(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5643303号
(P5643303)
(45)発行日　平成26年12月17日(2014.12.17)　(24)登録日　平成26年11月7日(2014.11.7)

(51)Int.Cl.　　F I
G06F 21/34 (2013.01)　　G06F 21/20 134
H04L 9/32 (2006.01)　　H04L 9/00 675A

請求項の数 12　(全 28 頁)

(21)出願番号　特願2012-516228(P2012-516228)
(86)(22)出願日　平成22年6月16日(2010.6.16)
(65)公表番号　特表2012-530967(P2012-530967A)
(43)公表日　平成24年12月6日(2012.12.6)
(86)国際出願番号　PCT/US2010/038776
(87)国際公開番号　WO2010/148059
(87)国際公開日　平成22年12月23日(2010.12.23)
審査請求日　平成25年5月8日(2013.5.8)
(31)優先権主張番号　12/486,738
(32)優先日　平成21年6月17日(2009.6.17)
(33)優先権主張国　米国(US)

(73)特許権者　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　100140109
弁理士　小野　新次郎
(74)代理人　100075270
弁理士　小林　泰
(74)代理人　100080137
弁理士　千葉　昭男
(74)代理人　100096013
弁理士　富田　博行
(74)代理人　100147991
弁理士　鳥居　健一

最終頁に続く

(54)【発明の名称】記憶装置のリモートアクセス制御

(57)【特許請求の範囲】
【請求項１】
アクセス制御デバイスであって、
暗号化されたデータを含む記憶装置との通信がそれを通じて確立される少なくとも１つの通信インターフェースと、
少なくとも１つの処理ユニットと、
前記記憶装置に格納された前記暗号化されたデータにアクセスすることを前記アクセス制御デバイスによって可能にされるエンティティについての識別を含むアクセス制御情報と、
前記少なくとも１つの通信インターフェースを介して通信が確立される前記記憶装置の前記暗号化されたデータを暗号解読することができる記憶関連暗号情報と、
前記少なくとも１つの処理ユニットによって実行されると、前記少なくとも１つの処理ユニットに、
前記記憶装置に格納された前記暗号化されたデータにアクセスしようとするエンティティについての識別を、前記記憶装置が通信可能に結合されるコンピューティングデバイスから受信するステップと、
前記エンティティについての受信された識別を前記アクセス制御情報と比較するステップと、
前記エンティティについての受信された識別が前記アクセス制御情報を含むエンティティについての識別のうちの少なくとも１つと一致することを前記比較が明らかにする場合

に、前記記憶関連暗号情報を前記記憶装置にセキュアな方法で提供することによって、前記記憶装置が前記暗号化されたデータを暗号解読することを可能にするステップと
を実行させるコンピューター実行可能命令を含むコンピューター読み取り可能な記憶媒体と
を備え、前記記憶装置及び前記コンピューティングデバイスの両方から物理的に分離可能であるアクセス制御デバイス。

【請求項２】
前記アクセス制御情報は、前記記憶装置に格納された前記暗号化されたデータにアクセスすることを前記アクセス制御デバイスによって可能にされる前記エンティティの少なくとも一部に関連付けられる認証情報をさらに含み、
さらに、前記コンピューター読み取り可能な記憶媒体は、前記少なくとも１つの処理ユニットによって実行されると、前記少なくとも１つの処理ユニットに、
前記エンティティから認証情報を受信するステップと、
前記受信された認証情報を前記アクセス制御情報と比較するステップと
を含むさらなるステップを実行させるコンピューター実行可能命令をさらに含む請求項１に記載のアクセス制御デバイス。

【請求項３】
前記アクセス制御情報は、前記アクセス制御デバイスが更新されたアクセス制御情報をそこから受信する、前記アクセス制御デバイスの外部にある許可コンピューティングデバイスとのセキュアな通信を確立するためのアクセス制御暗号情報をさらに含む請求項１に記載のアクセス制御デバイス。

【請求項４】
前記アクセス制御情報はアクセス制御暗号情報をさらに含み、
さらに、前記コンピューター読み取り可能な記憶媒体は、前記少なくとも１つの処理ユニットによって実行されると、前記少なくとも１つの処理ユニットに、
前記アクセス制御暗号情報を利用して、別のコンピューティングデバイスを介して許可コンピューティングデバイスとのセキュア通信トンネルを確立するステップと、
前記エンティティについての受信された識別を前記セキュア通信トンネルを介して前記許可コンピューティングデバイスに提供するステップと、
前記エンティティについての受信された識別を提供することに応答して前記許可コンピューティングデバイスから受信される情報が、前記エンティティがアクセスを付与されるべきであることを示す場合に、前記記憶関連暗号情報を前記記憶装置へセキュアな方法で提供することによって、前記記憶装置が前記暗号化されたデータを暗号解読することを可能にするステップと
を含むさらなるステップを実行させるコンピューター実行可能命令をさらに含む請求項１に記載のアクセス制御デバイス。

【請求項５】
前記通信インターフェースは、前記記憶装置の一部である物理的受容部に接続可能な物理コネクタを含み、前記記憶装置との確立された通信は前記記憶装置と前記アクセス制御デバイスとの間の直接的な通信である請求項１に記載のアクセス制御デバイス。

【請求項６】
前記記憶装置との確立された通信は、前記アクセス制御デバイス及び前記記憶装置の両方が独立して通信可能に接続されるコンピューティングデバイスを通じた間接的な通信である請求項１に記載のアクセス制御デバイス。

【請求項７】
前記コンピューター読み取り可能な記憶媒体は、前記少なくとも１つの処理ユニットによって実行されると、前記少なくとも１つの処理ユニットに、前記記憶関連暗号情報のうちの少なくとも一部を消去させる、コンピューター実行可能命令をさらに含む請求項１に記載のアクセス制御デバイス。

【請求項８】

前記コンピューター読み取り可能な記憶媒体は、前記少なくとも１つの処理ユニットによって実行されると、前記少なくとも１つの処理ユニットに、外部命令とは独立に、前記少なくとも１つの処理ユニットによって実行されると前記少なくとも１つの処理ユニットに前記記憶関連暗号情報のうちの少なくとも一部を消去させるコンピューター実行可能命令を実行することを決定させる、コンピューター実行可能命令をさらに含む請求項７に記載のアクセス制御デバイス。

【請求項９】

前記コンピューター読み取り可能な記憶媒体は、前記少なくとも１つの処理ユニットによって実行されると、前記少なくとも１つの処理ユニットに、

前記記憶装置に格納された前記暗号化されたデータの少なくとも一部を消去する命令を受信するステップと、

該受信に応答して、前記記憶関連暗号情報の少なくとも一部を消去するステップと

を含むステップを実行させる、コンピューター実行可能命令をさらに含む請求項７に記載のアクセス制御デバイス。

【請求項１０】

前記少なくとも１つの処理ユニットに前記記憶装置へ前記記憶関連暗号情報をセキュアな方法で提供させる前記コンピューター実行可能命令は、前記少なくとも１つの処理ユニットによって実行されると、前記少なくとも１つの処理ユニットに、前記記憶関連暗号情報が前記コンピューティングデバイスによって解読されることを防ぐために、該提供の前に前記記憶関連暗号情報を保護させる、コンピューター実行可能命令をさらに含む請求項６に記載のアクセス制御デバイス。

【請求項１１】

前記コンピューター読み取り可能な記憶媒体は、前記少なくとも１つの処理ユニットによって実行されると、前記少なくとも１つの処理ユニットに、前記エンティティについての識別が受信される場合に前記エンティティに関連付けられる認証情報についてのチャレンジを前記コンピューティングデバイスに提供させる、コンピューター実行可能命令をさらに含む請求項１に記載のアクセス制御デバイス。

【請求項１２】

前記記憶関連暗号情報は、

前記記憶装置の前記暗号化されたデータの第１の部分のみを暗号解読することができる第１の記憶関連暗号情報と、

前記記憶装置の前記暗号化されたデータの前記第１の部分とは異なる第２の部分のみを暗号解読することができる第２の記憶関連暗号情報と

を含み、

さらに、前記記憶装置への前記記憶関連暗号情報の提供をさせる前記コンピューター実行可能命令は、前記少なくとも１つの処理ユニットによって実行されると、前記少なくとも１つの処理ユニットに、

前記エンティティが前記第１の記憶関連暗号情報に関連付けられる場合に前記第１の記憶関連暗号情報のみを前記記憶装置へ提供させ、

前記エンティティが前記第２の記憶関連暗号情報に関連付けられる場合に前記第２の記憶関連暗号情報のみを前記記憶装置へ提供させる、

コンピューター実行可能命令を含む請求項１に記載のアクセス制御デバイス。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、記憶装置のリモートアクセス制御に関する。

【背景技術】

【０００２】

[0001]非公開にしておくつもりのデータ及び情報を処理し、格納するためにコンピューティングデバイスを使用することが益々増えている。そのようなデータ及び情報は、政治

機密を含む可能性があるが、ビジネス及び個人情報を含む可能性の方が高く、そのような情報が悪意のある第三者又は敵対者によって入手されると、一人又は複数の個人に損害を与える可能性がある。したがって、コンピューティングデバイスのハードウェア、及びコンピューティングデバイスのソフトウェアの両方との関連で、種々のセキュリティ機構が実施されている。そのようなハードウェアセキュリティ機構の例には、指紋のようなバイオメトリック情報に基づいてセキュアなパスワードを生成するように設計される周辺装置、及びキーボードロック、通信ポートロック等の、コンピューティングデバイスへの物理的なアクセス障壁が含まれる。コンピューティングデバイスのソフトウェアに関連付けられるセキュリティ機構の例は、種々の暗号化技術及び種々のアクセス制御技術を含む。

【発明の概要】

【発明が解決しようとする課題】

【０００３】

[0002]しかしながら、１つ又は複数のコンピューター読み取り可能な媒体上に格納されたデータの保護は、多くの場合に、コンピューティングデバイスと直接的に全く関連しない活動中に失敗する。例えば、１つ又は複数のコンピューター読み取り可能な媒体を含む、ハードディスクドライブのような記憶装置の物理的な輸送が適切に護衛されなかったために、結果として紛失されるか、さらには盗難されたときに、そのコンピューター読み取り可能な媒体上に格納されたデータは漏洩される可能性があり、さらには既に漏洩されている。同様に、１つ又は複数のコンピューター読み取り可能な媒体を含む記憶装置がホストからアクセスできなかったために、結果として廃棄されるときに、そのコンピューター読み取り可能な媒体上に格納されたデータは漏洩される可能性があり、さらには既に漏洩されている。多くの場合に、そのような「失敗に終わった」記憶装置は、コンピューティングデバイスが検索し、アクセスすることができる形で、そのコンピューター読み取り可能な媒体上に格納されたデータのうちのかなり高いパーセンテージを保持する。

【０００４】

[0003]特に、悪意のある第三者又は敵対者がコンピューター読み取り可能な媒体を含む記憶装置に物理的に近づくことができるようになった場合に、そのようなコンピューター読み取り可能な媒体上に格納されたデータの保護を高めるために、「フルボリューム」暗号化法が開発されており、その方法によれば、記憶装置のコンピューター読み取り可能な媒体上に格納されたデータの実質的に全てが暗号化された形で格納されており、悪意のある第三者又は敵対者がそのような記憶装置を物理的に制御できるようになった場合であっても、適当な暗号解読鍵がなければデータを解読することができないようにする。より高い性能を提供するために、記憶装置上に格納されたデータの暗号化は、そのようなデータを記憶及び検索するコンピューティングデバイスの１つ又は複数の中央処理ユニットに負荷をかけることによってではなく、記憶装置そのものの一部である専用の暗号ハードウェアによって実行することができる。

【０００５】

[0004]フルボリューム暗号化（full volume encryption）法に加えて、機密データが格納されたコンピューター可読記憶媒体、又は記憶装置全体を適切な方法で物理的に破壊することも、そのようなデータの保護及びセキュリティを同様に高めることができる。例えば、データが物理的に一致することも、又はコンピューター可読記憶媒体から物理的に再生可能であることもないように、保護されるべきデータを格納している可能性があるコンピューター可読記憶媒体を物理的に細かく切断することができるか、又はそのようなコンピューター可読記憶媒体にランダムな強い磁界をかけることができる。代替的には、記憶装置を物理的に破壊するのではなく、所定の安全消去ポリシー（secure erasure policy）に従って、コンピューター読み取り可能な媒体上に格納された機密データをコンピューティングデバイスによって何度も上書きすることができる。残念なことに、コンピューター可読記憶媒体及び記憶装置を物理的に破壊することは、いずれも、コスト及び時間がかかる可能性が高く、時間及び費用を抑えるために効率が求められると、そのような媒体上に格納されたデータの保護及び破壊を弱める可能性がある安易な方法が用いられることが

あり、それにより、物理的破壊の効果が弱められる。更なる非効率性、すなわち政府のセキュリティに関する法令、プライバシーに関する法令等の種々の法令を追加することは、コンピューター可読記憶媒体を適切に破壊する義務を負い、特定の様式で書類を提出するという要件のような、更なる負担をかける可能性がある。

【０００６】

[0005]サーバー環境又は企業情報技術（ＩＴ）環境のような数多くの使用シナリオでは、記憶装置は多くの場合にホスト間で動かされる。そのような環境では、種々の形のアクセス制御を実施することが役に立つ。残念なことに、記憶装置に種々の形のアクセス制御をプロビジョニングすることによって複雑になる可能性があり、結果として、ハードウェア構成要素、開発、その後の障害解析にかなりの追加コストがかかる可能性がある。

【課題を解決するための手段】

【０００７】

[0006]記憶装置を、本明細書において「アクセス制御デバイス」と呼ばれる物理的エンティティに関連付けることができ、アクセス制御デバイスは、記憶装置の残りの部分から物理的かつ通信的に切り離すことができる。さらに、コンピューティングデバイスが、記憶装置から独立して、アクセス制御デバイスと通信することができるコンピューター実行可能命令を含むことができる。

