、
ナビゲーションシステムと、
（ハンドヘルド）グローバル・ポジショニング・システム（Ｇｌｏｂａｌ　Ｐｏｓｉｔｉｏｎｉｎｇ　Ｓｙｓｔｅｍ：ＧＰＳ）デバイスと、
自動車制御システムと、
自動車媒体制御システム及び自動車媒体制御コンピュータと、
プリンタ、コピー機、若しくはＦＡＸ機、又はオールインワンデバイスと、
販売時点情報管理ＰＯＳデバイスと、
金銭登録機と、
メディアプレイヤと、
テレビと、
メディアレコーダと、
デジタル・ビデオ・レコーダ（Ｄｉｇｉｔａｌ　Ｖｉｄｅｏ　Ｒｅｃｏｒｄｅｒ：ＤＶＲ）と、
デジタルカメラと、
セル方式送受話器と、
コードレス電話の送受話器と、
電子ゲームと
のうちの１若しくはそれ以上のものを有するものであるＥＣ。

【００８５】
ＥＣ６０）少なくとも１つのフラッシュメモリを有するか、または当該フラッシュメモリに言及している前述のＥＣのいずれか１つにおいて、少なくとも１つのフラッシュメモリの少なくとも一部分は、
ＮＡＮＤフラッシュ技術記憶セル、および
ＮＯＲフラッシュ技術記憶セル
のうちの１若しくはそれ以上を有するＥＣ。

【００８６】
ＥＣ６１）少なくとも１つのフラッシュメモリを有するか、または当該フラッシュメモリに言及している前述のＥＣのいずれか１つにおいて、当該フラッシュメモリの少なくとも一部分は、
シングルレベルセル（ＳＬＣ）フラッシュ技術記憶セル、および
マルチレベルセル（ＭＬＣ）フラッシュ技術記憶セル
のうちの１若しくはそれ以上を有するＥＣ。

【００８７】
ＥＣ６２）少なくとも１つのフラッシュメモリを有するか、または当該フラッシュメモリに言及している前述のＥＣのいずれか１つにおいて、当該フラッシュメモリの少なくとも一部分は、
多結晶シリコン技術ベースの電荷蓄積セル、および
シリコン窒化膜技術ベースの電荷蓄積セル
のうちの１若しくはそれ以上を有するＥＣ。

【００８８】
ＥＣ６３）少なくとも１つのフラッシュメモリを有するか、または当該フラッシュメモリに言及している前述のＥＣのいずれかにおいて、当該フラッシュメモリの少なくとも一部分は、
２次元技術ベースのフラッシュメモリ技術、および
３次元技術ベースのフラッシュメモリ技術
のうちの１若しくはそれ以上を有するＥＣ。

【００８９】
システム

図１Ａは、ＮＶＭ要素（フラッシュメモリなど）によって実施されるような不揮発性記憶を管理するためのトランスポート暗号化層を使用するＳＳＤコントローラを含むＳＳＤ（１０１）の実施形態の選択された詳細を図示する。ＳＳＤコントローラはＮＶＭ要素（例えば、フラッシュメモリ）を介して実装される不揮発性ストレージなどの不揮発性ストレージを管理するためのものである。ＳＳＤコントローラ１００は１若しくはそれ以上の外部インターフェース１１０を介してホスト（図示せず）に通信するように結合される。様々な実施形態に従って、外部インターフェース１１０は、ＳＡＴＡインターフェース、ＳＡＳインターフェース、ＰＩＣｅインターフェース、ファイバー・チャンネル・インターフェース、イーサネット（登録商標）インターフェース（例えば、１０ギガビットのイーサネット（登録商標））、上記のインターフェースのうちのいずれかの規格外版、若しくは特注のインターフェース、又はストレージ及び／又は通信機器及び／又は計算デバイスを相互接続するために使用されるその他任意の種類のインターフェースのうちの１若しくはそれ以上である。例えば、一部の実施形態において、ＳＳＤコントローラ１００はＳＡＴＡインターフェースとＰＣＩｅインターフェースとを含む。

【００９０】

ＳＳＤコントローラ１００は、さらに、１つ若しくはそれ以上のデバイスインターフェース１９０を介して、１つ若しくはそれ以上のフラッシュデバイス１９２といった、１つ若しくはそれ以上の記憶デバイスを含むＮＶＭ１９９に通信可能に結合されている。様々な実施形態によれば、デバイスインターフェース１９０は、非同期インターフェース、同期インターフェース、シングルデータレート（ＳＤＲ）インターフェース、ダブルデータレート（ＤＤＲ）インターフェース、ＤＲＡＭ互換ＤＤＲ若しくはＤＤＲ２同期インターフェース、ＯＮＦＩ２．２やＯＮＦＩ３．０互換インターフェースといったＯＮＦＩ互換インターフェース、トグルモード互換フラッシュインターフェース、上記のインターフェースのいずれかの非標準バージョン、カスタムインターフェース、または記憶デバイスに接続するのに使用される任意の他の種類のインターフェースのうちの１つ若しくはそれ以上である。

【００９１】

各フラッシュデバイス１９２は、一部の実施形態では、１つ若しくはそれ以上の個々のフラッシュダイ１９４を有する。フラッシュデバイス１９２のうちの特定のフラッシュデバイスの種類に従って、特定のフラッシュデバイス１９２内の複数のフラッシュダイ１９４に、並列に、任意選択で、かつ／または選択的にアクセスすることができる。フラッシュデバイス１９２は、単に、ＳＳＤコントローラ１００に通信可能に結合することができるようにした記憶デバイスの一種を表しているにすぎない。様々な実施形態では、ＳＬＣ　ＮＡＮＤフラッシュメモリ、ＭＬＣ　ＮＡＮＤフラッシュメモリ、ＮＯＲフラッシュメモリ、多結晶シリコン若しくはシリコン窒化膜技術ベースの電荷蓄積セルを使用したフラッシュメモリ、２次元若しくは３次元技術ベースのフラッシュメモリ、読み出し専用メモリ、スタティック・ランダム・アクセス・メモリ、ダイナミック・ランダム・アクセス・メモリ、強磁性メモリ、相変化メモリ、レーストラックメモリ、または任意の他の種類のメモリデバイス若しくは記憶媒体といった、任意の種類の記憶デバイスを使用することができる。

【００９２】

様々な実施形態によれば、デバイスインターフェース１９０は、１つのバスにつき１つ若しくはそれ以上のフラッシュデバイス１９２を有する１つ若しくはそれ以上のバス；グループ内のバスにおおむね並列にアクセスさせる、１つのバスにつき１つ若しくはそれ以上のフラッシュデバイス１９２を有する１つ若しくはそれ以上のバスグループ；またはデバイスインターフェース１９０上へのフラッシュデバイス１９２の１つ若しくはそれ以上のインスタンスの任意の他の編成として編成される。

【００９３】

引き続き図１Ａにおいて、ＳＳＤコントローラ１００は、ホストインターフェース１１１、データ処理１２１、バッファ１３１、マップ１４１、リサイクラ１５１、ＥＣＣ１６

１、デバイスインターフェース論理１９１、ＣＰＵ１７１といった１つ若しくはそれ以上のモジュールを有する。図１Ａに図示する具体的なモジュールおよび相互接続は、単に、一実施形態を表すにすぎず、これらのモジュールの一部または全部、および図示されていないさらに別のモジュールの多くの配置および相互接続が考えられる。第１の例として、一部の実施形態では、デュアルポーティングを提供するための２つ以上のホストインターフェース１１１がある。第２の例として、一部の実施形態では、データ処理１２１および／またはＥＣＣ１６１がバッファ１３１と組み合わされている。第３の例として、一部の実施形態では、ホストインターフェース１１１がバッファ１３１に直接結合されており、データ処理１２１が、バッファ１３１に記憶されたデータに任意選択で、かつ／または選択的に作用する。第４の例として、一部の実施形態では、デバイスインターフェース論理１９１がバッファ１３１に直接結合されており、ＥＣＣ１６１が、バッファ１３１に記憶されたデータに任意選択で、かつ／または選択的に作用する。

【００９４】

ホストインターフェース１１１は、外部インターフェース１１０を介してコマンドおよび／またはデータを送受信し、一部の実施形態では、タグ追跡１１３によって個々のコマンドの進捗を追跡する。例えば、コマンドは、読み出すべきアドレス（ＬＢＡなど）およびデータの量（ＬＢＡ量、例えばセクタの数など）を指定する読み出しコマンドを含み、これに応答してＳＳＤは、読み出し状況および／または読み出しデータを提供する。別の例として、コマンドは、書き込むべきアドレス（ＬＢＡなど）およびデータの量（ＬＢＡ量、例えばセクタの数など）を指定する書き込みコマンドを含み、これに応答してＳＳＤは、書き込み状況を提供し、かつ／または書き込みデータを要求し、任意選択でその後に書き込み状況を提供する。さらに別の例として、コマンドは、もはや割り当てられる必要のなくなった１つ若しくはそれ以上のアドレス（１つ若しくはそれ以上のＬＢＡなど）を指定する割り当て解除コマンド（ｔｒｉｍコマンドなど）を含み、これに応答してＳＳＤは、マップをしかるべく変更し、任意選択で割り当て解除状況を提供する。あるコンテキストでは、ＡＴＡ互換ＴＲＩＭコマンドが割り当て解除コマンドの例である。さらに別の例として、コマンドは、超コンデンサ・テスト・コマンドまたはデータハーデニング成功問い合わせを含み、これに応答してＳＳＤは、適切な状況を提供する。一部の実施形態では、ホストインターフェース１１１は、ＳＡＴＡプロトコルと適合し、ＮＣＱコマンドを使用して、最高３２までの未処理のコマンドを有することができるようになっており、各コマンドは０から３１までの数として表された一意のタグを有する。一部の実施形態では、タグ追跡１１３は、外部インターフェース１１０を介して受け取ったコマンドのための外部タグを、ＳＳＤコントローラ１００による処理の間にコマンドを追跡するのに使用される内部タグと関連付けることができるようになっている。