【０００８】

[0007]一実施の形態では、アクセス制御デバイスに暗号情報をプロビジョニングすることができ、その暗号情報は、記憶装置のコンピューター読み取り可能な媒体に格納されたデータを直接的又は間接的に暗号化及び暗号解読するために、記憶装置のハードウェア暗号システムが用いることができる。アクセス制御デバイスが記憶装置のハードウェア暗号システムにのみその暗号情報を選択的に提供し、それにより、記憶装置が、該記憶装置上に格納されたデータへの選択的なアクセスを提供することを可能にするために、アクセス制御デバイスを更にプロビジョニングすることができる。結果として、アクセス制御デバイスが関連付けられる記憶装置に通信的に結合される場合であっても、アクセス制御デバイスは、所定の条件が満たされたときにのみ記憶装置のハードウェア暗号システムにその暗号情報を公開することによって、記憶装置上に格納された暗号化されたデータへのアクセスを制限することができる。

【０００９】

[0008]別の実施の形態では、アクセス制御デバイスに関連付けられる記憶装置上に格納されたデータにアクセスするのを許すことができるコンピューティングデバイス又はユーザーのようなエンティティのリストを、アクセス制御デバイスにプロビジョニングすることができる。その際、アクセス制御デバイスは、関連付けられる記憶装置に、リストに掲載されたエンティティの中にないエンティティからのデータ記憶関連通信に意味があるように応答しないように命令することができる。代替的に又はそれに加えて、アクセス制御デバイスが暗号情報をプロビジョニングされた場合には、アクセス制御デバイスは、格納されたデータにアクセスしようしているエンティティがリストに掲載されたエンティティの中にある場合にのみ、該アクセス制御デバイスの暗号情報を記憶装置のハードウェア暗号システムに与えることができ、それにより、記憶装置が、該記憶装置の格納されたデータへのアクセスを提供できるようにする。格納されたデータにアクセスしようとしているエンティティは、ユーザーパスワード、コンピューティングデバイス識別子、又はチャレンジ／レスポンス認証機構との関連の範囲内にあるような、セキュアコンテキストにおいて与えることができる他の同様の情報を通じて、自らを識別することができる。

【００１０】

[0009]更なる実施の形態では、アクセス制御デバイスに暗号情報をプロビジョニングすることができ、該暗号情報は、アクセス制御デバイスが許可コンピューティングデバイスとのセキュア通信トンネルを確立することを可能にする。アクセス制御デバイスに関連付けられる記憶装置上に格納されたデータにアクセスしようしているコンピューティングデバイスを用いて、アクセス制御デバイスが、セキュアトンネルを通じて許可コンピューテ

ィングデバイスと通信することを可能にする。その際、アクセス制御デバイスは許可コンピューティングデバイスに関連情報を提供することができ、該アクセス制御デバイスに関連付けられる記憶装置が要求側デバイスにデータを提供する動作が適切であることを許可コンピューティングデバイスが示す場合にのみ、その関連付けられる記憶装置が要求側デバイスにデータを提供することを可能にするか、又はその関連付けられる記憶装置に、要求側デバイスにデータを提供するように命令することができる。

【００１１】

[0010]また更なる実施の形態では、アクセス制御デバイスに実行可能命令をプロビジョニングすることができ、その命令によって、アクセス制御デバイスは自らを更新できるようになるか、又は顧客特有のアクセス制御ロジック及びアルゴリズムを提供するようにカスタマイズすることができる。そのような１組の実行可能命令、すなわち「スクリプトレット」を、プロビジョニング中にアクセス制御デバイスに与えることができ、その後、セキュアでかつ信頼性がある方法で外部コンピューティングデバイスから更新することができる。アクセス制御デバイスが、空間及び時間の一方又は両方を参照しながら、関連付けられる記憶装置又はコンピューティングデバイスとは別に自らを初期化するように、アクセス制御デバイスをプロビジョニングすることができる。

【００１２】

[0011]また更なる実施の形態では、アクセス制御デバイスに実行可能命令をプロビジョニングすることができ、その命令によって、アクセス制御デバイスは、関連する記憶装置上に格納されたデータを消去することが可能になるか、又はアクセス制御デバイス上に格納された任意の暗号情報を消去することが可能になり、それにより、そのような暗号情報を用いて暗号化された、関連付けられる記憶装置上のデータを読出し不可能かつアクセス不可能にすることができる。アクセス制御デバイスは、自らの判断に基づいて、又は許可コンピューティングデバイスからのような、遠隔受信される命令に基づいて、そのような実行可能命令を起動することができる。

【００１３】

[0012]この概要（発明の概要）は、概念の抜粋を簡単な形で紹介するために提供され、それらの概念は、詳細な説明（発明を実施するための形態）において後に更に説明される。この概要（発明の概要）は、特許請求される主題のアクセス制御機構又は不可欠な機構を特定することを意図されるものでもなければ、特許請求される主題の範囲を制限するために用いられることを意図されるものでもない。

【００１４】

[0013]更なる特徴及び利点が、添付の図面を参照しながら続けられる以下の詳細な説明から明らかにされる。

【００１５】

[0014]以下の詳細な説明は、添付の図面とともに取り上げられるときに最も良く理解することができる。

【図面の簡単な説明】

【００１６】

【図１】[0015]１つの例示的なプロビジョニングコンピューティングデバイス及び１つの例示的なアクセス制御デバイスのブロック図である。

【図２】[0016]１つの例示的なアクセス中のコンピューティングデバイス、１つの例示的なアクセス制御デバイス及び１つの例示的な記憶装置のブロック図である。

【図３】[0017]１つの例示的なアクセス中のコンピューティングデバイス、１つの例示的なアクセス制御デバイス及び１つの例示的な記憶装置の別のブロック図である。

【図４】[0018]アクセス制御デバイスと記憶装置との間の例示的な通信のブロック図である。

【図５】[0019]アクセス制御デバイスと記憶装置との間の更なる例示的な通信のブロック図である。

【図６】[0020]１つの例示的なプロビジョニングコンピューティングデバイスの１つの例

示的な動作の流れ図である。
【図７】[0021]１つの例示的なアクセス中のコンピューティングデバイスの１つの例示的な動作の流れ図である。
【発明を実施するための形態】
【００１７】
[0022]以下の説明は、記憶装置と、物理的かつ通信的に分離可能なアクセス制御デバイスとを備える記憶システムに関し、アクセス制御デバイスはアクセス制御情報を含み、アクセス制御情報は、アクセス制御デバイスが、記憶装置上に格納されたデータを、その記憶装置にアクセスしようとしているエンティティに入手可能にする時点を制御するために利用することができる。アクセス制御デバイスは、記憶装置上に既に格納されているデータを要求する通信、及び与えられたデータが記憶装置上に格納されることを要求する通信を含む、そのようなエンティティからのデータ記憶関連通信に対し、意味のあるように応答しないように記憶装置に命令する等によって、記憶装置が無許可のエンティティと通信するのを防ぐことができる。また、アクセス制御デバイスは暗号情報も含み、記憶装置のハードウェア暗号システムにその情報を選択的にプロビジョニングすることによって、記憶装置上に格納された暗号化されたデータへのアクセスを制御することができる。許可は、アクセス制御デバイスに、アクセスしようとしているエンティティのアイデンティティ（ＩＤ）を認可されたエンティティに関する予め提供されたリストと比較させること等によって、アクセス制御デバイスそのものによって与えることができるか、又はアクセス制御デバイスに通信的に結合され、アクセス中のコンピューターデバイスを経由して、アクセス制御デバイスに許可命令を与えることができる許可コンピューティングデバイスによって与えることができる。
【００１８】
[0023]本明細書において説明される技法は、限定はしないが、記憶装置、及び物理的にかつ通信的に分離可能であるアクセス制御デバイスに焦点を合わせている。実際には、以下に説明されるアクセス制御機構は、分離可能であることが意図されていない単一の記憶装置内の別々の構成要素によって同じように実施することもできるが、そのような場合には、アクセス制御デバイス及び記憶装置が物理的に分離されるときに存在するセキュリティに関する利点が存在しないことがある。しかしながら、そのようなセキュリティに関する利点は、以下に説明されるアクセス制御機構によって提供されるセキュリティから独立しており、それゆえ、以下に説明される機構の適用性を特定のハードウェア構成には限定しない。したがって、以下の説明は、物理的に分離可能なアクセス制御デバイスに関連付けられる記憶装置を参照するが、説明そのものの範囲は、そのように限定されることは意図されていない。
【００１９】
[0024]さらに、必要ではないが、以下の説明は、包括的には、１つ又は複数の処理ユニットによって実行される、プログラムモジュールのようなコンピューター実行可能命令との関連において行なわれる。より具体的には、その説明は、他に指示されない限り、１つ又は複数の処理ユニットによって実行される動作、及び演算の記号表現を参照する。したがって、時にはコンピューターによって実行されるものとして参照されるそのような動作及び演算は、処理ユニットによる、構造化された形態のデータを表す電気信号の操作を含むことは理解されよう。この操作は、データを変換するか、又はデータをメモリー内の位置に保持し、それにより、処理ユニット又は処理ユニットに接続される周辺装置の演算を、当業者によって十分に理解されるようにして再構成するか、又は別の方法で変更する。データが保持されるデータ構造は、データのフォーマットによって定義される特定の特性を有する物理的な位置である。
【００２０】
[0025]包括的には、プログラムモジュールは、特定のタスクを実行するか、又は特定の抽象データ型を実施するルーチン、プログラム、オブジェクト、コンポーネント、データ構造等を含む。さらに、参照される処理ユニットは、従来のパーソナルコンピューティン

グ処理ユニットに限定される必要はなく、周辺装置、ハンドヘルドデバイス、マルチプロセッサーシステム、マイクロプロセッサーに基づく家庭電化製品、又はプログラム可能な家庭電化製品において多くの場合に見られる専用プロセッサー、特定用途プロセッサー、通信プロセッサー、バスプロセッサー、コントローラー等を含む、他のプロセッサー構成を含むことは当業者には理解されよう。同様に、その機構は、通信ネットワークを通じてリンクされる遠隔処理デバイスによってタスクが実行される分散コンピューティング環境において実施することもできるので、以下の説明において参照されるコンピューティングデバイスは、独立型コンピューティングデバイスに限定される必要はない。分散コンピューティング環境では、プログラムモジュールは、局所及び遠隔両方の記憶装置内に配置することができる。

【００２１】

[0026]図１を参照すると、１つの例示的なプロビジョニングコンピューティングデバイス１１０及び１つの例示的なアクセス制御デバイス１７０を備える１つの例示的なシステム１００が示される。後に説明されるように、プロビジョニングコンピューティングデバイス１１０を用いて、アクセス制御デバイスに情報を与えること等によって、アクセス制御デバイス１７０をプロビジョニングすることができ、その情報によって、アクセス制御デバイスが関連付けられる記憶装置へのアクセスを制限できるようになる。

【００２２】

[0027]最初に、プロビジョニングコンピューティングデバイス１１０を参照すると、そのデバイスは、限定はしないが、１つ又は複数の中央処理ユニット（ＣＰＵ）１２０と、システムメモリー１３０と、システムメモリー１３０を含む種々のシステム構成要素を処理ユニット１２０に結合するシステムバス１２１とを備えることができる。システムバス１２１は、種々のバス又はポイント・ツー・ポイントアーキテクチャーのいずれかを用いる、メモリーバス又はメモリーコントローラー、周辺装置バス及びローカルバスを含む、いくつかのタイプのバス構造のいずれかとすることができる。具体的な物理的実施態様によるが、ＣＰＵ１２０及びシステムメモリー１３０のうちの１つ又は複数は、シングルチップ上等の、物理的に同じ場所に配置することができる。そのような事例では、システムバス１２１のうちのいくつか又は全てが、シングルチップ構造内のシリコン経路にすぎない可能性があり、図１の例示は、厳密には、例示するための表記上の便宜的なものとすることができる。

【００２３】

[0028]プロビジョニングコンピューティングデバイス１１０は通常、コンピューター読み取り可能な媒体も含み、コンピューター読み取り可能な媒体は、プロビジョニングコンピューティングデバイス１１０のようなコンピューティングデバイスによってアクセスすることができる任意の入手可能な媒体を含むことができ、揮発性媒体及び不揮発性媒体の両方、並びに取り外し可能な媒体及び取り外し不能な媒体の両方を含む。限定ではなく、例として、コンピューター読み取り可能な媒体は、コンピューター記憶媒体及び通信媒体を含むことができる。コンピューター記憶媒体は、コンピューター可読命令、データ構造、プログラムモジュール又は他のデータのような情報を記憶するための任意の方法又は技術において実現される媒体を含む。コンピューター記憶媒体は、限定はしないが、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリー又は他のメモリー技術、ＣＤ－ＲＯＭ、デジタルバーサタイルディスク（ＤＶＤ）若しくは他の光ディスク記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置若しくは他の磁気記憶装置、固体ディスク（ＳＳＤ）若しくは他の固体ベース記憶装置、又は所望の情報を格納するために用いることができ、かつプロビジョニングコンピューティングデバイス１１０のようなコンピューティングデバイスによってアクセスすることができる任意の他の媒体を含む。通信媒体は通常、搬送波又は他の移送機構のような被変調データ信号においてコンピューター可読命令、データ構造、プログラムモジュール及び他のデータを具現し、任意の情報配信媒体を含む。限定ではなく、例として、通信媒体は、有線ネットワーク又は直接有線接続のような有線媒体、並びに音響、ＲＦ、赤外線及び他の無線媒体のような無線媒体を含む。上記のいずれ

の組み合わせも、コンピューター読み取り可能な媒体の範囲に含まれるべきである。

【００２４】

[0029]システムメモリー１３０は、リードオンリーメモリー（ＲＯＭ）１３１及びランダムアクセスメモリー（ＲＡＭ）１３２のような揮発性メモリー及び／又は不揮発性メモリーの形態のコンピューター記憶媒体を含む。起動中等に、コンピューティングデバイス１００内の構成要素間で情報を転送するのに役に立つ基本ルーチンを含む、基本入力／出力システム１３３（ＢＩＯＳ）が通常、ＲＯＭ１３１に格納される。ＲＡＭ１３２は通常、処理ユニット１２０によって直ちにアクセス可能であり、かつ／又は現時点で操作されているデータ及び／又はプログラムモジュールを含む。限定するのではなく、例として、図１は、オペレーティングシステム１３４、他のプログラムモジュール１３５及びプログラムデータ１３６を示す。フルボリューム暗号化サービス１３７も示されており、実施形態によっては、オペレーティングシステム１３４の一部とすることができる。フルボリューム暗号化サービス１３７によって、プロビジョニングコンピューティングデバイス１１０のようなコンピューティングデバイスが、１つ又は複数のコンピューター可読記憶媒体上に格納された情報の実質的に全て、若しくは全て、又はコンピューティングデバイスのオペレーティングシステム１３４若しくは他の記憶コントローラーによって個々のボリュームとして定義される部分のような、その情報の一部の暗号化を提供できるようになる。

【００２５】

[0030]オプションで、フルボリューム暗号サービス１３７を含むことに加えて、プロビジョニングコンピューティングデバイス１１０のオペレーティングシステム１３４は、記憶装置ドライバースタック１３８を含むこともできる。記憶装置ドライバースタック１３８は、後に説明されるような、１つ又は複数の記憶装置との通信を確立し、保持することに関連するコンピューター可読命令を含むことができる。さらに、記憶装置ドライバースタック１３８は、アクセス制御デバイス拡張部１３９を含むことができ、アクセス制御デバイス拡張部は、アクセス制御デバイス１７０のようなアクセス制御デバイスとの通信を確立し、保持することに関連するコンピューター実行可能命令を含むことができる。記憶装置ドライバースタックが、アクセス制御デバイス１７０のようなアクセス制御デバイスがプロビジョニングコンピューティングデバイス１１０に通信的に結合されるという指示を受信する場合には、記憶装置ドライバースタック１３８によって、アクセス制御デバイス拡張部１３９を要求しロードすることができる。後に説明されるように、アクセス制御デバイス１７０のようなアクセス制御デバイスは、プロビジョニングコンピューティングデバイス１１０のようなコンピューティングデバイスに、有線通信接続又は無線通信接続等を通じて直に、又はアクセス制御デバイスが通信的に結合される記憶装置のような別の中間のデバイスを通じて通信的に結合することができる。

【００２６】

[0031]プロビジョニングコンピューティングデバイス１１０は、上記で説明されたものに加えて、取り外し可能／取り外し不能、揮発性／不揮発性コンピューター記憶装置を含む、記憶装置を含むことができる。例にすぎないが、図１は、ハードディスク記憶装置１４１、１４６及び１４７を示しており、それらのハードディスク記憶装置は、取り外し不能、不揮発性磁気媒体に対する読出し又は書込みを行う。例示的なコンピューティングデバイスとともに用いることができる他の取り外し可能／取り外し不能、揮発性／不揮発性コンピューター記憶媒体には、限定はしないが、磁気テープカセット、フラッシュメモリーカード、固体ドライブ（ＳＳＤ）及び他の固体ベースの記憶装置、デジタルバーサタイルディスク、デジタルビデオテープ、固体ＲＡＭ、固体ＲＯＭ等が含まれ。ハードディスク記憶装置１４１、１４６及び１４７、又はこれらの他の取り外し可能／取り外し不能、揮発性／不揮発性コンピューター記憶媒体のいずれかは通常、インターフェース１４０のようなメモリーインターフェースを通じて、システムバス１２１に直接的に又は間接的に接続される。図１に示される例示的なプロビジョニングコンピューティングデバイス１１０では、ハードディスク記憶装置１４１は、プロビジョニングコンピューティングデバイス１１０の内部にある物理的接続、又はポートを介して露出される外部接続等を通じて、

不揮発性メモリーインターフェース１４０に直に接続されるように示されており、一方、ハードディスク記憶装置１４６及び１４７は、例えば、低価格デバイス冗長アレイ（ＲＡＩＤ：Redundant Array of Inexpensive Devices）コントローラーのような、記憶装置ホストコントローラーに接続されているものとして示されており、そして、そのコントローラーは更に、再びコンピューティングデバイス１００の物理的に内部にある接続等を通じてインターフェース１４０に接続することができる。不揮発性メモリーインターフェース１４０は、限定はしないが、ユニバーサルシリアルバス（ＵＳＢ）インターフェース、ＩＥＥＥ１３９４仕様書のうちの任意の１つ若しくは複数に準拠するインターフェース、シリアルＡＴアタッチメント（ＳＡＴＡ）インターフェース、又は他の同様のインターフェースを含む、任意の不揮発性メモリーインターフェースとすることができる。

【００２７】

[0032]プロビジョニングコンピューティングデバイス１１０は、１つ又は複数のリモートコンピューティングデバイスに対する論理的接続を用いて、ネットワーク接続環境において動作することができる。図示を簡単にするために、プロビジョニングコンピューティングデバイス１１０は、図１において、ネットワーク１５５に接続されるように示されており、そのネットワークはいかなる特定のネットワーク又はネットワーキングプロトコルにも限定されない。図１に示される論理的接続は汎用ネットワーク接続１５１であり、その接続は、ローカルエリアネットワーク（ＬＡＮ）、ワイドエリアネットワーク（ＷＡＮ）又は他のネットワークとすることができる。プロビジョニングコンピューティングデバイス１１０は、ネットワークインターフェース又はアダプター１５０を通じて汎用ネットワーク接続１５１に接続され、そのインターフェース又はアダプターは更に、システムバス１２１に接続される。ネットワーク接続環境では、プロビジョニングコンピューティングデバイス１１０、又はその一部若しくは周辺装置に関して示されるプログラムモジュールは、１つ又は複数のコンピューティングデバイスのメモリーに格納することもでき、そのコンピューティングデバイスは、汎用ネットワーク接続１５１を通じてプロビジョニングコンピューティングデバイス１１０に通信的に結合される。例えば、以下に更に詳細に説明されるような、許可コンピューティングデバイスが、その動作が以下に説明されるコンピューター実行可能命令のうちのいくつか又は全てのためのホストとしての役割を果たすことができる。図示されるネットワーク接続は例示であり、コンピューティングデバイス間に通信リンクを確立する他の手段を用いることもできることは理解されよう。

【００２８】

[0033]以下の説明に関連するプロビジョニングコンピューティングデバイス１１０は、図１に示されるアクセス制御デバイス１７０のような、アクセス制御デバイスに通信的に結合することができる。アクセス制御デバイス１７０は、有線又は無線接続等を通じて、プロビジョニングコンピューティングデバイス１１０に直に通信的に結合することができるか、又はアクセス制御デバイスは、アクセス制御デバイスが直に通信的に結合される記憶装置を通じて、プロビジョニングコンピューティングデバイスに間接的に通信的に結合することができる。図１のシステム１００では、アクセス制御デバイス１７０は、不揮発性メモリーインターフェース１４０等を通じて、プロビジョニングコンピューティングデバイス１１０に直に通信的に結合されるように示される。図１の破線は、アクセス制御デバイス１７０をプロビジョニングコンピューティングデバイス１１０に取外し可能に通信的に結合することができることを示す。一実施形態では、製造効率のために、アクセス制御デバイス１７０は標準的なメモリーカード仕様に準拠することができ、したがって、例えば、内部メモリーカードリーダを通じて、又はプロビジョニングコンピューティングデバイスに通信的に接続される外部メモリーカードリーダ周辺装置を通じて、同じ仕様に準拠する任意の他のそのようなメモリーカードと同じようにして、プロビジョニングコンピューティングデバイス１１０に通信的に結合することができる。

【００２９】

[0034]アクセス制御デバイス１７０は１つ又は複数の処理ユニット１７１を備えることができ、その処理ユニットは一群の入力に基づいてその出力を調整することができるコン

トローラー又は他の構成要素を含むことができる。後に更に説明されるように、アクセス制御デバイス１７０の処理ユニット１７１を用いて、関連する記憶装置が、その記憶装置が通信的に接続されるアクセス中のコンピューティングデバイスにデータを与えるのを許可し、それを可能にするか否か、又はそのコンピューティングデバイスからのデータを格納するのを許可し、それを可能にするか否かを判断することに関連する動作を実行することができる。

【００３０】

[0035]そのようなゲートキーピングに関連する動作を実行する際に、アクセス制御デバイス１７０の処理ユニット１７１は、システム１００内に示されるように、プロビジョニングコンピューティングデバイス１１０によって提供することができるアクセス制御情報１７６を利用することができる。一実施形態では、アクセス制御情報１７６は、アクセス制御デバイス１７０の暗号情報を用いて暗号化されたデータへのアクセス許可を受けることができるエンティティのリストを含むことができ、その結果として、そのようなエンティティがアクセスを要求しているとアクセス制御デバイスが判断するときに、そのアクセス制御デバイスによって、関連する記憶装置が、要求しているエンティティのアクセスを許すことができるようになる。例えば、アクセス制御情報１７６は、媒体アクセス制御（ＭＡＣ）アドレス、ワールドワイドネーム（ＷＷＮ）、又は他の固有のデバイス若しくはエンティティ識別子のような、識別子のリストを含むことができる。アドレス制御情報１７６は、エンティティのパスワードも含むことができ、それにより、アクセス制御デバイスが暗号情報を公開する前に、そのパスワードを与えることによって、エンティティに、アクセス制御デバイス１７０に対してアイデンティティを証明するように要求することができる。類似のチャレンジ／レスポンステンプレートに基づく他の機構を含む、他の暗号機構も同じように用いて、アクセス制御デバイス１７０に対して、そのアクセス制御デバイス１７０が通信的に結合される記憶装置によって格納されたデータにアクセスしようとしているエンティティの認証を与えることができる。

【００３１】

[0036]一実施形態では、アクセス制御デバイス１７０は更に、記憶関連暗号情報１７５を含むことができ、その情報は、記憶装置によって、そのような記憶装置の記憶媒体上に格納されることになるデータを暗号化するために、かつ記憶媒体上に既に格納されている暗号化されたデータを暗号解読するために用いることができる。そのような場合に、その記憶装置へのアクセスを要求しているエンティティ及びそのデータが、アクセス制御情報１７６によってアクセスを許されることを示されるエンティティのうちの１つであることをアクセス制御デバイスが判断するまで、記憶装置に暗号情報を提供しないことによって、アクセス制御デバイス１７０は、記憶関連暗号情報１７５を用いて、記憶装置のデータへのアクセスを制御することができる。アクセス制御情報１７６が、許容できるエンティティのリスト、又はアクセスが拒否されるべきエンティティのリストを含む実施形態は、データにアクセスすることができるエンティティが限られ、相対的に動きのないホーム又は小規模のビジネス環境において特に役に立つ。

【００３２】

[0037]しかしながら、代替の実施形態では、アクセス制御デバイスが通信的に結合される記憶装置へのアクセスを許すか否かを判断するときに、許可コンピューティングデバイスのような、アクセス制御デバイス１７０の外部のコンピューティングデバイスを、アクセス制御デバイスによって参照することができる。そのような実施形態では、アクセス制御デバイス１７０は、アクセスを許すべきとき、又は許すべきでないときを命令するのに、許可コンピューティングデバイスに頼ることができる。当業者によって認識されるように、そのような実施形態は、特定のデータへのアクセス許可を受けることができるエンティティが、その時々で変化する企業環境において役に立つことができる。さらに、後に更に説明されるように、アクセス制御デバイス１７０が別のコンピューティングデバイスを参照する実施形態は、企業によって通常実施される既存のアクセス制御技術と統合することができる。

【００３３】
[0038]上記の実施形態において、プロビジョニングコンピューティングデバイス１１０によってアクセス制御デバイス１７０に与えられるアクセス制御情報１７６は、許可コンピューティングデバイスとの安全な通信の確立に関する情報を含むことができる。例えば、アクセス制御情報１７６は、許可コンピューティングデバイスの公衆アクセス制御のような暗号情報、又はアクセス制御デバイス１７０が許可コンピューティングデバイスとの安全な通信を提供するために用いる共用の秘密又は他のそのような暗号手段をネゴシエートすることができる他のそのような情報を含むことができる。アクセス制御情報１７６は、許可コンピューティングデバイスのドメインネームサーバー（ＤＮＳ）名又はそのネットワークアドレスのような、許可コンピューティングデバイスの識別情報（identification）も含むことができる。以下に更に説明される代替の実施形態では、そのような識別用情報（identifying information）は、代わりに、アクセス制御デバイス１７０が通信的に結合される記憶装置上のデータにアクセスしようとしているコンピューティングデバイスに与えることができる。

【００３４】
[0039]システム１００において示されるように、一実施形態では、プロビジョニングコンピューティングデバイス１１０のオペレーティングシステム１３４は、記憶装置ドライバースタック１３８を用いて、アクセス制御デバイス１７０と通信することができる。より具体的には、示されるように、記憶装置ドライバースタック１３８は、記憶装置ドライバースタックがアクセス制御デバイス１７０の存在を検出するときに、アクセス制御デバイス拡張部１３９を呼び出すか、又は他の方法でロードすることができる。アクセス制御デバイス拡張部１３９は、その際、アクセス制御情報１７６のプロビジョンを含む、アクセス制御デバイス１７０との通信を処理することができる。一実施形態では、図示されるように、プログラムモジュール１３５の一部とすることができる、セキュリティ関連プログラムのような１つ又は複数のプログラムが、アクセス制御デバイス拡張部１３９に、そしてそこからアクセス制御デバイス１７０に、アクセス制御情報１７６を与えることができ、その情報は、上記のように、アクセスが許されるべきエンティティのリストを含むことができるか、又は、同じく上記のように、暗号情報を含む、アクセス制御デバイス１７０の外部にある許可コンピューティングデバイスとの安全な通信接続を確立し、保持するための情報を含むことができる。