【００９５】

様々な実施形態によれば、データ処理１２１は、任意選択で、かつ／または選択的に、バッファ１３１と外部インターフェース１１０との間で送られる一部または全部のデータを処理する、およびデータ処理１２１は、任意選択で、かつ／または選択的に、バッファ１３１に記憶されたデータを処理する、以下のうちの１つ若しくはそれ以上が行われる。一部の実施形態では、データ処理１２１は、１つ若しくはそれ以上のエンジン１２３を使用して、書式設定、書式設定の変更、符号変換、ならびに他のデータ処理および／または操作タスクのうちの１つ若しくはそれ以上を行う。

【００９６】

バッファ１３１は、外部インターフェース１１０からデバイスインターフェース１９０へ／デバイスインターフェース１９０から外部インターフェース１１０へ送られたデータを記憶する。一部の実施形態では、バッファ１３１は、さらに、ＳＳＤコントローラ１００によって１つ若しくはそれ以上のフラッシュデバイス１９２を管理するのに使用される、一部または全部のマップ表といったシステムデータも記憶する。様々な実施形態では、バッファ１３１は、データの一時記憶に使用されるメモリ１３７、バッファ１３１への、かつ／またはバッファ１３１からのデータの移動を制御するのに使用されるＤＭＡ１３３

、ならびに高レベル誤り訂正および／または冗長性機能と、他のデータ移動および／または操作機能とを提供するのに使用されるＥＣＣ－Ｘ１３５のうちの１つ若しくはそれ以上を有する。高レベル冗長性機能の一例がＲＡＩＤ様の能力であり、ディスクレベルではなく、フラッシュ・デバイス（フラッシュデバイス１９２のうちの複数のものなど）レベルおよび／またはフラッシュダイ（フラッシュダイ１９４など）レベルの冗長性を備える。

【００９７】

様々な実施形態によれば、以下のうちの１つ若しくはそれ以上である。ＥＣＣ１６１は、任意選択で、かつ／または選択的に、バッファ１３１とデバイスインターフェース１９０との間で送られる一部または全部のデータを処理する；およびＥＣＣ１６１は、任意選択で、かつ／または選択的に、バッファ１３１に記憶されたデータを処理する。一部の実施形態では、ＥＣＣ１６１は、例えば１つ若しくはそれ以上のＥＣＣ技法に従った低レベル誤り訂正および／または冗長性機能を提供するのに使用される。一部の実施形態では、ＥＣＣ１６１は、ＣＲＣ符号、ハミング符号、ＲＳ符号、ＢＣＨ符号、ＬＤＰＣ符号、ビタビ符号、トレリス符号、硬判定符号、軟判定符号、消去ベースの符号、任意の誤り検出および／または訂正符号、ならびに上記の任意の組み合わせのうちの１つ若しくはそれ以上を実施する。一部の実施形態では、ＥＣＣ１６１は、１つ若しくはそれ以上の復号器（ＬＤＰＣ復号器など）を含む。

【００９８】

デバイスインターフェース論理１９１は、デバイスインターフェース１９０を介してフラッシュデバイス１９２のインスタンスを制御する。デバイスインターフェース論理１９１は、フラッシュデバイス１９２のプロトコルに従ってフラッシュデバイス１９２のインスタンスへ／からデータを送ることができるようになっている。デバイスインターフェース論理１９１は、デバイスインターフェース１９０を介したフラッシュデバイス１９２のインスタンスの制御を選択的に配列するスケジューリング１９３を含む。例えば、一部の実施形態では、スケジューリング１９３は、フラッシュデバイス１９２のインスタンスへの操作を待ち行列に入れ、フラッシュデバイス１９２（またはフラッシュダイ１９４）のインスタンスの個々のインスタンスへの操作を、フラッシュデバイス１９２（またはフラッシュダイ１９４）のインスタンスの個々のインスタンスが利用可能になるに従って選択的に送ることができるようになっている。

【００９９】

マップ１４１は、外部インターフェース１１０上で使用されるデータアドレス指定と、デバイスインターフェース１９０上で使用されるデータアドレス指定との間の変換を行い、表１４３を使用して外部データアドレスからＮＶＭ１９９内の位置へマップする。例えば、一部の実施形態では、マップ１４１は、外部インターフェース１１０上で使用されるＬＢＡを、表１４３によって提供されるマッピングにより、１つ若しくはそれ以上のフラッシュダイ１９４を対象とするブロックおよび／またはページアドレスに変換する。ドライブ製造または割り当て解除以来一度も書き込まれていないＬＢＡでは、マップは、ＬＢＡが読み取出された場合に返すべきデフォルト値を指し示す。例えば、割り当て解除コマンドを処理するときに、マップは、割り当て解除されたＬＢＡに対応するエントリがデフォルト値のうちの１つを指し示すように変更される。様々な実施形態では、様々なデフォルト値があり、各々が対応するポインタを有する。複数のデフォルト値は、ある（例えば第１の範囲内の）割り当て解除されたＬＢＡを１つのデフォルト値として読み出し、ある（例えば第２の範囲内の）割り当て解除されたＬＢＡを別のデフォルト値として読み出すことを可能にする。デフォルト値は、様々な実施形態では、フラッシュメモリ、ハードウェア、ファームウェア、コマンドおよび／若しくはプリミティブ引数および／若しくはパラメータ、プログラマブルレジスタ、またはそれらの様々な組み合わせによって定義される。

【０１００】

一部の実施形態では、マップ１４１は、表１４３を使用して、外部インターフェース１１０上で使用されるアドレスと、デバイスインターフェース１９０上で使用されるデータ

アドレス指定との間の変換を行い、かつ／またはルックアップする。様々な実施形態によれば、表１４３は、１レベルマップ、２レベルマップ、マルチレベルマップ、マップキャッシュ、圧縮マップ、あるアドレス空間から別のアドレス空間への任意の種類のマッピング、および上記の任意の組み合わせのうちの１つ若しくはそれ以上である。様々な実施形態によれば、表１４３は、スタティック・ランダム・アクセス・メモリ、ダイナミック・ランダム・アクセス・メモリ、ＮＶＭ（フラッシュメモリなど）、キャッシュメモリ、オンチップメモリ、オフチップメモリ、および上記の任意の組み合わせのうちの１つ若しくはそれ以上を含む。

【０１０１】

一部の実施形態では、リサイクラ１５１は、ガーベジコレクションを行う。例えば、一部の実施形態では、フラッシュデバイス１９２のインスタンスは、ブロックが書き換え可能になる前に消去されなければならないブロックを含む。リサイクラ１５１は、例えば、マップ１４１によって維持されるマップをスキャンすることによって、フラッシュデバイス１９２のインスタンスのどの部分が実際に使用されているか（例えば、割り当て解除されているのではなく割り当てられていること）を決定し、フラッシュデバイス１９２のインスタンスの未使用の（例えば割り当て解除された）部分を消去することによって書き込みに利用できるようにすることができるようになっている。別の実施形態では、リサイクラ１５１は、フラッシュデバイス１９２のインスタンスのより大きい連続した部分を書き込みに利用できるようにするために、フラッシュデバイス１９２のインスタンス内に記憶されたデータを移動することができるようになっている。

【０１０２】

一部の実施形態では、フラッシュデバイス１９２のインスタンスは、異なる種類および／または属性のデータを記憶するための１つ若しくはそれ以上のバンドを保持するように、選択的に、かつ／または動的に構成され、管理され、かつ／または使用される。バンドの数、配置、サイズ、および種類は、動的に変更可能である。例えば、コンピューティングホストからのデータはホット（アクティブな）バンドに書き込まれ、リサイクラ１５１からのデータはコールド（あまりアクティブではない）バンドに書き込まれる。ある使用シナリオでは、コンピューティングホストが長い順次のストリームを書き込む場合には、ホットバンドのサイズが増加し、コンピューティングホストがランダムな書き込みを行い、またはわずかな書き込みしか行わない場合には、コールドバンドのサイズが増加する。

【０１０３】

ＣＰＵ１７１は、ＳＳＤコントローラ１００の様々な部分を制御する。ＣＰＵ１７１は、ＣＰＵコア１７２を含む。ＣＰＵコア１７２は、様々な実施形態によれば、１つ若しくはそれ以上のシングルコアプロセッサまたはマルチコアプロセッサである。ＣＰＵコア１７２内の個々のプロセッサコアは、一部の実施形態では、マルチスレッド化されている。ＣＰＵコア１７２は、命令および／またはデータのキャッシュおよび／またはメモリを含む。例えば、命令メモリは、ＣＰＵコア１７２が、ＳＳＤコントローラ１００を制御するためのプログラム（ファームウェアとも呼ばれるソフトウェアなど）を実行することを可能にする命令を含む。一部の実施形態では、ＣＰＵコア１７２によって実行されるファームウェアの一部または全部が、（例えば、図１ＢのＮＶＭ１９９のファームウェア１０６として図示されている）フラッシュデバイス１９２のインスタンス上に記憶される。

【０１０４】

様々な実施形態では、ＣＰＵ１７１は、外部インターフェース１１０を介して受け取られるコマンドを、コマンドが進行している間に追跡し、制御するコマンド管理１７３、バッファ１３１の割り当ておよび使用を制御するバッファ管理１７５、マップ１４１を制御する変換管理１７７、データアドレス指定の整合性を制御し、例えば、外部データアクセスと再利用データアクセスとの間の矛盾を回避するコヒーレンシ管理１７９、デバイスインターフェース論理１９１を制御するデバイス管理１８１、識別情報の変更および通信を制御する識別情報管理１８２、ならびに、任意選択で、他の管理部をさらに含む。ＣＰＵ１７１によって果たされる管理機能は、そのいずれか、若しくは全部が、ハードウェア、

ソフトウェア（ＣＰＵコア１７２上や、外部インターフェース１１０を介して接続されたホスト上で実行されるファームウェアなど）、またはそれらの任意の実施形態によって制御され、かつ／または管理され、あるいは、そのどれも、制御も管理もされないものである。