【００３５】
[0040]プロビジョニングコンピューティングデバイス１１０は、例えば、アクセス制御デバイス拡張部１３９を通じて、アクセス制御デバイス１７０にアクセス制御情報１７６をプロビジョニングすることができ、オプションでは、アクセス制御デバイスに記憶関連暗号情報１７５もプロビジョニングすることができる。記憶関連暗号情報１７５、及び関連付けられる通信は、オプションであることを指示するために、システム１００において破線で示される。アクセス制御デバイス１７０が記憶装置から通信的に切断されている場合には、記憶関連暗号情報１７５が存在しないと、そのような記憶装置の記憶媒体上に格納された暗号化されたデータへのアクセスを不可能にすることができる。その結果として、そのような記憶装置からのアクセス制御デバイス１７０の通信の切断は、記憶装置が物理的に紛失又は盗難される場合の付加的な保護層を提供することができ、それは、そのような記憶装置の記憶媒体上に格納された暗号化されたデータの暗号消去又は破壊の証拠としての役割を果たすことができる。

【００３６】
[0041]一実施形態では、記憶関連暗号情報１７５は、「物理アドレス制御」を含むことができ、物理アドレス制御は、当業者に既知であるような暗号化演算及び暗号解読演算のためのアクセス制御として利用することができる一連のビットとすることができる。それゆえ、用語「物理アドレス制御」は、以下の説明において、アクセス制御デバイス１７０のような、物理的に取外し可能な情報源から与えられ、かつ該情報源に格納された暗号アクセス制御として利用される一群のデータを指すように意図される。そのような物理アド

レス制御は、「論理アドレス制御」と対照を成すことが意図されており、論理アドレス制御は、そのようなアクセス制御を用いて暗号化されたデータが格納された媒体とは物理的に分離することはできない。

【００３７】

[0042]プロビジョニングコンピューティングデバイス１１０によってアクセス制御デバイス１７０にオプションでプロビジョニングされる記憶関連暗号情報１７５は、アクセス制御デバイス拡張部１３９を通じて、プロビジョニングコンピューティングデバイスの複数のサブシステムのうちのいずれか１つが与えることができる。例えば、論理アクセス制御を利用することに加えて、フルボリューム暗号化サービス１３７は、その既存の機能を活用して、物理アクセス制御を生成し、それを、記憶関連暗号情報１７５の少なくとも一部としてアクセス制御デバイス１７０に与えることができる。代替的には、物理アクセス制御、又は他の記憶関連暗号化情報１７５は、記憶装置ホストコントローラー１４５又は他の記憶装置インターフェース内に存在することができるハードウェアのような、専用ハードウェアによって生成することができる。更に別の代替形態として、記憶関連暗号情報１７５は、ＢＩＯＳ１３３からアクセス制御デバイス１７０に与えることができる。

【００３８】

[0043]アクセス制御デバイス１７０に与えられるオプションの記憶関連暗号情報１７５の安全性及び秘密性（secrecy）を保持するために、そのような情報は、プロビジョニングコンピューティングデバイス１１０上で実行される悪意のあるコンピューター実行可能命令等を通じて、敵対者によってそのような情報が入手される可能性を最小限に抑えるようにして、プロビジョニングコンピューティングデバイス１１０によって与えることができる。それゆえ、一実施形態では、アクセス制御デバイス１７０に与えられる記憶関連暗号情報１７５は、プロビジョニングコンピューティングデバイス１１０のブートが完了する前に与えることができ、与えられた情報は、同じくプロビジョニングコンピューティングデバイスのブートが完了する前にプロビジョニングコンピューティングデバイスから消去することができる。悪意のあるコンピューター実行可能命令は通常、ホストコンピューティングデバイスのブートが完了する前に動作することはできないので、プロビジョニングコンピューティングデバイス１１０のブートが完了する前に、アクセス制御デバイス１７０に記憶関連暗号情報１７５を与え、その後、破棄することによって、プロビジョニングコンピューティングデバイス上でその後に実行される可能性がある任意の悪意のあるコンピューター実行可能命令から、与えられた情報を保護することができる。

【００３９】

[0044]例えば、ＢＩＯＳ１３３は、プロビジョニングコンピューティングデバイス１１０のインターフェースに通信的に接続されるアクセス制御デバイス１７０の存在を検出することができ、例えば、オペレーティングシステム１３４の実行の開始を含む、プロビジョニングコンピューティングデバイス上で任意の他の処理を開始する前に、アクセス制御デバイス１７０に記憶関連暗号情報１７５を与えることができる。同様に、記憶装置ホストコントローラー１４５は、コントローラーが最初に初期化されるときに、かつオペレーティングシステム１３４のブートの開始前とはいかないまでも、少なくともその完了前に、アクセス制御デバイス１７０の存在を検出することができる。その際、コントローラー１４５は、同じように、プロビジョニングコンピューティングデバイス１１０上で任意の悪意のあるコンピューター実行可能命令が実行可能になる前に、アクセス制御デバイス１７０に記憶関連暗号情報１７５を与えることができ、それを破棄することができる。別の代替形態として、フルボリューム暗号化サービス１３７は、プロビジョニングコンピューティングデバイス１１０上で実行される悪意のあるコンピューター実行可能命令からその論理アクセス制御を保護するように設計される機構を既に備える可能性があるので、それらの機構を利用して、アクセス制御デバイス１７０に記憶関連暗号情報１７５を安全にプロビジョニングすることができ、その後にその情報を破棄して、プロビジョニングコンピューティングデバイス１１０上でその情報が発見される確率を更に小さくすることができる。そのような実施形態では、アクセス制御デバイス拡張部１３９を参照して上記で説明

された機能のうちの少なくともいくつかを、ＢＩＯＳ１３３又は記憶装置ホストコントローラー１４５等によって、オペレーティングシステム１３４の外部で実施することができる。

【００４０】

[0045]アクセス制御デバイス１７０がプロビジョニングコンピューティングデバイス１１０によってプロビジョニングされると、アクセス制御デバイス１７０は、プロビジョニングコンピューティングデバイス１１０から通信的に切断することができ、かつオプションでは物理的に切り離すことができ、その後、記憶装置とともに利用して、記憶装置が暗号化されたデータを格納できるようにし、かつそのような記憶装置のコンピューター読み取り可能な媒体上に既に格納されている暗号化されたデータにアクセスできるようにすることができる。

【００４１】

[0046]図２を参照すると、アクセス中のコンピューターデバイス２１０と、アクセス制御デバイス１７０と、アクセス制御デバイスが通信的に結合することができる１つの例示的な記憶装置２７０とを備えるシステム２００が示されている。以下で更に説明されるように、アクセス制御デバイス１７０と例示的な記憶装置２７０との間の通信可能な結合は、そうである必要はないが、物理的結合とすることができる。例示的な記憶装置２７０は、記憶装置２４１、２４６又は２４７のうちのいずれか１つ又は複数を表すことができ、それらの記憶装置は、アクセス中のコンピューティングデバイス２１０に通信的に結合されるように示される。アクセス中のコンピューティングデバイス２１０は、上記で詳細に説明されたプロビジョニングコンピューティングデバイス１１０とは異なるコンピューティングデバイスとすることもできるし、同じコンピューティングデバイス、例えば、それをプロビジョニングコンピューティングデバイスとして用いることができる管理者、及びそれをアクセス中のコンピューティングデバイスとして用いることができるユーザーの両方によって利用されるコンピューティングデバイス等とすることもできる。それゆえ、参照及び図示を容易にするために、プロビジョニングコンピューティングデバイス２１０の構成要素は、コンピューティングデバイス１１０の類似の構成要素と異なるように符号を付されるが、その機能は同様であるか、又は同じである場合もある。それゆえ、ＣＰＵ２２０、システムバス２２１、システムメモリー２３０、オプションの不揮発性メモリーインターフェース２４０及び記憶装置ホストコントローラー２４５は全て、上記のＣＰＵ１２０、システムバス１２１、システムメモリー１３０、インターフェース１４０及び記憶装置ホストコントローラー１４５と同様である。同様に、ＢＩＯＳ２３３を有するＲＯＭ２３１、並びに記憶装置ドライバースタック２３８及びアクセス制御デバイス拡張部２３９を含むオペレーティングシステム２３４と、プログラムモジュール２３５と、プログラムデータ２３６とフルボリューム暗号化サービス２３７とを有するＲＡＭ２３２も、上記のＲＯＭ１３１、ＢＩＯＳ１３３、ＲＡＭ１３２、オペレーティングシステム１３４、記憶装置ドライバースタック１３８、アクセス制御デバイス拡張部１３９、プログラムモジュール１３５、プログラムデータ１３６及びフルボリューム暗号化サービス１３７に類似である。しかしながら、アクセス制御デバイス１７０は、上記で詳細に説明された同じアクセス制御デバイスとすることができる。

【００４２】

[0047]図２のシステム２００の記憶装置２７０を参照すると、記憶装置２７０は、上記の記憶装置１４１、１４６及び１４７のいずれかと同じように用いることができ、そのいずれかの代わりに用いることができるか、又はそのいずれかの役割を果たすことができ、その類似の装置が図２において記憶装置２４１、２４６及び２４７として示される。実際には、直ぐ近くにあるその図式的な配置によって示されるように、記憶装置２７０は、アクセス中のコンピューティングデバイス２１０に通信的に結合される記憶装置２４１、２４６及び２４７のうちのいずれか１つ又は複数を、更に詳細に表すことを意図している。

【００４３】

[0048]記憶装置２７０は、１つ又は複数のコンピューター読み取り可能な媒体２９０を

備えることができ、そのコンピューター読み取り可能な媒体は、上記のいずれか１つを含む、取り外し不能、不揮発性磁気媒体、取り外し不能、不揮発性固体ベース記憶媒体、又は他の取り外し可能／取り外し不能、揮発性／不揮発性コンピューター記憶媒体を含むことができる。記憶装置２７０のコンピューター読み取り可能な媒体２９０は、コンピューティングデバイスによって、そのようなコンピューティングデバイスのためのコンピューター可読命令、データ構造、プログラムモジュール及び他のデータを格納するために用いることができる。例えば、記憶装置２７０のコンピューター読み取り可能な媒体２９０は、データ２９５を格納するように示されており、そのデータは、記憶装置２７０によって与えられるときに、アクセス中のコンピューティングデバイス２１０のオペレーティングシステム２３４、他のプログラムモジュール２３５又はプログラムデータ２３６のうちのいくつか又は全てのための基礎であるデータとすることができる。

【００４４】

[0049]コンピューター読み取り可能な媒体２９０に加えて、例示的な記憶装置２７０はオプションでハードウェア暗号システム２８０も備えることができ、ハードウェア暗号システムは、コンピューター読み取り可能な媒体２９０に格納するために記憶装置２７０に与えられるデータを暗号化することができ、コンピューター読み取り可能な媒体から読み出され、その後に、アクセス中のコンピューティングデバイス２１０に与えられることになるデータを暗号解読することができる。したがって、ハードウェア暗号システム２８０は、ＣＰＵ２２０又はアクセス中のコンピューティングデバイス２１０の他の構成要素に負荷をかけることなく、その暗号機能を実行することができ、アクセス中のコンピューティングデバイスは、一実施形態において、データ暗号化及び暗号解読を気にすることなく、任意の他の記憶装置と同じようにして、記憶装置２７０を取り扱うことができる。さらに、アクセス中のコンピューティングデバイス２１０がフルボリューム暗号化サービス２３７のような関連する暗号構成要素を備えない場合であっても、関連するアクセス制御デバイス１７０の記憶関連暗号情報１７５をハードウェア暗号システム２８０によって管理することができる。ハードウェア暗号システム２８０は、アクセス制御デバイス１７０の記憶関連暗号情報１７５と同様に、オプションの構成要素であることを示すために、図２において破線で示される。

【００４５】

[0050]しかしながら、記憶装置２７０のハードウェア暗号システム２８０はオプションとすることができるが、１つ又は複数の処理ユニット２８１及びファームウェア２８３のような、下位構成要素として示される他の構成要素は、ハードウェア暗号システムの存在とは関係なく、存在することができる。より具体的には、一実施形態では、処理ユニット２８１及びファームウェア２８３は、記憶装置２７０に、例えば、種々のメンテナンス及び通信タスクのような、少なくとも基本的な命令を独立して処理する能力を与えることができる。しかしながら、別の実施形態では、処理ユニット２８１及びファームウェア２８３は、記憶装置に与えられるデータの暗号化及びコンピューター読み取り可能な媒体２９０から読み出されるデータの暗号解読のような、暗号機能を実行するために少なくとも一部を利用することができる。そのような実施形態では、処理ユニット２８１及びファームウェア２８３は、少なくとも部分的に、ハードウェア暗号システム２８０の一部と見なすことができる。さらに、アクセス制御デバイス１７０の処理ユニット１７１の場合のように、記憶装置２７０の処理ユニット２８１は、コントローラー、又は一群の入力に基づいてその出力を調整することができる他の構成要素を含むことができる。

【００４６】

[0051]アクセス制御デバイス１７０の記憶関連暗号情報１７５は、それが存在する実施形態では、記憶装置２７０のハードウェア暗号システム２８０が参照することができ、ハードウェア暗号システムによって実行された暗号化及び暗号解読を通知することができる。一実施形態では、ハードウェア暗号システム２８０は、アクセス制御デバイス１７０の記憶関連暗号情報１７５、及び例えば、アクセス中のコンピューティングデバイス２１０において実行されるフルボリューム暗号化サービス２３７、又は別の同様の暗号システム