【０１０５】

一部の実施形態では、ＣＰＵ１７１は、性能統計の収集および／または報告、ＳＭＡＲＴの実施、電源逐次開閉機構の制御、電力消費の制御および／または調整、電源障害への応答、クロック速度の制御および／またはモニタリングおよび／または調整、ならびに他の管理タスクのうちの１つ若しくはそれ以上といった、他の管理タスクを行うことができるようになっている。

【０１０６】

様々な実施形態は、ＳＳＤコントローラ１００と同様の、例えば、ホストインターフェース１１１および／または外部インターフェース１１０の適応による、様々なコンピューティングホストを用いた動作と適合するコンピューティングホスト・フラッシュ・メモリ・コントローラを含む。様々なコンピューティングホストは、コンピュータ、ワークステーションコンピュータ、サーバコンピュータ、ストレージサーバ、ＳＡＮ、ＮＡＳデバイス、ＤＡＳデバイス、ストレージアプライアンス、ＰＣ、ラップトップコンピュータ、ノートブックコンピュータ、ネットブックコンピュータ、タブレット機器またはタブレットコンピュータ、ウルトラブックコンピュータ、電子読み出し装置（ｅ－ｒｅａｄｅｒなど）、ＰＤＡ、ナビゲーションンシステム、（ハンドヘルド型）ＧＰＳ機器、自動通信路制御システム、自動車媒体制御システムまたはコンピュータ、プリンタ、コピー機またはファックス機またはオールインワン機器、ＰＯＳ機器、金銭登録機、メディアプレーヤ、テレビ、メディアレコーダ、ＤＶＲ、ディジタルカメラ、セルラハンドセット、コードレス電話機ハンドセット、および電子ゲームのうちの１つまたはそれらの任意の組み合わせを含む。

【０１０７】

様々な実施形態では、ＳＳＤコントローラ（またはコンピューティングホスト・フラッシュ・メモリ・コントローラ）の全部または任意の部分が、単一のＩＣ、マルチダイＩＣの単一のダイ、マルチダイＩＣの複数のダイ、または複数のＩＣ上で実施される。例えば、バッファ１３１は、ＳＳＤコントローラ１００の他の要素と同じダイ上に実施される。別の例では、バッファ１３１は、ＳＳＤコントローラ１００の他の要素と異なるダイ上に実施される。

【０１０８】

図１Ｂに、図１ＡのＳＳＤの１つ若しくはそれ以上のインスタンスを含むシステムの様々な実施形態の選択された詳細を図示する。ＳＳＤ１０１は、デバイスインターフェース１９０を介してＮＶＭ１９９に結合されたＳＳＤコントローラ１００を含む。図には、様々な種別の実施形態、すなわち、ホストに直接結合された単一のＳＳＤ、各々がそれぞれの外部インターフェースを介してホストに直接それぞれ結合されている複数のＳＳＤ、および様々な相互接続要素を介してホストに間接的に結合された１つ若しくはそれ以上のＳＳＤが示されている。

【０１０９】

ホストに直接結合された単一のＳＳＤの例示的実施形態としては、ＳＳＤ１０１の１つのインスタンスが、外部インターフェース１１０を介してホスト１０２に直接結合される（例えば、スイッチ／ファブリック／中間コントローラ１０３が省かれ、バイパスされ、またはパススルーされる）。各々がそれぞれの外部インターフェースを介してホストに直接結合されている複数のＳＳＤの例示的実施形態としては、ＳＳＤ１０１の複数のインスタンスの各々が、外部インターフェース１１０のそれぞれのインスタンスを介してホスト１０２に直接それぞれ結合される（例えば、スイッチ／ファブリック／中間コントローラ１０３が省かれ、バイパスされ、またはパススルーされる）。様々な相互接続要素を介してホストに間接的に結合された１つ若しくはそれ以上のＳＳＤの例示的実施形態としては

、ＳＳＤ１０１の１つ若しくはそれ以上のインスタンスの各々が、ホスト１０２に間接的にそれぞれ結合される。各間接結合は、スイッチ／ファブリック／中間コントローラ１０３に結合された外部インターフェース１１０のそれぞれのインスタンス、およびホスト１０２に結合する中間インターフェース１０４を介したものである。

【０１１０】

スイッチ／ファブリック／中間コントローラ１０３を含む実施形態の一部は、メモリインターフェース１８０を介して結合された、ＳＳＤによってアクセス可能なカードメモリ１１２Ｃも含む。様々な実施形態では、ＳＳＤ、スイッチ／ファブリック／中間コントローラ、および／またはカードメモリのうちの１つ若しくはそれ以上が、物理的に識別可能なモジュール、カード、または差し込み可能な要素（入出力カード１１６など）上に含まれる。一部の実施形態では、ＳＳＤ１０１（またはその変形）は、ホスト１０２として動作するイニシエータ（開始プログラム）に結合されたＳＡＳドライブまたはＳＡＴＡドライブに対応する。

【０１１１】

ホスト１０２は、ＯＳ１０５、ドライバ１０７、アプリケーション１０９、マルチデバイス管理ソフトウェア１１４の様々な組み合わせといった、ホストソフトウェア１１５の様々な要素を実行することができるようになっている。点線矢印１０７Ｄは、ホストソフトウェア←→入出力装置通信、例えば、ＳＳＤ１０１のインスタンスのうちの１つ若しくはそれ以上から／へ、ドライバ１０７を介したＯＳ１０５、ドライバ１０７、および、ドライバ１０７を介して、またはＶＦとして直接アプリケーション１０９のうちの任意の１つ若しくはそれ以上へ／から送られ／受け取られるデータを表す。

【０１１２】

ＯＳ１０５は、ＳＳＤとインターフェースするための（概念的にはドライバ１０７によって図示されている）ドライバを含み、かつ／またはそのようなドライバを用いて動作することができるようになっている。Ｗｉｎｄｏｗｓ（登録商標）の様々なバージョン（９５、９８、ＭＥ、ＮＴ、ＸＰ、２０００、サーバ、Ｖｉｓｔａ、および７など）、Ｌｉｎｕｘ（登録商標）の様々なバージョン（Ｒｅｄ　Ｈａｔ、Ｄｅｂｉａｎ、およびＵｂｕｎｔｕなど）、ならびにＭａｃＯＳの様々なバージョン（８、９およびＸなど）がＯＳ１０５の例である。様々な実施形態では、ドライバは、ＳＡＴＡ、ＡＨＣＩ、ＮＶＭ　Ｅｘｐｒｅｓｓといった標準のインターフェースおよび／またはプロトコルを用いて動作する標準のドライバおよび／または汎用のドライバ（「シュリンクラップされた（市販の）」または「プリインストールされた」ともいう）であり、あるいは、任意選択で、ＳＳＤ１０１に特有のコマンドの使用を可能にするようにカスタマイズされており、かつ／またはベンダ特有のものである。あるドライブおよび／またはドライバは、アプリケーションレベルのプログラム、例えば最適化ＮＡＮＤアクセス（Ｏｐｔｉｍｉｚｅｄ　ＮＡＮＤ　Ａｃｃｅｓｓ）（ＯＮＡともいう）または直接ＮＡＮＤアクセス（Ｄｉｒｅｃｔ　ＮＡＮＤ　Ａｃｃｅｓｓ）（ＤＮＡともいう）の各技法によるアプリケーション１０９などが、コマンドをＳＳＤ１０１に直接伝えることを可能にするパススルーモードを有し、カスタマイズされたアプリケーションが、汎用ドライバとでさえもＳＳＤ１０１に特有のコマンドを使用することを可能にする。ＯＮＡの技法は、非標準変更子（ｈｉｎｔｓ）の使用、ベンダ特有のコマンドの使用、非標準の統計の通信、例えば圧縮可能性に従った実際のＮＶＭの使用、および他の技法のうちの１つ若しくはそれ以上を含む。ＤＮＡの技法は、ＮＶＭへのマップされていない読み出し、書き込み、および／または消去アクセスを提供する非標準のコマンドまたはベンダ特有の（コマンド）の使用、例えば、入出力装置が通常は行うはずのデータの書式設定をバイパスすることによる、ＮＶＭへのより直接的なアクセスを提供する非標準の、またはベンダ特有のコマンドの使用、および他の技法のうちの１つ若しくはそれ以上を含む。ドライバの例は、ＯＮＡまたはＤＮＡサポートなしのドライバ、ＯＮＡ使用可能ドライバ、ＤＮＡ使用可能ドライバ、ＯＮＡ／ＤＮＡ使用可能ドライバである。ドライバの別の例は、ベンダ提供ドライバ、ベンダ開発ドライバ、および／またはベンダ拡張ドライバ、ならびにクライアント提供ドライバ、クライアント開発ドライバ

、および／またはクライアント拡張ドライバである。

【０１１３】

アプリケーションレベルのプログラムの例は、ＯＮＡまたはＤＮＡサポートなしのアプリケーション、ＯＮＡ使用可能アプリケーション、ＤＮＡ使用可能アプリケーション、およびＯＮＡ／ＤＮＡ使用可能アプリケーションである。点線矢印１０９Ｄは、アプリケーション←→入出力装置通信（ドライバによるバイパスや、アプリケーションのためのＶＦによるバイパスなど）、例えば、ＯＳを仲介として使用するアプリケーションなしでＳＳＤと通信するＯＮＡ使用可能アプリケーションおよびＯＮＡ使用可能ドライバなどを表す。点線矢印１０９Ｖは、アプリケーション←→入出力装置通信（アプリケーションのためのＶＦによるバイパスなど）、例えば、ＯＳまたはドライバを仲介として使用するアプリケーションなしでＳＳＤと通信するＤＮＡ使用可能アプリケーションおよびＤＮＡ使用可能ドライバなどを表す。

【０１１４】

ＮＶＭ１９９の１つ若しくはそれ以上の部分が、一部の実施形態では、ファームウェア記憶、例えばファームウェア１０６に使用される。ファームウェア記憶は、１つ若しくはそれ以上のファームウェアイメージ（またはその部分）を含む。ファームウェアイメージは、例えばＳＳＤコントローラ１００のＣＰＵコア１７２によって実行される、例えばファームウェアの１つ若しくはそれ以上のイメージを有する。ファームウェアイメージは、別の例では、例えばファームウェア実行時にＣＰＵコアによって参照される、定数、パラメータ値、ＮＶＭデバイス情報の１つ若しくはそれ以上のイメージを有する。ファームウェアのイメージは、例えば、現在のファームウェアイメージおよび０以上の（ファームウェア更新に対して）前のファームウェアイメージに対応する。様々な実施形態では、ファームウェアは、汎用動作モード、標準動作モード、ＯＮＡ動作モード、および／またはＤＮＡ動作モードを提供する。一部の実施形態では、ファームウェア動作モードのうちの１つ若しくはそれ以上が、ドライバによって任意選択で伝えられ、かつ／または提供される、鍵または様々なソフトウェア技法によって使用可能とされる（例えば、１つ若しくはそれ以上のＡＰＩが「ロック解除」される）。

【０１１５】

スイッチ／ファブリック／中間コントローラを欠く一部の実施形態では、ＳＳＤは、外部インターフェース１１０を介して直接ホストに結合される。様々な実施形態では、ＳＳＤコントローラ１００は、ＲＡＩＤコントローラといった他のコントローラの１つ若しくはそれ以上の中間レベルを介してホストに結合される。一部の実施形態では、ＳＳＤ１０１（またはその変形）は、ＳＡＳドライブまたはＳＡＴＡドライブに対応し、スイッチ／ファブリック／中間コントローラ１０３は、イニシエータにさらに結合されたエキスパンダに対応し、あるいは、スイッチ／ファブリック／中間コントローラ１０３は、エキスパンダを介してイニシエータに間接的に結合されたブリッジに対応する。一部の実施形態では、スイッチ／ファブリック／中間コントローラ１０３は、１つ若しくはそれ以上のＰＣＩｅスイッチおよび／またはファブリックを含む。

【０１１６】

様々な実施形態、例えば、コンピューティングホストとしてのホスト１０２（コンピュータ、ワークステーションコンピュータ、サーバコンピュータ、ストレージサーバ、ＳＡＮ、ＮＡＳデバイス、ＤＡＳデバイス、ストレージアプライアンス、ＰＣ、ラップトップコンピュータ、ノートブックコンピュータ、および／またはネットブックコンピュータなど）を有する実施形態のあるものでは、コンピューティングホストは、任意選択で、１つ若しくはそれ以上のローカルサーバおよび／またはリモートサーバ（例えば、任意選択のサーバ１１８）と（例えば、任意選択の入出力装置／リソースおよび記憶装置／リソース１１７および任意選択のＬＡＮ／ＷＡＮ１１９を介して）通信することができるようになっている。通信は、例えば、ＳＳＤ１０１要素のうちの任意の１つ若しくはそれ以上のローカルおよび／またはリモートのアクセス、管理、および／または使用を可能にする。一部の実施形態では、通信は、全部または一部がイーサネット（登録商標）（Ｅｔｈｅｒｎ

ｅｔ（登録商標））によるものである。一部の実施形態では、通信は、全部または一部がファイバチャネルによるものである。ＬＡＮ／ＷＡＮ１１９は、様々な実施形態では、１つ若しくはそれ以上のローカル・エリア・ネットワークおよび／または広域ネットワーク、例えば、サーバファーム内のネットワーク、サーバファームを結合するネットワーク、メトロエリアネットワーク、およびインターネットのうちの任意の１つ若しくはそれ以上を表す。

【０１１７】

様々な実施形態では、１つ若しくはそれ以上のＮＶＭと組み合わされたＳＳＤコントローラおよび／またはコンピューティングホスト・フラッシュ・メモリ・コントローラが、ＵＳＢ記憶コンポーネント、ＣＦ記憶コンポーネント、ＭＭＣ記憶コンポーネント、ｅＭＭＣ記憶コンポーネント、サンダーボルト記憶コンポーネント、ＵＦＳ記憶コンポーネント、ＳＤ記憶コンポーネント、メモリスティック記憶コンポーネント、ｘＤピクチャカード記憶コンポーネントといった不揮発性記憶コンポーネントとして実施される。

【０１１８】

様々な実施形態では、ＳＳＤコントローラ（またはコンピューティングホスト・フラッシュ・メモリ・コントローラ）の全部またはいずれかの部分、またはその機能が、コントローラが結合されるべきホスト（図１Ｂのホスト１０２など）において実施される。様々な実施形態では、ＳＳＤコントローラ（若しくはコンピューティングホスト・フラッシュ・メモリ・コントローラ）の全部またはいずれかの部分、またはその機能が、ハードウェア（論理回路など）、ソフトウェアおよび／若しくはファームウェア（ドライバソフトウェア若しくはＳＳＤ制御ファームウェアなど）、またはそれらの任意の組み合わせによって実施される。例えば、（例えば図１ＡのＥＣＣ１６１および／またはＥＣＣ－Ｘ１３５と同様の）ＥＣＣ部の、またはＥＣＣ部と関連付けられた機能が、一部はホスト上のソフトウェアによって、一部はＳＳＤコントローラ内のファームウェアとハードウェアとの組み合わせによって実施される。別の例として、（例えば図１Ａのリサイクラ１５１と同様の）リサイクラ部の、またはリサイクラ部と関連付けられた機能が、一部はホスト上のソフトウェアによって、一部はコンピューティングホスト・フラッシュ・メモリ・コントローラ内のハードウェアによって実施される。

【０１１９】

トランスポート暗号化の使用法および動作の例

図２に、図１Ａに示すような不揮発性記憶を管理するための暗号化トランスポートの技法を使用した暗号化トランスポートＳＳＤ２００の具体的応用の一例を示す。コンピュータ２０２は、後でインターネット経由でリモートサーバ２０４からダウンロードされ、暗号化トランスポートＳＳＤ２００上に一時的に記憶され、閲覧するためのＶＧＡディスプレイ２０６に送られるペイパービュー映画を選択し、そのレンタル料の支払いを行うのに使用される。よって、映画は、サーバから移行している間、ＶＧＡディスプレイを制御するＶＧＡビデオ信号２０８としてコンピュータから出てくるまで、（盗難などから）保護される。

【０１２０】

映画は、暗号化形式でサーバからトランスポートされ、暗号化形式でＳＳＤ内に記憶され、暗号化形式でＶＧＡコントローラ２１０に送られる。状況によっては、ＶＧＡビデオ信号２０８は高品質ビデオ記録に適さず、よって、映画がＶＧＡビデオ信号として盗まれることになる可能性が低減される。

【０１２１】

コンピュータは、映画の暗号化トランスポートを、リモートサーバと暗号化トランスポートＳＳＤ２００との間で（破線２１２で概念的に図示されている）セキュアな通信リンクを確立することにより開始する。セキュアな通信リンクが確立されると、ホストとして働くリモートサーバは、ＳＳＤと暗号化鍵を交換する。リモートサーバは、交換した鍵に従って映画を暗号化し、暗号化した映画を、セキュアな通信リンクを介して、閲覧を待つ間の一時的記憶のために暗号化トランスポートＳＳＤ２００に転送する。

【０１２２】
暗号化トランスポートＳＳＤ２００は、フラッシュメモリ２１４に記憶するためにダウンロードされた映画を圧縮する。ある実施形態および／または使用シナリオでは、圧縮は、例えば、フラッシュメモリ書き込み増幅を最小化すること、および／または見かけの記憶容量を増加させることを可能にする。しかし、状況によっては、暗号化された映画は効果的に圧縮されない場合もある。したがって、（例えば、単一の集積回路として実施された）セキュアな物理境界（ＳＳＤコントローラ）２１６内で、ＳＳＤは、交換した暗号化鍵を使用してダウンロードされた映画を復号化する。復号化された映画は圧縮され、次いで、記憶のためにセキュアな物理境界（ＳＳＤコントローラ）２１６からフラッシュメモリ２１４にエクスポートされる前に再暗号化される。ダウンロードが完了すると、リモートサーバはセキュアな通信リンクを切断する。

【０１２３】
映画の閲覧を開始するために、コンピュータは、ＶＧＡコントローラ２１０と暗号化トランスポートＳＳＤ２００との間に（破線２１８で概念的に示されている）セキュアな通信リンクを確立し、ダウンロードされた映画の記憶アドレスを提供する。暗号化鍵交換が、ホストとして働くＶＧＡコントローラと暗号化トランスポートＳＳＤ２００との間で行われる。暗号化トランスポートＳＳＤ２００は、フラッシュメモリ２１４から記憶された映画を読み出し、セキュアな物理境界（ＳＳＤコントローラ）２１６内で読み出した映画を復号化し、その結果を展開し、交換した暗号化鍵を使用して再暗号化し、次いで、再暗号化した映画をＶＧＡコントローラ２１０にエクスポートする。ＶＧＡコントローラは、暗号化された映画を受け取り、ＶＧＡコントローラ２１０のセキュアな物理境界（ＶＧＡコントローラ）２２０内で、交換した暗号化鍵を使用して映画を復号化し、ＶＧＡ制御信号２０８を提供して、ＶＧＡディスプレイ２０６による映画の閲覧を可能にする。セキュアな物理境界（ＳＳＤコントローラ）２１６およびセキュアな物理境界（ＶＧＡコントローラ）２２０の外部のいかなる点においても、非暗号化形式で利用可能な映画が改ざんまたは盗難の対象となることはない。