によって与えられるような、付加的な暗号情報の両方を参照して、その暗号機能を実行することができる。

【００４７】

[0052]上記で詳細に説明した方法等で予めプロビジョニングすることができるアクセス制御デバイス１７０は、図２の破線の双方向通信矢印によって示されるように、記憶装置２７０に通信的に接続することができる。後に更に説明されるように、アクセス制御デバイス１７０と記憶装置２７０との間のそのような通信接続は、有線又は無線とすることができ、直接的にすることもできるし、アクセス中のコンピューティングデバイス２１０等を通じて間接的にすることもできる。

【００４８】

[0053]アクセス中のコンピューティングデバイス２１０は、記憶装置に適切な読出しコマンドを送信することによって、記憶装置２７０のデータ２９５へのアクセスを試みることができる。アクセス制御デバイス１７０がまだ記憶装置２７０に通信的に接続されていない場合には、一実施形態において、記憶装置は、データ２９５へのアクセスを提供できないことを、アクセス中のコンピューティングデバイス２１０に通知することができる。しかしながら、代替の実施形態では、アクセス制御デバイス１７０が存在しない場合、記憶装置２７０を従来通りに利用できるようにすることができる。アクセス制御デバイス１７０が記憶関連暗号情報１７５を含む場合に、そのような実施形態において、アクセス制御デバイスが記憶装置に通信的に結合されない場合には、暗号化されたデータを暗号解読するために、記憶装置のハードウェア暗号システム２８０によって必要とされる記憶関連暗号情報１７５が入手できないので、記憶装置は、データ２９５（そのような実施形態では、暗号化された形にある）にアクセスできないことをアクセス中のコンピューティングデバイス２１０に通知することができる。一方、アクセス制御デバイス１７０が記憶装置２７０に通信的に結合されている場合には、アクセス制御デバイスは、記憶装置２７０がアクセス中のコンピューティングデバイス２１０にデータ２９５へのアクセスを提供できるか否かを判断することもできるし、それに関する判断を受信することもできる。そのようなアクセスは、アクセス制御デバイス１７０によって通知されるか又は呼び出され、アクセス中のコンピューティングデバイス２１０がデータ２９５にアクセスするのを拒否するように動作する処理ユニット２８１等が、命令の実行を通じて拒否することができる。それに加えて又はその代わりに、そのようなアクセスは、暗号化されたデータを暗号解読するために必要とされる記憶関連暗号情報１７５へのアクセスを拒否することを通じて拒否することができる。

【００４９】

[0054]記憶装置２７０は、適切な記憶関連通信プロトコルを利用してアクセス制御を実施しているアクセス制御デバイス１７０の存在をアクセス中のコンピューティングデバイスに通知することができる。後に更に説明されるように、記憶装置２７０は、記憶装置の記憶媒体２９０上に格納されたデータ２９５へのアクセスを試みるのに応答して、アクセス中のコンピューティングデバイス２１０にエラーメッセージを返すことができる。そのようなエラーメッセージは、アクセス中のコンピューティングデバイス２１０に、通信的に結合されるアクセス制御デバイス１７０の存在を示すことができる。記憶装置２７０と通信するためにオペレーティングシステム２３４によってロードされた記憶装置ドライバースタック２３８によって受信することができるそのようなエラーメッセージに応答して、記憶装置ドライバースタック２３８は、アクセス制御デバイス拡張部２３９を呼び出すこともできるし、別の方法でロードされるようにすることもでき、それにより、その後、アクセス中のコンピューティングデバイス２１０はアクセス制御デバイス１７０と通信できるようになる。アクセス制御デバイス拡張部２３９は、動的ライブラリ（dynamically loaded library）モジュール（ＤＬＬ）、プリロード済みルーチン、又は任意の他のランタイム制限実行可能コンピューターコードとして実装することができる。

【００５０】

[0055]図２のシステム２００によって示されるような一実施形態では、アクセス中のコ

ンピューティングデバイス２１０のアクセス制御デバイス拡張部２３９は、アクセス制御デバイス１７０と通信し、情報を与えて、アクセス制御デバイスの処理ユニット１７１が、アクセス制御デバイスがプロビジョニングされたアクセス制御情報１７６に基づいて、アクセス制御を決定できるようにする。例えば、アクセス制御デバイス１７０によって要求され、かつアクセス制御デバイス１７０に与えられる情報は、アクセス中のコンピューティングデバイス２１０又は記憶装置２７０の識別用情報を含むことができる。そのような識別用情報によって、アクセス制御デバイス１７０は、例えば、アクセス制御情報１７６に基づいて、アクセス中のコンピューティングデバイス２１０及び記憶装置２７０が認可されたエンティティであるか否かを判断できるようになる可能性がある。そのようにして、データ２９５へのアクセスは、安全なエリア内にあるデバイス、又はＷＡＮアクセスを用いないデバイスのような、特定のアクセス中のコンピューティングデバイス２１０のみに制限することができる。別の例として、信頼性及び性能の理由から、上記の記憶装置ホストコントローラー１４５に類似の記憶装置ホストコントローラー２４５のようなコントローラーの製造業者は、そのコントローラーとともに特定のタイプの記憶装置だけが利用されることを要求することができる。そのような事例では、関連付けられた記憶装置２７０に相互使用を認めることができる１つ又は複数のコントローラーの１つ又は複数の識別子を、アクセス制御デバイス１７０にアクセス制御情報１７６の形でプロビジョニングすることができる。代替的には、記憶装置２７０のような特定の記憶装置、及び相互使用を認められるアクセス中のコンピューティングデバイス２１０の記憶装置ホストコントローラー２４５のような特定のコントローラーの識別子をアクセス制御デバイス１７０にプロビジョニングすることができる。記憶装置及びアクセス中のコンピューティングデバイスの両方がそれぞれ、アクセス制御情報１７６によって指定されるような、認可されたエンティティである場合であっても、記憶装置２７０が適切なアクセス中のコンピューティングデバイス２１０に通信的に接続されることを確認することによって、データ２９５へのアクセスをそのように制限することができる。

【００５１】

[0056]別の実施形態では、暗号化された状態において格納することができる、記憶装置２７０内のデータ２９５の個々の区画、又は他のセグメンテーションを、提供された記憶関連暗号情報及びアクセスを参照して独立して暗号解読することができるように、アクセス制御デバイス１７０は複数組の記憶関連暗号情報１７５を含むことができる。そのような実施形態では、アクセス中のコンピューティングデバイスによって提供される情報は、ユーザー名及びパスワードのようなユーザー識別用情報を含むことができ、その情報はアクセス制御デバイス１７０の処理ユニット１７１によって利用され、ユーザーが適切に認証されたか否か、及びアクセス制御情報１７６によって保持されるような認可リスト上にあるか否かを判断することができる。アクセス制御情報１７６は、記憶装置２７０に与えることができる記憶関連暗号情報１７５が、ユーザーがアクセスすることを許可されたコンピューター読み取り可能な媒体２９０の予めフォーマットされた区画によって定義することができるような、暗号化されたデータの部分のみを暗号解読することを、特定のユーザーのために指定することができる。そのような実施形態は、マルチユーザー、又は時分割方式のアクセス中のコンピューターデバイス２１０にとって有用である可能性がある。

【００５２】

[0057]システム２００において示されるように、アクセス中のコンピューターデバイス２１０によって提供される情報は、アクセス制御デバイスがプロビジョニングコンピューティングデバイス１１０によってプロビジョニングされたアクセス制御情報１７６に照らして、アクセス制御デバイス１７０の処理ユニット１７１が考慮することができ、アクセス制御デバイスの処理ユニットは、そのような考慮に基づいて、記憶装置２７０がアクセス中のコンピューティングデバイスからのデータ記憶関連通信に意味のあるように応答するのを許すか否か、またそれにより、アクセス中のコンピューティングデバイス２１０がコンピューター読み取り可能な媒体２９０上のデータ２９５を読み出すのを、又はコンピューター読み取り可能な媒体上に付加的なデータを書き込むのを許すか否かを判断するこ

とができる。一実施形態では、上記のように、記憶装置２７０がデータ記憶関連通信に意味のあるように応答するのを許すか否かの判断は、アクセス制御デバイス１７０の処理ユニット１７１が、ファームウェア２８３からの適切な命令を実行するように記憶装置２７０の処理ユニット２８１に命令することによって実施することができる。例えば、処理ユニット２７１が、アクセス中のコンピューティングデバイス２１０が記憶装置２７０上にデータを格納すること、又はその記憶装置からデータを読み出すことを許されるべきでないと判断した場合には、処理ユニット１７１は、処理ユニット２８１に、コンピューター読み取り可能な媒体２９０にデータを書き込む要求、又はそこに既に格納されているデータ２９５を読み出す要求が拒否されていることをアクセス中のコンピューターデバイス２１０に通知するファームウェア２８３からの命令を実行するように命令することができる。さらに、ファームウェア２８３から実行される命令は、アクセス中のコンピューティングデバイス２１０に、適切なエラーコードのような、否定のための理由の指示を提供することができる。同じく上記で示された別の実施形態では、記憶装置２７０がデータ記憶関連通信に意味のあるように応答するのを許すか否かの判断は、アクセス制御デバイス１７０の処理ユニット１７１が、記憶装置２７０のハードウェア暗号システム２８０の処理ユニット２８１に記憶関連暗号情報１７５を公開するか否かによって、それにより、ハードウェア暗号システム２８０が（暗号化された形で格納された）データ２９５を暗号解読するのを許すか否か、それゆえ、アクセス中のコンピューティングデバイス２１０にそのようなデータへのアクセスを提供するのを許すか否かによって実施することができる。アクセス制御デバイス１７０によって提供されるそのようなアクセス制御は、アクセスできないようにすることに加えて、記憶装置２７０から、記憶関連暗号情報１７５を含む、アクセス制御デバイス１７０との通信を切断することによって、それにより、記憶装置がその上に格納された暗号化されたデータにアクセスできるようにするために、記憶装置に必要な記憶関連暗号情報を提供する任意の能力を通信的に中断することによって果たすことができる。

【００５３】

[0058]図３のシステム３００によって示されるような別の実施形態では、アクセス制御デバイス１７０は、アクセス制御情報１７６によって通知されるような自らの判断に基づくのではなく、アクセス制御デバイス１７０を通信的に結合することができる許可コンピューティングデバイス３１０の判断に基づいて、記憶装置２７０がアクセス中のコンピューティングデバイス２１０からのデータ記憶関連通信に意味のあるように応答するのを許すこともできるし、許さないこともできる。図３を参照すると、システム２００のアクセス中のコンピューティングデバイス２１０と、アクセス制御デバイス１７０と、記憶装置２７０とを備えるシステム３００が示される。しかしながら、それに加えて、システム３００は、ネットワーク１５５等を介して、アクセス中のコンピューティングデバイス２１０に通信的に結合することができる許可コンピューティングデバイス３１０も備えており、アクセス中のコンピューティングデバイス及び許可コンピューティングデバイスはいずれも、ネットワーク１５５に対して、それぞれ別々のネットワーク接続２５１及び３５１を保持する。

【００５４】

[0059]システム３００によって示される実施形態では、アクセス制御デバイス１７０は、アクセス制御情報１７６の一部として、アクセス中のコンピューティングデバイス２１０を通じて許可コンピューティングデバイス３１０へのセキュア通信トンネル３２０を確立するために用いることができるアクセス制御暗号情報３７６を有することができる。上記で説明されたように、アクセス中のコンピューティングデバイス２１０が、記憶装置２７０に格納されたデータ２９５にアクセスしようとするとき、記憶装置は、アクセス制御デバイス１７０の存在をアクセス中のコンピューティングデバイスに通知することができ、それにより、アクセス中のコンピューティングデバイスのオペレーティングシステム２３４の記憶装置ドライバースタック２３８が、アクセス中のコンピューティングデバイスとアクセス制御デバイスとの間の通信を可能にするアクセス制御デバイス拡張部２３９を

ロードすることができるか、又は実行させることができる。それらの通信を通じて、アクセス制御デバイス１７０は、アクセス中のコンピューティングデバイス２１０のアクセス制御デバイス拡張部２３９がアクセス制御デバイスからのメッセージを許可コンピューティングデバイス３１０に送り、逆に、許可コンピューティングデバイスからのメッセージをアクセス制御デバイスに与えることを要求することができる。そのようにして、アクセス制御デバイス１７０は、許可コンピューティングデバイス３１０とのセキュア通信トンネル３２０を確立することができる。

【００５５】

[0060]アクセス制御デバイス１７０からのメッセージを許可コンピューティングデバイス３１０に与えるために、アクセス制御デバイス拡張部２３９は、アクセス中のコンピューティングデバイス２１０のネットワークインターフェース２５０が許可コンピューティングデバイスへの通信接続を確立することを要求することができる。一実施形態では、そのネットワークアドレス又はＤＮＳ名のような、許可コンピューティングデバイス３１０の位置を、アクセス制御デバイス１７０のアクセス制御情報１７６から、アクセス制御デバイス拡張部２３９に、それにより、ネットワークインターフェース２５０に与えることができる。代替の実施形態では、許可コンピューティングデバイス３１０の位置は、アクセス中のコンピューティングデバイス２１０に既に知られていることができる。例えば、通常、アクセス中のコンピューティングデバイス２１０のようなコンピューティングデバイスが、ネットワーク１５５とのネットワーク接続２５１を確立するとき、そのコンピューティングデバイスは、例えばＤＮＳサーバーのアドレス、コンピューティングデバイスにサービス提供するルータのアドレスを含む、特定のネットワーク情報を提供される。同じようにして、上記の実施形態によれば、アクセス中のコンピューティングデバイス２１０のようなコンピューティングデバイスは、ネットワーク１５５上にあるか又はコンピューティングデバイスが接続されているネットワークの同じ部分にあるコンピューティングデバイスにサービスを提供することができる、許可コンピューティングデバイス３１０のような許可コンピューティングデバイスのためのネットワークアドレス、又は他の位置情報の提供を受けることができる。