【０１２４】
ある実施形態では、リモートサーバとＳＳＤとの間のセキュアな通信リンクは、複数の要素、すなわち、リモートサーバとコンピュータとの間の結合２２２、コンピュータを介したトランスポート、およびコンピュータとＳＳＤとの間の結合２２４を使用する。リモートサーバとコンピュータとの間の結合２２２は、例えば、リモートサーバ２０４およびインターネットへの結合（図示せず）、インターネットを介したトランスポート、ならびにコンピュータ２０２のネットワーキングインターフェースを介してインターネットへの別の結合などによるものである。コンピュータとＳＳＤとの間の結合２２４は、例えば、コンピュータ２０２のストレージインターフェース（図示せず）および暗号化トランスポートＳＳＤ２００の外部インターフェースなどによるものである。ある実施形態では、ＶＧＡコントローラとＳＳＤとの間のセキュアな通信リンクは、複数の要素、すなわち、コンピュータを介したトランスポート、およびコンピュータとＳＳＤとの間の結合２２４を使用する。

【０１２５】
様々な実施形態において、暗号化トランスポートＳＳＤ２００は、図１Ａに示す１若しくはそれ以上の要素に従って実施される。例えば、フラッシュメモリ２１４は図１ＡのＮＶＭ１９９に対応し、および／またはＳＳＤとコンピュータとの間の結合２２４は図１Ａの１若しくはそれ以上の外部インターフェース１１０に対応する。様々なコンテキストにおいて、図２に示す具体的応用は、図１Ｂに示す１若しくはそれ以上の要素に従って実施される。例えば、暗号化トランスポートＳＳＤ２００は図１ＢのＳＳＤ１０１のインスタンスに対応し、コンピュータ２０２は図１Ｂのホスト１０２に対応する。

【０１２６】
トランスポート暗号化層の実施形態
上記の例では、リモートサーバ２０４は、ペイパービュー映画のダウンロードおよび記

憶の間はホストであった。次いで、閲覧中は、ＶＧＡコントローラ２１０がホストの役割を果たした。「ホスト」の一例は、この用語が図２、図３Ａ、図３Ｂ、図４、および図５に関連して使用される場合には、暗号化トランスポートＳＳＤの具体的実施形態を用いたデータの暗号化トランスポートの間の暗号化鍵交換およびデータ暗号化／復号化を実行するシステムプラットフォームである。

【０１２７】

図３Ａ、図３Ｂ、図４、および図５に、暗号化トランスポートＳＳＤの機能の具体的実施形態の詳細を示す。図３Ａには、２段の圧縮後データ暗号化を含む書き込みデータパス機能が示されている。図３Ｂには、図３Ａの書き込みデータパス機能の「反転」と合致する、２段の展開前復号化を含む読み取りデータパス機能が示されている。図４には、暗号化鍵および復号化鍵の交換と、ホストと暗号化トランスポートＳＳＤとの間のデータ転送とのためのセキュアな通信リンクを確立するのに使用されるハンドシェーキングが示されている。図５には、図３Ａおよび図３Ｂに示すようなデータパスを含む、ホストと暗号化トランスポートＳＳＤとの間の書き込みデータ転送動作および読み取りデータ転送動作が示されている。

【０１２８】

図３Ａのブロック図には、暗号化鍵を交換し、フラッシュメモリ３０６に記憶するための暗号化データ３０４をトランスポートするために暗号化トランスポートＳＳＤ３０２と通信可能に結合されたホスト３００が示されている。暗号化トランスポートＳＳＤ３０２は、フラッシュメモリ３０６とＳＳＤコントローラ３０８とを含む。様々な実施形態および／または使用シナリオにおいて、暗号化トランスポートＳＳＤ３０２、ＳＳＤコントローラ３０８、およびフラッシュメモリ３０６は、それぞれ、図１Ａのソリッドステートディスク１０１、ＳＳＤコントローラ１００、およびＮＶＭ１９９に対応する。

【０１２９】

一具体的実施形態では、ＳＳＤコントローラ３０８は、ホスト３００とフラッシュメモリ３０６との間の暗号化データのトランスポートを処理するための書き込みデータパス３１０を含む。書き込みデータパス３１０は、セッション復号化層３１４、可逆的圧縮層３１６、内部暗号化層３１８、バックエンド暗号化層３２０、および書き込み－書式設定層３２２を含む。書き込みデータパス３１０は、暗号化データ３０４を受け取り、フラッシュメモリ３０６に記憶するために暗号化書式設定データ３１２をエクスポートする。

【０１３０】

ある実施形態では、書き込みデータパス３１０の１若しくはそれ以上の動作の任意選択の部分は、図１ＡのＳＳＤ１０１の１若しくはそれ以上の要素の部分によって実行される。例えば、データ処理１２１の部分は、バッファ１３１、ＥＣＣ１６１、デバイスインターフェース論理１９１、およびデバイスインターフェース１９０と連携して、書き込みデータパス３１０の動作を実行する。他の実施形態では、前述の層のうちの１若しくはそれ以上は、１若しくはそれ以上の専用ハードウェア論理回路ブロックならびに／または１若しくはそれ以上の組み込みプロセッサおよび関連付けられたファームウェアで実施される。ＳＳＤコントローラ３０８が単一の集積回路内で実施されるときに、単一の集積回路は、復号化データ３２６および圧縮データ３２８内の復号化情報、ならびに任意選択の交換された鍵が（例えば改ざんや盗難などから）保護されていることを保証するセキュアな物理境界（図示せず）を提供する。

【０１３１】

ある実施形態では、暗号化データがフラッシュメモリ３０６に書き込まれる前に、ホスト３００と暗号化トランスポートＳＳＤ３０２とは、セキュアな接続を確立し、セッション暗号化鍵および復号化鍵を交換する。あるシナリオでは、ホストは、書き込みコマンド、記憶アドレスを発行し、次いで、（図３ＡにK_Hで示されている）セッション暗号化鍵を使用したデータの暗号化を開始し、結果３０４をエクスポートする。

【０１３２】

ＳＳＤコントローラ３０８は暗号化データ３０４を受け取り、受け取ったデータを、（

図３ＡにＫ$_{C}$で示されている）セッション復号化鍵を使用してセッション復号化層３１４で復号化し、復号化データ３２６を生成する。復号化データ３２６は、可逆的圧縮層３１６によって圧縮され、圧縮データ３２８を生成する。ある実施形態および／または使用シナリオでは、可逆的圧縮は、有利には、書き込み増幅率を低減させ、かつ／または記憶されなければならないデータの量を低減させることによってフラッシュメモリに書き込まれるデータの見かけの記憶容量を増加させる。一具体的実施形態では、圧縮の技法は、ＬＺ可逆的圧縮（例えば、ＬＺ７７といった辞書コーダ）である。

【０１３３】

圧縮データ３２８は、内部暗号化層３１８によって暗号化され、暗号化圧縮データ３３０を生成する。一具体的実施形態では、内部暗号化層３１８は、ホスト３００によって使用されたセッション暗号化の技法（例えば、Ｋ$_{B}$＝Ｋ$_{H}$である同じ暗号化アルゴリズム）を使用して暗号化データ３０４を生成する。別の実施形態では、内部暗号化層３１８の暗号化の技法は、例えば、ＴＣＧ　Ｏｐａｌといったセキュリティプロトコルによって決定される。そのようなセキュリティプロトコルの一具体的実施形態では、内部暗号化層３１８によって使用される暗号化鍵Ｋ$_{B}$は、少なくとも一部は、記憶アドレス範囲といったメタデータによって決定される。別の実施形態では、複数のアドレス範囲があり、各範囲はそれぞれの暗号化鍵と関連付けられている。別の実施形態では、アドレス範囲のうちのどれも一致しない場合には、グローバルな「上記のどれでもない」鍵がある。

【０１３４】

ある実施形態では、暗号化圧縮データ３３０は、バックエンド暗号化層３２０で、暗号化鍵Ｋ$_{A}$を使用して２度目の暗号化を施され、バックエンド暗号化データ３３２を生成する。別の具体的実施形態では、バックエンド暗号化層３２０は、暗号化の技法および／または内部暗号化層３１８によって使用された鍵とは異なる（１若しくはそれ以上の）鍵（例えばＫ$_{A}$！＝Ｋ$_{B}$）を使用する。さらに別の実施形態では、暗号化の代わりにスクランブラが使用される。

【０１３５】

バックエンド暗号化データ３３２は、記憶アドレスマッピング、誤り訂正のための符号化、変調といった技法により、書き込み－書式設定層３２２によって処理され、フラッシュメモリ３０６にエクスポートされる暗号化書式設定データ３１２を生成する。

【０１３６】

書き込みデータパス３１０の別の実施形態（図示せず）では、内部暗号化層３１８は存在せず、バックエンド暗号化層３２０への圧縮データ３２８の直接入力を可能にする。様々な実施形態において、単一段の圧縮後暗号化書き込みデータパスは、（ａ）バックエンド暗号化、（ｂ）ホスト３００によって使用されたトランスポートセッション暗号化、および（ｃ）セキュリティプロトコルによって決定される暗号化のうちの１つを用いる。

【０１３７】

書き込みデータパス３１０の別の実施形態（図示せず）では、ホストによって送られるデータは暗号化されず、平文として送られる。セッション復号化層３１４は存在せず、ホストから可逆的圧縮層３１６へのデータの直接入力を可能にする。内部暗号化鍵Ｋ$_{B}$の値はセキュリティプロトコルによって決定される。バックエンド暗号化層３２０は鍵Ｋ$_{A}$を使用してバックエンド暗号化を行う。

【０１３８】

書き込みデータパス３１０の別の実施形態（図示せず）では、セッション復号化層３１４も内部暗号化層３１８も存在しない。ホストからの平文データ入力は可逆的圧縮層３１６に直接適用され、圧縮データ３２８はバックエンド暗号化層３２０に直接適用される。バックエンド暗号化鍵Ｋ$_{A}$の値は、（ａ）バックエンド暗号化鍵値、および（ｂ）セキュリティプロトコルによって決定される値のうちの１つである。