【００５６】

[0061]アクセス制御暗号情報３７６は、許可コンピューティングデバイス３１０の公開アクセス鍵、許可コンピューティングデバイスとアクセス制御デバイス１７０との間で共有される秘密情報、又は任意の同様の暗号情報を含むことができ、それらの情報によって、アクセス制御デバイス１７０及び許可コンピューティングデバイス３１０は、ポイント・ツーポイントトンネリングプロトコル（ＰＰＴＰ）又はレベル２トンネリングプロトコル（Ｌ２ＴＰ）と同様、又は同一のプロトコルを含む、標準的なトンネリング機構等を通じて、セキュア通信トンネル３２０を確立できるようになる。当業者によって知られることになるように、そのようなトンネリング機構は、共通パスワード若しくはアクセス制御のような種々のセキュリティ証明書（セキュリティ認証情報、security credentials）の交換に頼ることができるか、又はケルベロス若しくはＲＡＤＩＵＳサーバーのような、独立した検証機構によって与えられるセキュリティ証明書に頼ることができ、それらの認証情報のうちのいずれか又は全てが、アクセス制御暗号情報３７６としてアクセス制御デバイス１７０に与えられていることができる。セキュアトンネル３２０によれば、アクセス中のコンピューティングデバイス２１０によってメッセージが中継され、それゆえ、メッセージがアクセス中のコンピューティングデバイス上で実行されるコンポーネント及びプロセスに見えるという事実にもかかわらず、そのようなコンポーネント及びプロセスは、そのようなメッセージの内容を理解することができず、それゆえ、許可コンピューティングデバイス３１０が別の方法でそのような記憶関連暗号情報のプロビジョンが適切であったことを示さなかったとき、アクセス制御デバイス１７０は記憶関連暗号情報１７５を与えることはできない。上記で示されたように、セキュア通信トンネル３２０を確立するために利用される認証情報及び他の情報を含むことができるアクセス制御暗号情報３７６は、プロビジョニング中に、プロビジョニングコンピューティングデバイス１１０によって

アクセス制御デバイス１７０に与えられていたはずである。

【００５７】

[0062]一実施形態では、許可コンピューティングデバイス３１０は、ネットワークアクセス保護（ＮＡＰ）、ネットワークアドミッションコントロール（ＮＡＣ）、セキュアネットワークアクセス（ＳＮＡ）又は他の同様の技術のような、既存のアクセス制御技術及び方法と統合することができる。例えば、既存のＮＡＰサーバーコンピューティングデバイスは、更新されたアンチマルソフトウェア、適用されたオペレーティングシステム更新、及び他の同様の情報によって定量化されるようなコンピューティングデバイスのセキュリティを既に認識している可能性がある。既存のＮＡＰサーバーコンピューティングデバイスによって判断されるような、セキュリティのしきい値レベルを満たすことができないコンピューティングデバイスは、同様に、許可コンピューティングデバイス３１０にも識別することができ、許可コンピューティングデバイスは、アクセス制御デバイス１７０に、そのようなコンピューティングデバイスに通信的に結合される記憶装置に記憶関連暗号情報１７５を与えないように命令することができる。

【００５８】

[0063]それゆえ、図３に示されるように、アクセス制御デバイス１７０は依然として、アクセス中のコンピューティングデバイス２１０において実行される記憶装置ドライバースタック２３８のアクセス制御デバイス拡張部２３９との通信を通じて、アクセス制御デバイスが現在通信的に結合されるアクセス中のコンピューティングデバイス及び記憶装置２７０に関連付けられた特定の情報を知ることができる。そのような情報は、上記で示されたように、アクセス中のコンピューティングデバイス２１０を使用するユーザー、アクセス中のコンピューティングデバイスそのもの、記憶装置ホストコントローラー２４５、記憶装置２７０のアイデンティティを含むことができ、セキュアトンネル３２０を通じて、アクセス制御デバイス１７０によって許可コンピューティングデバイス３１０に他の同様の情報を与えることができる。そのような与えられた情報、及び上記のＮＡＰ情報のような、入手することができる他の情報に基づいて、許可コンピューティングデバイス３１０は、記憶装置２７０がアクセス中のコンピューティングデバイス２１０からのデータ記憶関連通信に意味のある応答を与えることができるか否かを判断することができる。許可コンピューティングデバイス３１０からアクセス制御デバイス１７０への命令は、図に示されるように、セキュアトンネル３２０を通じて受信することができる。一実施形態では、許可コンピューティングデバイス３１０からの命令は、アクセス制御デバイス１７０の処理ユニット１７１によって受信することができ、処理ユニットは、上記のように、記憶装置２７０の処理ユニット２８１に、ファームウェア２８３からの適切な命令を実行して、アクセス中のコンピューティングデバイス２１０からのデータ記憶関連通信に意味のあるように応答するか、又はアクセス中のコンピューティングデバイス２１０からの記憶関連通信若しくは要求に適切なエラー若しくは他の拒否によって応答するように命令することができる。別の実施形態では、許可コンピューティングデバイス３１０からの命令は、アクセス制御デバイス１７０の処理ユニット１７１によって受信することができ、処理ユニットは、同じく上記のように、記憶装置２７０の処理ユニット２８１に記憶関連暗号情報１７５を与えて、記憶装置２７０がアクセス中のコンピューティングデバイス２１０からのデータ記憶関連通信に意味のあるように応答することができるようにするか、又は記憶関連暗号情報１７５を拒否して、記憶装置２７０がアクセス中のコンピューティングデバイス２１０からのデータ記憶関連通信に意味のあるように応答するのを防ぐことができる。

【００５９】

[0064]一実施形態では、許可コンピューティングデバイス３１０上で実行される許可プロセスは、アクセス中のコンピューティングデバイス２１０とは別の独立型コンピューティングデバイス上で実行するのではなく、代わりに、アクセス中のコンピューティングデバイスの保護空間内で実行することができる。そのような実施形態では、許可コンピューティングデバイス３１０は、アクセス中のコンピューティングデバイス２１０上で実行さ

れる仮想機械又は他の保護された独立プロセスとすることができる。上記の実施形態では、アクセス中のコンピューティングデバイス２１０が、許可コンピューティングデバイス３１０との間でメッセージを搬送したので、許可コンピューティングデバイスは、代わりに、アクセス制御デバイス１７０に変更を加えることなく、アクセス中のコンピューティングデバイス上でのコンピューター実行可能命令の実行を通じて実現することができる。

【００６０】

[0065]図４を参照すると、図２及び図３において破線の通信矢印で示されるような、アクセス制御デバイス１７０と記憶装置２７０との間の通信接続が、更に詳細に図示及び説明される。一実施形態では、システム４００によって示されるように、記憶装置２７０は、上記で説明されたハードウェア暗号システム２８０及びコンピューター読み取り可能な媒体２９０を備えるだけでなく、アクセス制御デバイスインターフェース４１０も備えることができる。アクセス制御デバイスインターフェース４１０は、一例にすぎないが、記憶装置２７０上のスロット又はコネクタとすることができ、アクセス制御デバイス１７０が挿入若しくは接続されるときに記憶装置２７０の寸法を実質的に変更しないように、アクセス制御デバイス１７０を物理的にアクセス制御デバイスインターフェース４１０に挿入できるか、又は別の方法で接続できるようにする。そのような事例において、記憶装置２７０は、アクセス制御デバイスを用いない同様のタイプの任意の他の記憶装置の場合と同様に、上記で詳細に説明された、アクセス中のコンピューティングデバイス２１０のようなコンピューティングデバイスが利用することができる。例えば、記憶装置２７０が標準的なハードディスクドライブサイズに準拠するように設計された場合には、アクセス中のコンピューティングデバイス２１０は、記憶装置２７０を、この記憶装置に物理的に接続されるアクセス制御デバイス１７０とともに、内部ハードディスクドライブとして利用することができ、アクセス制御デバイスの有無は、そのような使用を禁止する記憶装置２７０の物理的寸法を変更しないであろう。

【００６１】

[0066]別の例として、アクセス制御デバイス１７０は、携帯電話のために一般的に利用されるような、ＧＳＭ（Global System for Mobile Communications）の加入者識別モジュール（ＳＩＭ）の形をとることができる。そのような事例では、アクセス制御デバイスインターフェース４１０は再び、携帯電話に通常含まれるような、ＧＳＭ　ＳＩＭインターフェースとすることができる。そのような実施形態は、アクセス制御デバイス１７０及びアクセス制御デバイスインターフェース４１０の物理的なフォームファクターをいずれも共通に利用することができ、それゆえ、安価であるので、コストに関する利点を提供することができる。

【００６２】

[0067]更に別の例として、アクセス制御デバイス１７０は、同様に、対応するアクセス制御デバイスインターフェース４１０として、ユニバーサル・シリアル・バス（ＵＳＢ）コネクタのような共通のコネクタを含むことができる。上記のＧＳＭ　ＳＩＭ実施形態の場合のように、ＵＳＢコネクタも、広く行き渡っていることに起因して、同様にコストに関する利点を提供する。そのような実施形態では、アクセス制御デバイス１７０とハードウェア暗号システム２８０との間の以下に説明される通信は、既知のＵＳＢ通信プロトコルを介して実行することができる。

【００６３】

[0068]しかしながら、アクセス制御デバイス１７０は、記憶装置に通信的に接続されるのに記憶装置２７０に必ずしも物理的に接続される必要はない。上記の実施形態は、記憶装置の共通のタイプのインターフェースを介して命令又は暗号情報１７５のいずれかを処理ユニット２８１に送信するのを避けるために、アクセス制御デバイス１７０と記憶装置２７０との間の物理的な接続を設ける。そのようにして、アクセス制御デバイス１７０及び記憶装置２７０のハードウェア設計は、処理ユニット１７１によって与えられる命令又は記憶関連暗号情報１７５を外部エンティティが入手できないのを確実にすることができる。

【００６４】
[0069]代替の実施形態では、処理ユニット１７１によって処理ユニット２８１に与えられる命令及び記憶関連暗号情報１７５は、そのうちの少なくともいくつかの情報が記憶装置２７０の外部通信インターフェースを介して転送されるにもかかわらず、安全にすることができる。したがって、システム４５０において示されるように、アクセス制御デバイス１７０及び記憶装置２７０が物理的に離れているにもかかわらず、アクセス中のコンピューティングデバイス２１０を介して、アクセス制御デバイス１７０と記憶装置２７０との間に通信接続を確立することができる。図に示されるように、システム４５０は、アクセス中のコンピューティングデバイス２１０と、アクセス制御デバイス１７０と、記憶装置２７０とを備えることができ、アクセス制御デバイス及び記憶装置はいずれも、アクセス中のコンピューティングデバイスに独立して接続される。システム４５０では、アクセス中のコンピューティングデバイス２１０、アクセス制御デバイス１７０及び記憶装置２７０が別個の物理的なエンティティとして示されるように図示されるが、そのように物理的に別個である必要ではない。例えば、記憶装置２７０は、内部ハードディスクドライブ等の形態で、アクセス中のコンピューティングデバイス２１０の内部に接続することができる。アクセス制御デバイス１７０は更に、有線及び無線の両方のインターフェースを含む、普及している周辺装置又は記憶装置インターフェースのような、アクセス中のコンピューティングデバイス２１０の外部インターフェースに接続することができる。そのような実施形態では、アクセス制御デバイス１７０と記憶装置２７０との間の通信は、アクセス中のコンピューティングデバイス２１０の記憶装置ドライバースタック２３８によって中継することができ、その記憶装置ドライバースタックは、自らの機構を通じて、かつアクセス制御デバイス拡張部２３９を通じて、アクセス制御デバイス及び記憶装置の両方と通信することができる。

【００６５】
[0070]図５を参照すると、アクセス中のコンピューティングデバイス２１０とアクセス制御デバイス１７０との間の例示的な通信交換が、システム５００を参照しながら更に具体的に示される。図５に示されるように、システム５００は、アクセス制御デバイス１７０、記憶装置２７０、アクセス中のコンピューティングデバイス２１０及びオプションで、許可コンピューティングデバイス３１０を含む、上記で詳細に説明されたシステム２００及び３００と同じ基本構成要素を備えることができる。最初に、通信５１０によって示されるように、アクセス中のコンピューティングデバイス２１０、より具体的には、アクセス中のコンピューティングデバイスのオペレーティングシステム２３４（図示せず）の記憶装置ドライバースタック２３８が、例えば、読出し要求、初期化要求、又は他の同様のアクセス要求を発行すること等によって、記憶装置２７０のデータ記憶関連要求を行なうことができる。データ記憶関連要求５１０に応答して、記憶装置は、エラーコードを含むエラー通信５２０を与えることができる。当業者であれば分かるように、記憶装置ドライバースタック２３８によって実行されることになる通信のような、記憶装置との通信は、エラーコードの形でエラー通信を与えることができ、各コードは、記憶装置２７０の一部における、特定のエラー、又はエラーのタイプを示す。一実施形態では、エラーコードは、通信５２０の一部として、記憶装置２７０によって記憶装置ドライバースタック２３８に与えることができ、通信５２０は、記憶装置がアクセス制御デバイス１７０に通信的に結合されることを示すことができ、かつ、例えば、処理ユニット２８１に命令することによって、又は要求されたデータを暗号解読するために必要とされる記憶関連暗号情報１７５を与えること等によって、通信的に結合されるアクセス制御デバイスが、データ記憶要求５１０に対する応答を意味のあるように提供することを記憶装置２７０にまだ許可していないので、データ２９５にアクセスする試みが失敗したことを更に示すことができる。

【００６６】
[0071]そのようなエラーコードに応答して、記憶装置ドライバースタック２３８は、動作５３０によって示されるように、アクセス制御デバイス拡張部２３９をロードすること

ができるか、ロードさせることができるか、又は別の方法で実行させることができる。上記のように、アクセス制御デバイス拡張部２３９は、アクセス制御デバイス１７０のようなアクセス制御デバイスと通信するように構成されるコンピューター実行可能命令を含むことができ、それは、そのようなアクセス制御デバイスが記憶装置を通じてコンピューティングデバイスに間接的にのみ通信的に結合される場合を含む。アクセス制御デバイス拡張部２３９がロードされると、通信５４０のような通信をアクセス制御デバイス１７０に向けることができる。一実施形態では、通信５４０は、記憶装置２７０に従来通りに向けられるような書込みコマンドを含むことができるが、書込みコマンドはアドレス、又はアドレスの範囲を指定することができ、それにより、その通信がアクセス制御デバイス１７０に向けられることを記憶装置に示すことができる。したがって、図５に示されるように、アドレス制御デバイス拡張部２３９からの通信５４０は、最初に記憶装置２７０に与えることができ、その後、指定されたアドレス、又はアドレス範囲に基づいて、記憶装置が更に、アクセス制御デバイス１７０に通信５４０を与えることができる。

【００６７】

[0072]アクセス制御デバイス１７０は応答通信５５０を与えることができ、その通信は、例えば、最初にアクセス制御デバイスによって記憶装置２７０に与えられ、その後、記憶装置から記憶装置ドライバースタック２３８に与えられることによって、アクセス制御デバイス拡張部２３９に戻すことができる。その際、記憶装置ドライバースタック２３８は、その応答５５０の受信時に、それをアクセス制御デバイス拡張部２３９に相応しい応答として認識することができ、その応答に対してアクセス制御デバイス拡張部を向けることができる。上記のように、実施形態によっては、応答５５０のような応答は、応答５５０に含まれている場合がある特定のデータを、アクセス制御デバイス拡張部２３９が許可コンピューティングデバイス３１０に転送することを要求することができる。そのような事例では、アクセス制御デバイス拡張部２３９は、例えば、アクセス中のコンピューティングデバイス２１０において実行される関連するネットワークプロセスが、ネットワークインターフェース２５０とともに、要求５６０によって示されるような、許可コンピューティングデバイス３１０への通信接続を確立することを要求することができる。それにより、アクセス制御デバイス拡張部２３９は、アクセス制御デバイス１７０及び許可コンピューティングデバイス３１０との間でデータを交換できるようにし、それにより、アクセス制御デバイス及び許可コンピューティングデバイスがセキュア通信トンネル３２０を確立できるようにする。

【００６８】

[0073]図６を参照すると、流れ図６００が、図１のシステム１００内に示され、上記で詳細に説明された例示的なプロビジョニングコンピューティングデバイス１１０によって実行できるような、アクセス制御デバイス１７０の例示的なプロビジョニングの更なる例示を提供する。流れ図６００から明らかであるように、最初に、ステップ６１０において、アクセス制御デバイス１７０のようなアクセス制御デバイスのプロビジョニングを開始することができる。ステップ６１０のプロビジョニング開始は、プロビジョニングコンピューティングデバイスに通信的に結合されるアクセス制御デバイスの検出への応答のように、自動的に開始することができるか、又はプロビジョニングコンピューティングデバイス上で実行される１つ又は複数のプロセスによって提示することができる適切なユーザーインターフェース等を通じて手動で開始することができ、すなわち、プロビジョニングはユーザーが開始することができる。その後、ステップ６２０において、プロビジョニングされるアクセス制御デバイスが許可コンピューティングデバイスとともに用いられることになるか否か、又は独立して制御決定を実行することになるか否かに関して判断を行なうことができる。ステップ６２０において、プロビジョニングされるアクセス制御デバイスが、許可コンピューティングデバイスとともに用いられないと判断される場合には、ステップ６３０において、アクセス制御デバイスにアクセス制御情報をプロビジョニングすることができ、アクセス制御情報は、そのアクセス制御デバイスが通信的に結合される記憶装置のデータ関連能力へのアクセス許可を受けることができる、ユーザー、コンピューテ

ィングデバイス、記憶装置、記憶装置ホストコントローラー又はその組み合わせのようなエンティティの識別情報を含むことができる。代替的には、ステップ６２０において、プロビジョニングされるアクセス制御デバイスが許可コンピューティングデバイスとともに用いられることになると判断される場合には、ステップ６４０において、アクセス制御デバイスに、アクセス制御暗号情報を含むアクセス制御情報をプロビジョニングすることができ、その情報によって、例えば上記で詳細に説明されたようにして、アクセス制御デバイスがアクセス中のコンピューターデバイスを通じて許可コンピューティングデバイスとのセキュア通信トンネルを確立できるようになる。

【００６９】

[0074]アクセス制御デバイスが、ステップ６３０において独立したアクセス制御動作のためにプロビジョニングされるにしても、又はステップ６４０において許可コンピューティングデバイスとの相互作用のためにプロビジョニングされるにしても、いずれの場合も、処理は、破線の枠線によってオプションとして示されるオプションのステップ６５０に進むことができ、記憶装置上に格納されたデータを暗号解読するか、又は格納されることになるデータを暗号化するために、アクセス制御デバイスが通信的に結合される記憶装置によって用いることができる記憶関連暗号情報をアクセス制御デバイスにプロビジョニングすることができる。一実施形態では、そのアクセス制御デバイスと通信する後続の各記憶装置が次の物理アクセス制御を取得し、それを使用中として示すことができるように、ステップ６５０における記憶関連暗号情報のプロビジョニングは、そのアクセス制御デバイスに複数組の、例えば、物理アクセス制御をプロビジョニングすることができる。そのようにして、単一のアクセス制御デバイスを、複数の記憶装置によって共用することもできるし、複数の記憶装置とともに用いることもできる。オプションでは、ステップ６５０において、記憶関連暗号情報がアクセス制御デバイスにプロビジョニングされると、図に示されるように、ステップ６６０において関連する処理を終了することができる。

【００７０】

[0075]図７を参照すると、流れ図７００が示されており、上記で詳細に説明された、例示的なアクセス中のコンピューティングデバイス２１０のようなアクセス中のコンピューティングデバイスの例示的な動作を更に示す。流れ図７００を参照すると、図に示されるように、最初に、ステップ７０５において、アクセス中のコンピューティングデバイスは、アクセス要求のようなデータ記憶関連要求を、そのアクセス中のコンピューティングデバイスが通信的に結合される記憶装置に発行することができる。ステップ７０５においてそのようなデータ記憶関連要求に応答して、ステップ７１０において、アクセス中のコンピューティングデバイスは、アクセスしている記憶装置がアクセス制御デバイスに通信的に結合されることを示すエラーを受信することができる。ステップ７１０においてそのようなエラーが受信されない場合には、ステップ７１５において、アクセス中のコンピューティングデバイスは、従来通りに記憶装置を利用するように進むことができる。その後、ステップ７６０において、関連する処理を終了することができる。

【００７１】

[0076]ステップ７１０において、アクセス中のコンピューティングデバイスが、記憶装置から、その記憶装置がアクセス制御デバイスに通信的に結合されることを示すエラーを受信する場合には、ステップ７２０において、アクセス中のコンピューティングデバイスは、アクセス制御デバイス拡張部をロードし、上記のように、アクセス制御デバイス拡張部を用いてアクセス制御デバイスと通信することができる。ステップ７２５において、アクセス制御デバイスが情報を要求しているか否かに関して判断を行なうことができる。アクセス制御デバイスが情報を要求している場合には、ステップ７３０において、要求された情報を与えることができる。上記のように、そのような要求された情報は、アクセス中のコンピューティングデバイスのアイデンティティ、そのようなコンピューティングデバイスを使用するユーザー、記憶装置にアクセスする記憶装置ホストコントローラーのアイデンティティ、及び記憶装置そのもののアイデンティティを含むことができる。また上記のように、そのようなアイデンティティは、例えば、パスワード又は他のセキュリティ機

構を通じて認証することができ、そのような事例では、ステップ７３０において与えられる要求された情報は、それらのパスワード、又はステップ７２５においてアクセス制御デバイスによって与えられていた可能性があるチャレンジへの他の応答を含むことができる。ステップ７３０において、要求された情報が与えられたとすると、処理はステップ７２５に戻り、アクセス制御デバイスからの更なる情報要求を待ち受けることができる。

【００７２】

[0077]ステップ７２５において、アクセス制御デバイスが何も情報を要求しない場合には、処理はステップ７３５に進むことができ、アクセス制御デバイスが許可コンピューティングデバイスへの接続を要求しているか否かを判断することができる。ステップ７３５において、そのような接続が要求されなかった場合には、ステップ７６０において関連する処理を終了することができる。しかしながら、ステップ７３５において、そのような接続が要求された場合には、ステップ７４０において、要求するコンピューティングデバイスは、例えば、上記で詳細に説明されたようにして、許可コンピューティングデバイスとの接続を確立することができる。その後、ステップ７４５において、同じく上記のように、アクセス中のコンピューティングデバイスによって、アクセス制御デバイスと許可コンピューティングデバイスとの間のデータ交換を促進することができる。

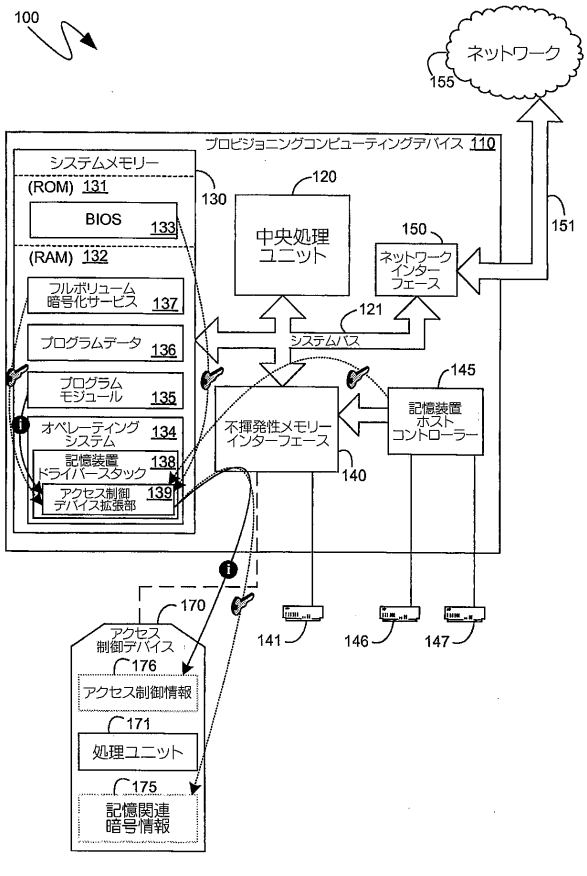
【００７３】

[0078]ステップ７５０において、アクセス制御デバイスが許可コンピューティングデバイスとの接続を終了するのを要求しているか否かを判断するようにチェックすることができる。そのような要求が行なわれていない場合には、処理はステップ７４５に戻ることができ、アクセス制御デバイスと許可コンピューティングデバイスとの間でデータを交換し続けることができる。しかしながら、ステップ７５０において、アクセス制御デバイスが、許可コンピューティングデバイスとの接続が終了されることを要求する場合には、ステップ７５５において、接続を終了することができ、ステップ７６０において、関連する処理を終了することができる。

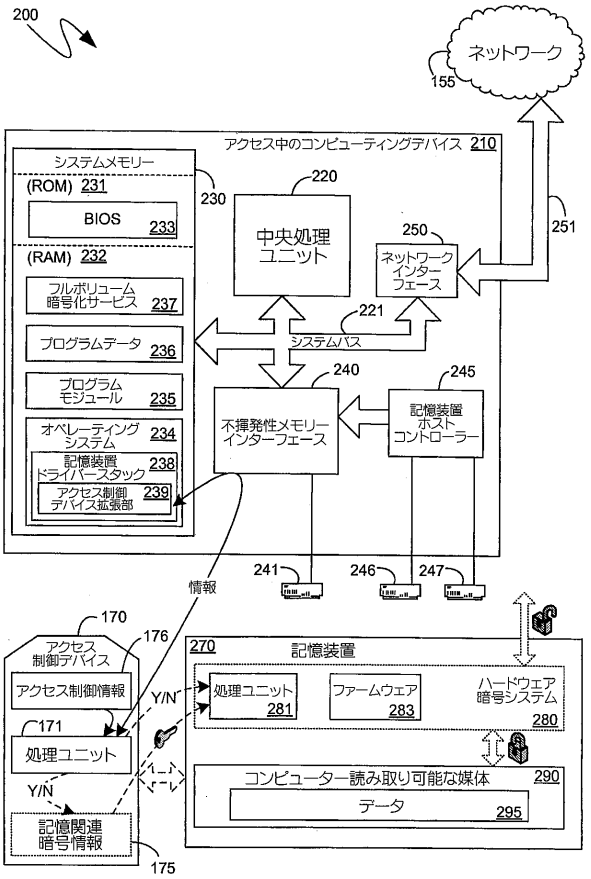
【００７４】

[0079]上記の説明から明らかであるように、記憶装置へのアクセスを制御することができるアクセス制御デバイスが提供された。本明細書において説明される主題の数多くの可能な変形に鑑みて、本発明者らは、添付の特許請求の範囲及びその均等物の範囲に入ることができる全てのそのような実施形態を本発明として特許請求する。