【０１３９】

図３Ｂに示すブロック図には、暗号化鍵を交換し、暗号化トランスポートＳＳＤ３０２内の記憶からホスト３００に暗号化データ３０４をトランスポートするために暗号化トラ

ンスポートＳＳＤ３０２と通信可能に結合されたホスト３００が示されている。図３Ｂには、図３Ａに示されている暗号化トランスポートＳＳＤの書き込みデータパス機能と適合する読み取りデータパス機能の一実施形態の選択された詳細が示されており、読み取りデータパス機能は２段の展開前復号化を含む。

【０１４０】

一具体的実施形態では、ＳＳＤコントローラ３０８は、フラッシュメモリ３０６とホスト３００との間の暗号化データのトランスポートを処理するための読み取りデータパス３４６を含む。読み取りデータパス３４６は、読み取り書式解除層３３６、バックエンド復号化層３３８、内部復号化層３４０、読み取り展開層３４２、およびセッション暗号化層３４４を含む。読み取りデータパス３４６は、フラッシュメモリ３０６内の記憶から暗号化書式設定データ３１２をインポートし、ホスト３００に暗号化データ３０４を出力する。

【０１４１】

ある実施形態では、読み取りデータパス３４６の１若しくはそれ以上の動作の任意選択の部分は、図１ＡのＳＳＤ１０１の１若しくはそれ以上の要素の部分によって実行される。例えば、データ処理１２１の部分は、バッファ１３１、ＥＣＣ１６１、デバイスインターフェース論理１９１、およびデバイスインターフェース１９０と連携して、読み取りデータパス３４６の動作を実行する。他の実施形態では、前述の層のうちの１若しくはそれ以上は、１若しくはそれ以上の専用ハードウェア論理回路ブロックならびに／または１若しくはそれ以上の組み込みプロセッサおよびファームウェアで実施される。ＳＳＤコントローラ３０８が単一の集積回路内で実施されるときに、単一の集積回路は、復号化データ３２６および圧縮データ３２８内の復号化情報、ならびに任意選択の交換された鍵が（例えば、改ざんや盗難などから）保護されていることを保証するセキュアな物理境界（図示せず）を提供する。

【０１４２】

ある実施形態では、暗号化書式設定データ３１２がフラッシュメモリ３０６から読み取られる前に、ホスト３００と暗号化トランスポートＳＳＤ３０２とは、セキュアな接続を確立し、セッション暗号化鍵および復号化鍵を交換する。あるシナリオでは、ホストは、読み取りコマンド、および読み出しアドレスを発行し、次いで、暗号化トランスポートＳＳＤ３０２による暗号化データ３０４の送出を待つ。ホスト３００は（図３ＢにK_Hとして図示されている）セッション復号化鍵を使用して受け取ったデータを復号化する。

【０１４３】

ＳＳＤコントローラ３０８は、フラッシュメモリ３０６から暗号化書式設定データ３１２をインポートする。ＳＳＤコントローラ３０８は読み取り書式解除層３３６でインポートしたデータを書式解除し、記憶アドレスマッピング、誤り訂正のための復号、復調といった技法により、バックエンド暗号化データ３３２を生成する。バックエンド暗号化データ３３２は、バックエンド復号化層３３８で復号化され、暗号化圧縮データ３３０を生成する。暗号化圧縮データ３３０は、内部復号化層３４０で復号化され、圧縮データ３２８を生成する。圧縮データ３２８は読み取り展開層３４２で展開され、復号化データ３２６を生成する。復号化データ３２６は、セッション暗号化層３４４によってセッション暗号化鍵K_Cを使用して暗号化され、暗号化データ３０４を生成する。読み取り動作は、書き込み動作の逆相似動作である。読み取り書式解除層３３６、復号化層３３８および３４０、読み取り展開層３４２、ならびにセッション暗号化層３４４は、データをフラッシュメモリ３０６に記憶させた書き込み動作の結果を反転させる。

【０１４４】

書き込み時に内部暗号化層３１８によって使用された暗号化鍵K_Bが、少なくとも一部は、記憶アドレス範囲といったメタデータによって決定されているとき、またはそれぞれの暗号化鍵が複数のアドレス範囲によって決定されている場合、またはアドレス範囲のどれも一致しないために「上記のどれでもない」鍵が使用された場合には、対応する復号化鍵が、内部復号化層３４０によって圧縮データ３２８を生成するのに使用される。

【０１４５】
読み取りデータパス３４６の別の実施形態（図示せず）では、内部復号化層３４０は存在せず、読み取り展開層３４２へのバックエンド復号化データの直接入力を可能にする。様々な実施形態において、単一段の展開前復号化読み取りデータパスは、（ａ）バックエンド復号化、（ｂ）ホスト３００によって使用されたトランスポートセッション復号化、および（ｃ）セキュリティプロトコルによって決定される復号化のうちの１つを用いる。
【０１４６】
読み取りデータパス３４６の別の実施形態（図示せず）では、ホストによって受け取られるデータは暗号化されず、平文として送られる。セッション暗号化層３４４は存在せず、読み取り展開層３４２がホストに直接データを提供することを可能にする。内部復号化鍵K_Bの値はセキュリティプロトコルによって決定される。バックエンド復号化層３３８は、鍵K_Aを使用して、フラッシュメモリへのデータ書き込み時に使用されたバックエンド暗号化を反転させる。
【０１４７】
読み取りデータパス３４６の別の実施形態（図示せず）では、内部復号化層３４０もセッション暗号化層３４４も存在せず、読み取り展開層３４２へのバックエンド復号化データの直接入力を可能にし、読み取り展開層３４２がデータを平文としてホストに直接提供することを可能にする。バックエンド復号化層３３８は、（ａ）バックエンド暗号化鍵値、および（ｂ）セキュリティプロトコルによって決定される値のうちの１つを使用して、フラッシュメモリへのデータ書き込み時に使用されたバックエンド暗号化を反転させる。
【０１４８】
さらに別の実施形態（図示せず）では、ホストと暗号化トランスポートＳＳＤとの間で送られるデータは、選択的に、暗号化されて伝えられ、さもなければ、平文として伝えられる。例えば、ホストデータの１若しくはそれ以上のアドレス範囲は、暗号化形式で（例えばＴＣＧ　Ｏｐａｌなどのようにそれぞれの鍵に従って）伝えられ、他のアドレス範囲は平文形式で伝えられる。別の例では、ホストからのある種のコマンドは、データが暗号化して伝えられるか、それとも平文として伝えられるか（暗号化されたコマンドを読み取り、または書き込む、平文コマンドを読み取り、または書き込むなど）を指定する。
【０１４９】
様々な実施形態では、ＳＳＤコントローラにおいて、（書き込みデータパス３１０といった）ホストからフラッシュへの書き込みデータパスおよび（読み取りデータパス３４６といった）フラッシュからホストへの読み取りデータパスの同時の、非干渉の動作を可能にするのに十分なリソースが実装され、ホストと暗号化トランスポートＳＳＤとの間の同時の、非干渉双方向の書き込み動作および読み取り動作を可能にする。他の実施形態では、書き込みデータパスおよび読み取りデータパスの任意選択の部分またはすべての部分は共用され、ホストと暗号化トランスポートＳＳＤとの間の同時の、かつ／または非干渉の書き込み動作および読み取り動作を妨げるが、ハードウェアの低減を可能にする（例えば、ある状況では、コストを有利に低減させる）。
【０１５０】
図４は、図２、図３Ａ、および図３Ｂに関連して図示し、説明したような、例えば暗号化トランスポートＳＳＤのコンテキストでの、暗号化トランスポートデータ転送を実行するためのホストとＳＳＤコントローラとの間のセキュアな通信リンクの作成、使用、および放棄の一実施形態を示す流れ図である。ホスト動作４０９は右側に図示されており、コントローラ動作４１９は左側に図示されている。
【０１５１】
要約すると、セキュアな通信リンクが確立され、ホストとコントローラとが各々相手側の識別情報を認証し、対称暗号化鍵および復号化鍵が交換され、暗号化データの転送が行われ、完了すると、通信リンクは切断され、コントローラは、対称暗号化鍵および復号化鍵のコントローラ側のコピーを破壊する。
【０１５２】

開始４０１で、ホストはコントローラを「チャネルを開く」受諾４１２に進ませる「チャネルを開く」要求４０２を行う。「チャネルを開く」受諾４１２はホストによって確認され、ホスト側の認証４０３に進む。コントローラはコントローラ側の認証４１３に進む。あるシナリオでは、両方の側が相手側の識別情報を認証した後で、各々の側は相手側に公開暗号化鍵を送り、セキュアな通信リンクの作成を完了する。

【０１５３】

セキュアな通信リンクを使用して、双方が対称暗号化鍵および復号化鍵を交換する（コントローラ側の鍵交換４１４およびホスト側の鍵交換４０４）。ある実施形態では、ＡＥＳ１２８、ＡＥＳ１９２、ＡＥＳ２５６といったＡＥＳ暗号化の技法が使用される。そのような実施形態では、単一の鍵が双方によって暗号化と復号化の両方に使用される（$K_C = K_H$）

セキュアなトラフィック交換が行われ（コントローラ側のトラフィック交換４１５およびホスト側のトラフィック交換４０５）、その間に、例えば図３Ａについて説明した暗号化データ書き込み動作、例えば図３Ｂについて説明した暗号化データ読み取り動作、またはその両方が行われる。例えば、対称暗号化鍵および復号化鍵の交換によって決定される鍵K_Cは、図３Ａのセッション復号化層３１４および図３Ｂのセッション暗号化層３４４の鍵K_Cに対応する。ホストからコントローラに送られるデータは、参照番号５０８（ホスト側のコントローラ側へのトラフィック５０８）で指示されており、コントローラからホストに送られるデータは、参照番号５１０（コントローラ側のホスト側へのトラフィック５１０）で指示されている。