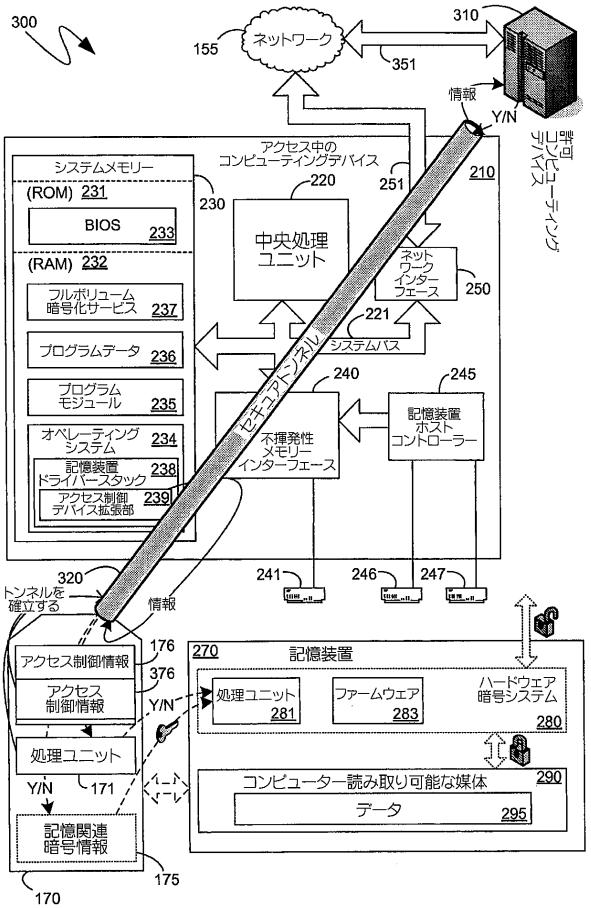
【図１】


100
ネットワーク
155
プロビジョニングコンピューティングデバイス 110
システムメモリー
(ROM) 131
BIOS 133
(RAM) 132
フルボリューム暗号化サービス 137
プログラムデータ 136
プログラムモジュール 135
オペレーティングシステム 134
記憶装置ドライバースタック 138
アクセス制御デバイス拡張部 139
130
120
中央処理ユニット
150
ネットワークインターフェース
151
121
システムバス
145
不揮発性メモリーインターフェース
記憶装置ホストコントローラー
140
170
アクセス制御デバイス
176
アクセス制御情報
171
処理ユニット
175
記憶関連暗号情報
141
146
147

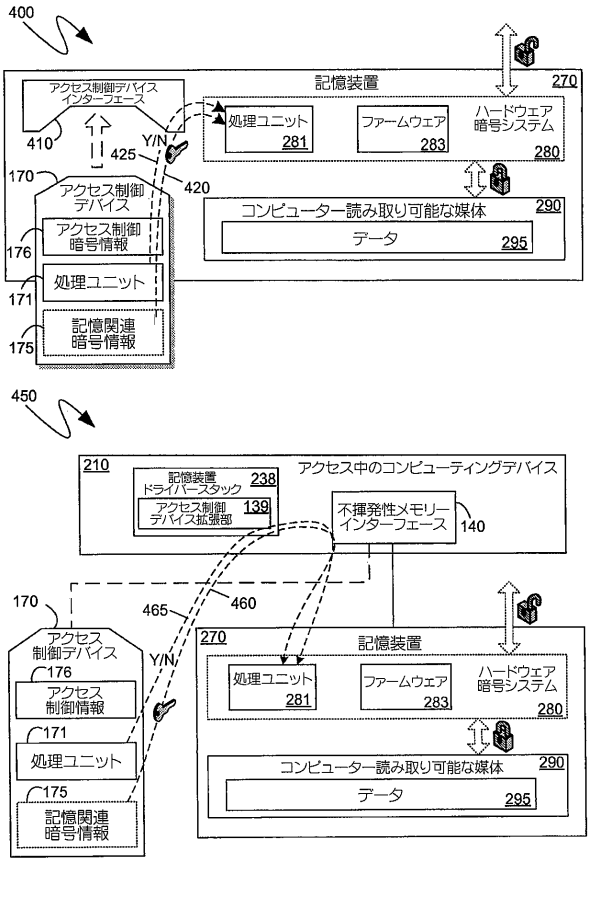
【図２】


200
ネットワーク
155
アクセス中のコンピューティングデバイス 210
システムメモリー
(ROM) 231
BIOS 233
(RAM) 232
フルボリューム暗号化サービス 237
プログラムデータ 236
プログラムモジュール 235
オペレーティングシステム 234
記憶装置ドライバースタック 238
アクセス制御デバイス拡張部 239
230
220
中央処理ユニット
250
ネットワークインターフェース
251
221
システムバス
240
不揮発性メモリーインターフェース
245
記憶装置ホストコントローラー
情報
241
246
247
170
アクセス制御デバイス
176
アクセス制御情報
171
処理ユニット
175
記憶関連暗号情報
Y/N
270
記憶装置
処理ユニット 281
ファームウェア 283
ハードウェア暗号システム 280
コンピューター読み取り可能な媒体 290
データ 295

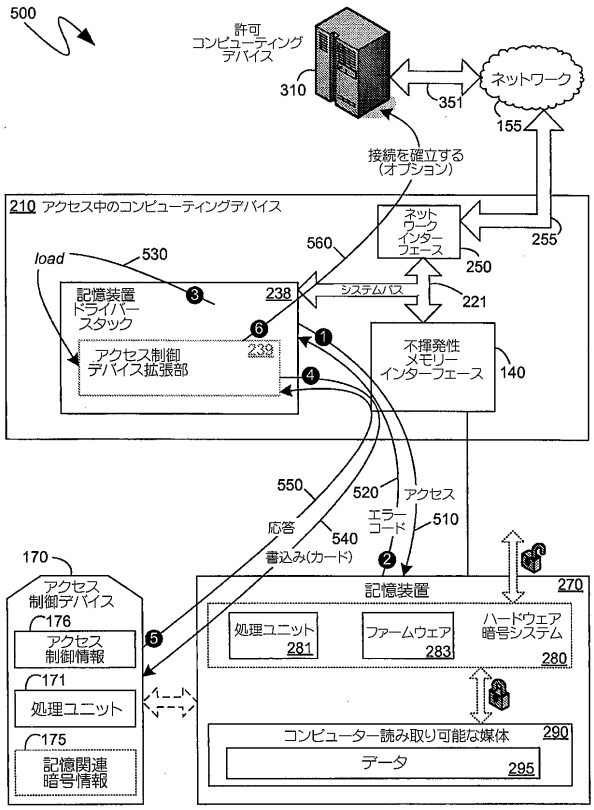
【図３】


300
ネットワーク
155
310
351
情報
Y/N
許可されたコンピューティングデバイス
アクセス中のコンピューティングデバイス 210
システムメモリー
(ROM) 231
BIOS 233
(RAM) 232
フルボリューム暗号化サービス 237
プログラムデータ 236
プログラムモジュール 235
オペレーティングシステム 234
記憶装置ドライバースタック 238
アクセス制御デバイス拡張部 239
230
220
251
中央処理ユニット
250
ネットワークインターフェース
221
システムバス
240
不揮発性メモリーインターフェース
245
記憶装置ホストコントローラー
セキュアトンネル
320
トンネルを確立する
241
246
247
情報
176
アクセス制御情報
376
アクセス制御情報
Y/N
処理ユニット
171
Y/N
記憶関連暗号情報
175
170
270
記憶装置
処理ユニット 281
ファームウェア 283
ハードウェア暗号システム 280
コンピューター読み取り可能な媒体 290
データ 295

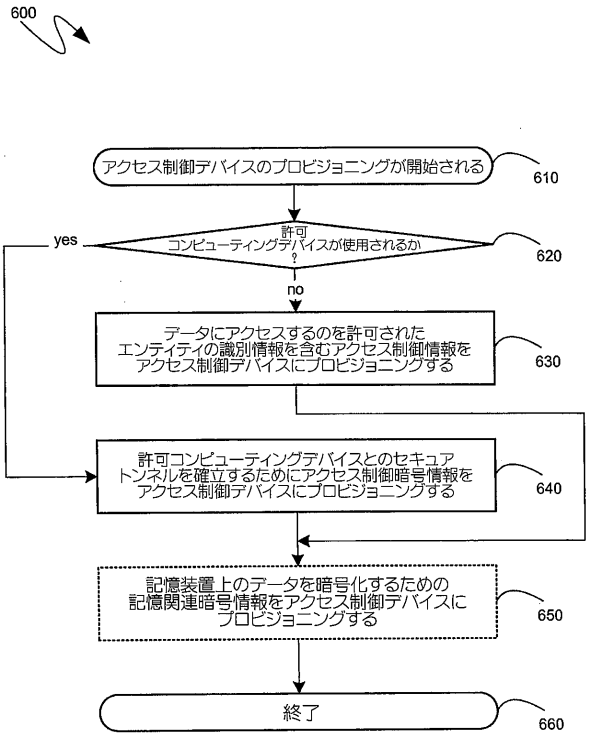
【図４】


400
記憶装置
270
アクセス制御デバイスインターフェース
410
425
Y/N
処理ユニット 281
ファームウェア 283
ハードウェア暗号システム 280
420
170
アクセス制御デバイス
176
アクセス制御暗号情報
171
処理ユニット
175
記憶関連暗号情報
コンピューター読み取り可能な媒体 290
データ 295
450
210
アクセス中のコンピューティングデバイス
記憶装置ドライバースタック 238
アクセス制御デバイス拡張部 139
不揮発性メモリーインターフェース 140
460
465
170
アクセス制御デバイス
176
アクセス制御情報
171
処理ユニット
175
記憶関連暗号情報
Y/N
270
記憶装置
処理ユニット 281
ファームウェア 283
ハードウェア暗号システム 280
コンピューター読み取り可能な媒体 290
データ 295

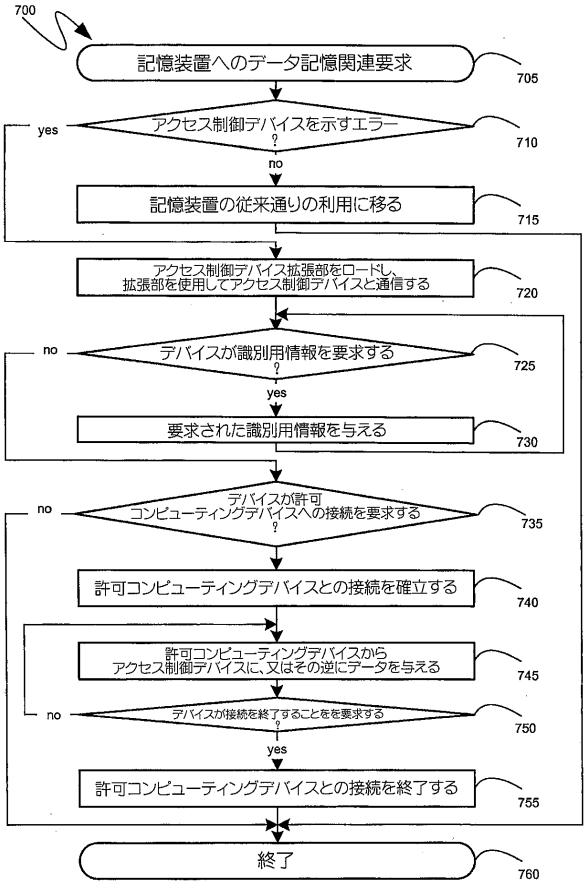
【図５】


500
許可
コンピューティング
デバイス
310
ネットワーク
351
155
接続を確立する
(オプション)
210 アクセス中のコンピューティングデバイス
ネット
ワーク
インター
フェース
560
255
250
load
530
記憶装置
ドライバー
スタック
238
システムバス
221
アクセス制御
デバイス拡張部
239
不揮発性
メモリー
インターフェース
140
550
520
アクセス
エラー
コード
510
応答
540
書込み(カード)
170
アクセス
制御デバイス
176
アクセス
制御情報
171
処理ユニット
175
記憶関連
暗号情報
記憶装置
270
処理ユニット
281
ファームウェア
283
ハードウェア
暗号システム
280
コンピューター読み取り可能な媒体
290
データ
295

【図６】


600
アクセス制御デバイスのプロビジョニングが開始される
610
許可
コンピューティングデバイスが使用されるか
?
620
yes
no
データにアクセスするのを許可された
エンティティの識別情報を含むアクセス制御情報を
アクセス制御デバイスにプロビジョニングする
630
許可コンピューティングデバイスとのセキュア
トンネルを確立するためにアクセス制御暗号情報を
アクセス制御デバイスにプロビジョニングする
640
記憶装置上のデータを暗号化するための
記憶関連暗号情報をアクセス制御デバイスに
プロビジョニングする
650
終了
660

【図７】


700
記憶装置へのデータ記憶関連要求
705
アクセス制御デバイスを示すエラー
?
710
yes
no
記憶装置の従来通りの利用に移る
715
アクセス制御デバイス拡張部をロードし、
拡張部を使用してアクセス制御デバイスと通信する
720
デバイスが識別用情報を要求する
?
725
no
yes
要求された識別用情報を与える
730
デバイスが許可
コンピューティングデバイスへの接続を要求する
?
735
no
許可コンピューティングデバイスとの接続を確立する
740
許可コンピューティングデバイスから
アクセス制御デバイスに、又はその逆にデータを与える
745
デバイスが接続を終了することをを要求する
?
750
no
yes
許可コンピューティングデバイスとの接続を終了する
755
終了
760

フロントページの続き

(72)発明者　サドフスキー，ヴラジミール
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，マイクロソフト　コーポレーション，エルシーエイ－インターナショナル・パテンツ
(72)発明者　オラリグ，ソンポン・ポール
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，マイクロソフト　コーポレーション，エルシーエイ－インターナショナル・パテンツ
(72)発明者　リオネッティ，クリス
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，マイクロソフト　コーポレーション，エルシーエイ－インターナショナル・パテンツ
(72)発明者　ハミルトン，ジェームズ・ロバート
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，マイクロソフト　コーポレーション，エルシーエイ－インターナショナル・パテンツ

審査官　木村　励

(56)参考文献　特開２００８－０１６００１（ＪＰ，Ａ）
特開２００９－０２６２６７（ＪＰ，Ａ）
特開２００３－３１６６５５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／００　－　２１／８８
Ｈ０４Ｌ　９／３２