【０１５４】

ある実施形態では、概念的にはセキュアなトラフィック交換の「下で」動作するセキュリティプロトコルが任意選択で用いられる。コントローラは、内部暗号化鍵および復号化鍵を決定するのに使用される情報、および／または、コントローラ側のＴＣＧ　Ｏｐｓ／ストレージアクセス４１５Ｘで図示される、コントローラ側のセキュリティプロトコルに基づくアクセスを可能にするプロトコル情報を受け取り、記憶する。ホストは、内部暗号化鍵および復号化鍵を決定するのに使用される対応する情報、および／または、ホスト側のＴＣＧ　Ｏｐｓ／ストレージアクセス４０５Ｘで図示される、ホスト側のセキュリティプロトコルに基づくアクセスを可能にするプロトコル情報を決定し、かつ／または受け取り、次いで記憶する。任意選択のセキュリティプロトコルとのセキュアなトラフィック交換は、内部暗号化鍵および復号化鍵および／またはコントローラ側のＴＣＧ　Ｏｐｓ／ストレージアクセス４１５Ｘと関連付けられたプロトコル情報を使用して、内部暗号化層３１８（図３Ａに示されているホスト書き込み）および内部復号化層３４０（図３Ｂに示されているホスト読み取り）に鍵情報を提供する。ある実施形態、例えば、セキュリティプロトコルとしてのＴＣＧ　Ｏｐａｌに基づくある実施形態では、内部暗号化／復号化層のための鍵情報は、ホスト要求と関連付けられた１若しくはそれ以上のアドレス範囲に依存する。

【０１５５】

セキュアなトラフィック交換が完了すると、ホスト側は「チャネルを閉じる」要求４０６に進み、コントローラ側は「チャネルを閉じる」受諾４１６に進む。セキュアな通信リンクは放棄され、コントローラは、対称暗号化鍵および復号化鍵K_Cのコントローラ側のコピーを破壊する（鍵を破壊する４１７）。

【０１５６】

図５は、（図２、図３Ａ、図３Ｂ、および図４に関連して図示し、説明したような）暗号化トランスポートＳＳＤコントローラのデータパス制御および／または動作の一実施形態を示す流れ図である。図５で、書き込みデータパス制御動作５０１～５０７は左側にあり、読み取りデータパス制御動作５１７～５１１は右側にある。データパス制御および／または動作は、図３Ａおよび図３Ｂに示すように、２段の圧縮後暗号化データパスに適用され、図４のコントローラ側のセキュアなトラフィック交換４１５の間に発生するイベントに対応する。図５に適用可能な動作コンテキストの一例は図１Ｂであり、図１Ｂでは、

概念的に、ホスト１０２はＳＳＤコントローラ１００を介してＮＶＭ１９９に暗号化データを書き込み、ＳＳＤコントローラを介してＮＶＭ１９９から暗号化データを読み取る。

【０１５７】

書き込み操作の間に、ＳＳＤコントローラは、（例えばホストから）暗号化書き込みデータを受け取り（書き込みデータを受け取る５０１）、（例えば図３Ａの３１４により）交換された暗号化鍵および復号化鍵K_H（$K_C = K_H$）（鍵＝K_H５２２Ｋ）を使用して暗号化書き込みデータを復号化する（書き込みデータを復号化する５０２）。復号化されたデータは（例えば図３Ａの３１６によって）圧縮される（復号化したデータを圧縮する５０３）。圧縮されたデータは、内部暗号化鍵K_Bを使用して、内部暗号化層によって（例えば図３Ａの３１８によって）暗号化される（圧縮したデータを暗号化する５０４）。暗号化された圧縮されたデータは、バックエンド暗号化層によって（例えば図３Ａの３２０によって）バックエンド暗号化鍵K_A（鍵＝K_A５２５Ｋ）を使用して（再）暗号化される（暗号化したデータを（再）暗号化する５０５）。バックエンド暗号化データは（例えば図３Ａの３２２によって）変調され（（再）暗号化したデータを変調する５０６）、ＮＶＭ１９９に記憶される（変調したデータを記憶する５０７）。ある実施形態では、内部暗号化鍵K_Bは、書き込みデータを受け取るのに使用された鍵と別個のものである（$K_B ! = K_C$）（鍵＝K_B５２４Ｋ）。他の実施形態では、K_Bの値はセキュリティプロトコルによって決定され、一具体的実施形態では、$K_B = K_H$である。参照番号５０８（ホスト側のコントローラ側へのセキュアなトラフィック５０８）は、ホストからＳＳＤコントローラに転送されるデータを表し、参照番号５１０（コントローラ側のホスト側へのセキュアなトラフィック５１０）は、ＳＳＤコントローラからホストに転送されるデータを表す。

【０１５８】

読み取り操作の間に、ＳＳＤコントローラはＮＶＭ１９９から暗号化書式設定データをインポートし（データを読み取る５１７）、（例えば図３Ｂの３３６によって）読み取ったデータを復調する（読み取ったデータを復調する５１６）。復調されたデータは（例えば図３Ｂの３３８によって）復号化され（復調したデータを復号化する５１５）、結果は（例えば図３Ｂの３４０によって）再度復号化される（復号化したデータを復号化する５１４）。結果は（例えば図３Ｂの３４２によって）展開され（（再）復号化したデータを展開する５１３）、次いで（例えば図３Ｂの３４４によって）暗号化され（展開したデータを暗号化する５１２）、結果として得られる暗号化データはホスト１０２に提供される（暗号化したデータを提供する５１１）。

【０１５９】

実施技法の例

ある実施形態では、（例えばフラッシュメモリを有する）暗号化トランスポートＳＳＤコントローラ、コンピューティングホスト・フラッシュ・メモリ・コントローラ、および／またはＳＳＤコントローラ（例えば図１ＡのＳＳＤコントローラ１００）、ならびにプロセッサ、マイクロプロセッサ、システム・オン・チップ、特定用途向け集積回路、ハードウェアアクセラレータ、または前述の動作の全部または部分を提供する他の回路によって行われる動作の全部またはいずれかの部分の様々な組み合わせが、コンピュータシステムによる処理と適合する仕様によって指定される。仕様は、様々な記述、例えば、ハードウェア記述言語、回路記述、ネットリスト記述、マスク記述、またはレイアウト記述に従ったものである。記述の例には、Ｖｅｒｉｌｏｇ、ＶＨＤＬ、ＳＰＩＣＥ、ＳＰＩＣＥの変形、例えば、ＰＳｐｉｃｅ、ＩＢＩＳ、ＬＥＦ、ＤＥＦ、ＧＤＳ－ＩＩ、ＯＡＳＩＳ、または他の記述が含まれる。様々な実施形態では、処理は、１若しくはそれ以上の集積回路上に含めるのに適する論理および／または回路を生成し、検証し、または指定するための解釈、コンパイル、シミュレーション、および合成の任意の組み合わせを含む。各集積回路は、様々な実施形態によれば、様々な技法に従って設計することができ、かつ／または製造することができる。技法には、プログラマブルな技法（例えば、フィールド若しくはマスク・プログラマブル・ゲート・アレイ集積回路）、セミカスタムの技法（例えば、

全部若しくは一部がセルベースの集積回路）、およびフルカスタムの技法（例えば、実質的に専門化された集積回路）、それらの任意の組み合わせ、または集積回路の設計および／若しくは製造と適合する任意の他の技法が含まれる。

【０１６０】

ある実施形態では、命令のセットを記憶しているコンピュータ可読媒体によって記述される動作の全部または部分の様々な組み合わせが、１若しくはそれ以上のプログラム命令の実行および／若しくは解釈によって、１若しくはそれ以上のソースおよび／若しくはスクリプト言語命令文の解釈および／若しくはコンパイルによって、または、プログラミングおよび／若しくはスクリプティング言語命令文で表現された情報をコンパイルし、変換し、かつ／または解釈することによって生成されるバイナリ命令の実行によって実行される。命令文は任意の標準のプログラミングまたはスクリプティング言語（例えば、Ｃ、Ｃ＋＋、Ｆｏｒｔｒａｎ、Ｐａｓｃａｌ、Ａｄａ、Ｊａｖａ（登録商標）、ＶＢｓｃｒｉｐｔ、Ｓｈｅｌｌ）と適合する。プログラム命令、言語命令文、またはバイナリ命令のうち１若しくはそれ以上が、任意選択で、１若しくはそれ以上のコンピュータ可読記憶媒体要素上に記憶される。様々な実施形態では、プログラム命令の一部、全部、または様々な部分が、１若しくはそれ以上の関数、ルーチン、サブルーチン、インラインルーチン、プロシージャ、マクロ、またはそれらの部分として実現される。

【０１６１】

結論

ある特定の選択が、説明において、テキストおよび図面を作成するに際の単なる便宜のためになされており、別の指示がない限り、それらの選択は、それ自体で、前述の実施形態の構造または動作に関する追加情報を伝えるものと解釈すべきではない。選択の例には、図の符番に使用される呼称の特定の編成または割り当て、および実施形態の特徴および要素を識別し、参照するのに使用される要素識別子（コールアウトや数値識別子など）の特定の編成または割り当てが含まれる。

【０１６２】

「ｉｎｃｌｕｄｅｓ」または「ｉｎｃｌｕｄｉｎｇ」という語は、開放型範囲の論理集合を記述する抽象概念として解釈されるべきことが明確に意図されており、後に続けて「ｗｉｔｈｉｎ」という語が明示されない限り物理的包含を伝えるためのものではない。

【０１６３】

前述の実施形態は、説明および理解の明確さのためにある程度詳細に説明されているが、本発明は提示した詳細だけに限定されるものではない。本発明の多くの実施形態がある。開示の実施形態は例示であり、限定ではない。

【０１６４】

説明と整合性を有する、構成、配置、および使用における多くの変形が可能であり、それらの変形は、発行される特許の特許請求の範囲内にあることが理解されるであろう。例えば、相互接続および機能ユニットのビット幅、クロック速度、および使用される技術の種類は、各構成要素ブロックにおける様々な実施形態に従って変わりうる。相互接続および論理に与えられた名称は、単なる例であり、説明した概念を限定するものと解釈すべきではない。フローチャートおよび流れ図のプロセス、動作、および機能要素の順序および配置は、様々な実施形態に従って変わりうる。また、特に別に指定しない限り、指定される値範囲、使用される最大値および最小値、または他の特定の仕様（例えば、フラッシュメモリ技術の種類、レジスタおよびバッファ内のエントリまたは段の数）は、単に前述の実施形態のものにすぎず、実施技術の改善および変更を追跡することが見込まれるものであり、限定として解釈すべきではない。

【０１６５】

当分野で公知の機能的に等価の技法を、様々なコンポーネント、サブシステム、動作、関数、ルーチン、サブルーチン、インラインルーチン、プロシージャ、マクロ、またはそれらの部分を実施するのに、前述の技法の代わりに用いることができる。また、実施形態の多くの機能的態様を、より高速な処理（以前にハードウェアにあった機能のソフトウェ

アへの移行を円滑化する）およびより高い集積密度（以前にソフトウェアにあった機能のハードウェアへの移行を円滑化する）の実施形態に依存する設計制約条件および技術傾向に応じて、選択的に、ハードウェア（おおむね専用の回路など）で、またはソフトウェアで（例えば、プログラムされたコントローラ若しくはプロセッサのある方式によって）実現できることも理解される。様々な実施形態の具体的な変形は、これに限定されるものではないが、分割の違い、フォームファクタおよび構成の違い、異なるオペレーティングシステムおよび他のシステムソフトウェアの使用、異なるインターフェース規格、ネットワークプロトコル、または通信リンクの使用、本明細書で説明した概念を、特定の用途の固有の技術的業務的制約条件に従って実施するときに予期されるべき他の変形を含む。

【０１６６】

各実施形態は、前述の各実施形態の多くの態様の最小限の実施に必要とされるものを大きく超えた詳細および環境的コンテキストと共に説明されている。ある実施形態は、残りの要素間での基本的協働を変更せずに開示の構成要素または機能を割愛することを当業者は理解するであろう。よって、開示の詳細の多くが前述の実施形態の様々な態様を実施するのに必要ではないことが理解される。残りの要素が先行技術と区別できる範囲内で、割愛される構成要素および特徴は本明細書で説明した概念を限定するものではない。

【０１６７】

設計におけるすべてのそのような変形は、前述の実施形態によって伝えられる教示に対する実質的な変更ではない。また、本明細書で説明した実施形態は、他のコンピューティング用途およびネットワーキング用途に幅広い適用性を有し、前述の実施形態の特定の用途または産業だけに限定されるものではないことも理解される。よって本発明は、発行される特許の特許請求の範囲内に包含されるあらゆる可能な改変形態および変形形態を含むものと解釈すべきである。

【図１Ａ】

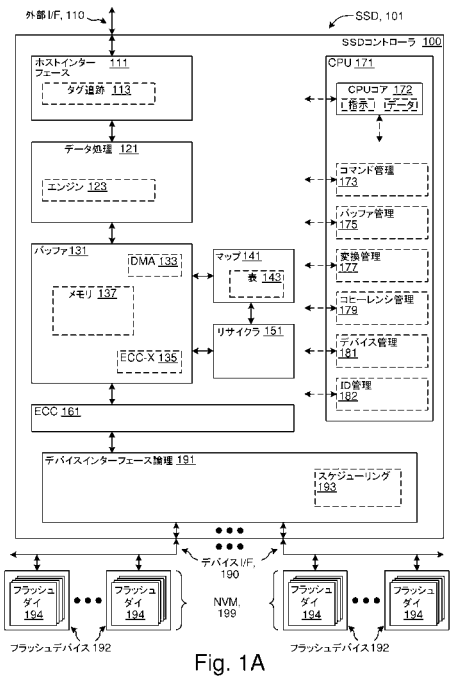

Fig. 1A

【図１Ｂ】

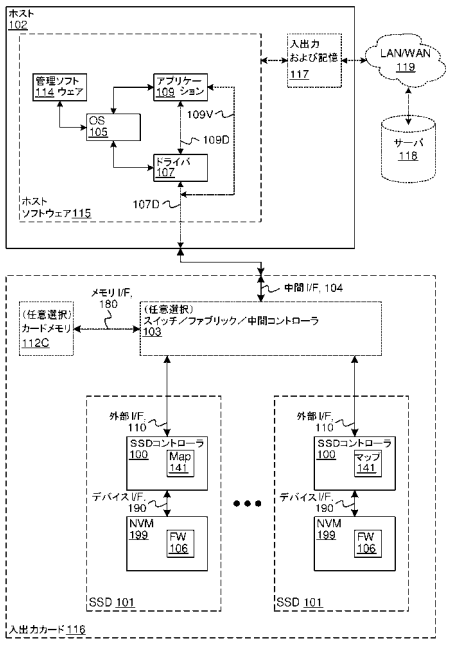

Fig. 1B

【図２】

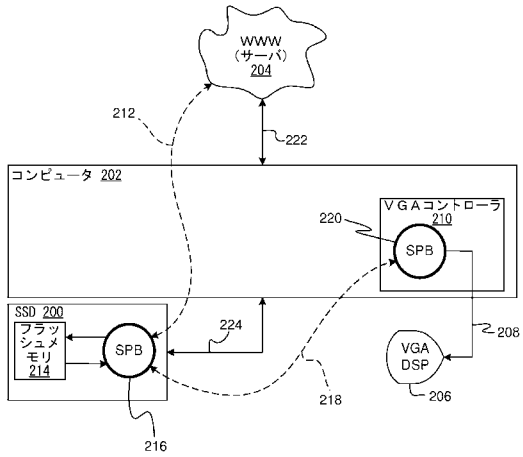

Fig. 2

【図３Ａ】

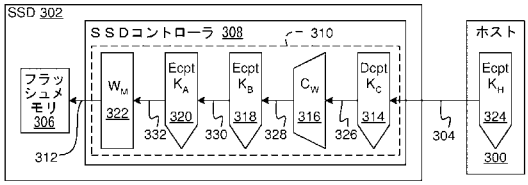

Fig. 3A

【図３Ｂ】

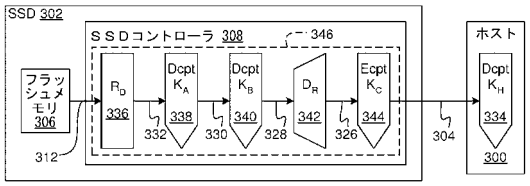

Fig. 3B

【図４】

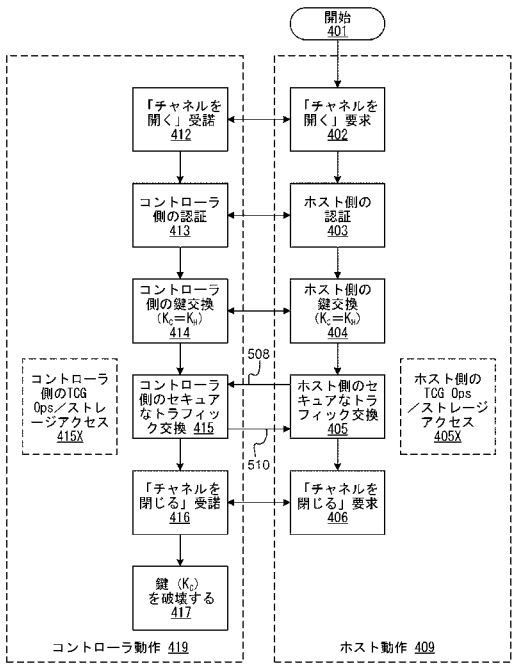

Fig. 4

【図５】

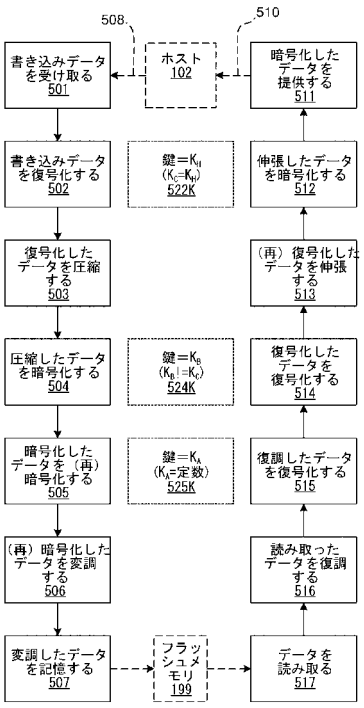

Fig. 5

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/034452

A. CLASSIFICATION OF SUBJECT MATTER

G11C 16/06(2006.01)i, G11C 16/22(2006.01)i, G06F 13/14(2006.01)i, G06F 21/00(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G11C 16/06; H04K 1/00; H04L 9/28; G06F 11/08; G06F 12/00; G06F 12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: encrypt, decrypt, compress, format, SSD, controller, host, transfer

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2011-0055664 A1 (BURD GREGORY et al.) 03 March 2011 See paragraphs [0030]-[0050],[0081]-[0091]; figures 1,6.	1-21
A	US 7706538 B1 (HUGHES JAMES P. et al.) 27 April 2010 See column 5, line 65 - column 7, line 24; figure 2.	1-21
A	US 2008-0205635 A1 (JAQUETTE GLEN ALAN et al.) 28 August 2008 See paragraphs [0041]-[0054],[0061]-[0065]; figures 1-2,5.	1-21
A	US 2008-0072070 A1 (MICHAEL PHILIP LAMACCHIA et.al) 20 March 2008 See paragraphs [0015]-[0029]; figure 1.	1-21

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 NOVEMBER 2012 (21.11.2012)	**23 NOVEMBER 2012 (23.11.2012)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	HAN, Seon Kyoung Telephone No. 82-42-481-8523

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2012/034452

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011-0055664 A1	03.03.2011	CN 102483687 A WO 2011-028802 A1	30.05.2012 10.03.2011
US 7706538 B1	27.04.2010	US 7814316 B1	12.10.2010
US 2008-0205635 A1	28.08.2008	None	
US 2008-0072070 A1	20.03.2008	None	

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN

【要約の続き】
【選択図】 図３Ａ