(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5922113号
(P5922113)

(45)発行日　平成28年5月24日(2016.5.24)　(24)登録日　平成28年4月22日(2016.4.22)

(51)Int.Cl.　　F I
H04L 9/08 (2006.01)　　H04L 9/00 601A
H04L 9/32 (2006.01)　　H04L 9/00 675B

請求項の数 14　(全 28 頁)

(21)出願番号　特願2013-516601 (P2013-516601)
(86)(22)出願日　平成23年6月10日 (2011.6.10)
(65)公表番号　特表2013-531436 (P2013-531436A)
(43)公表日　平成25年8月1日 (2013.8.1)
(86)国際出願番号　PCT/US2011/040063
(87)国際公開番号　WO2011/162990
(87)国際公開日　平成23年12月29日 (2011.12.29)
審査請求日　平成26年6月10日 (2014.6.10)
(31)優先権主張番号　12/819,883
(32)優先日　平成22年6月21日 (2010.6.21)
(33)優先権主張国　米国 (US)

(73)特許権者　314015767
マイクロソフト　テクノロジー　ライセンシング，エルエルシー
アメリカ合衆国　ワシントン州　９８０５２　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介

最終頁に続く

(54)【発明の名称】暗号化データにアクセスするための一度限り使用可能な認証方法

(57)【特許請求の範囲】
【請求項１】
第１のコンピュータの保護されたボリュームに記憶された暗号化データにアクセスする一度限り使用可能な認証方法であって、
前記保護されたボリュームに記憶された前記暗号化データを復号するために必要とされるボリューム固有の暗号鍵を、ランダムに生成される非対称な公開鍵と秘密鍵の対の前記公開鍵で暗号化することにより、キープロテクタを生成するステップであって、前記公開鍵はキープロテクタ識別子及び前記秘密鍵の記憶場所を判定するキープロテクタ属性とともに配信される、ステップと、
前記キープロテクタを前記第１のコンピュータのローカルメモリに記憶するステップであって、前記キープロテクタが一度限り使用可能なキープロテクタであることを示す識別子とともに前記キープロテクタが記憶される、ステップと、
前記保護されたボリュームにアクセスする試みを検出するのに応答して、
前記秘密鍵を取得するステップ、
前記秘密鍵を使用して前記キープロテクタを復号して前記ボリューム固有の暗号鍵を取得するステップ、
前記キープロテクタとともに記憶された識別子に基づき、前記キープロテクタが一度限り使用可能なキープロテクタであるか判断するステップ、
および
前記キープロテクタとともに記憶された識別子が一度限り使用可能なキープロテク

タであることを示すとき、前記キープロテクタを一度使用した後に、前記キープロテクタを前記第１のコンピュータの前記ローカルメモリから削除するステップ
を行うステップと
を含む方法。
【請求項２】
前記ボリューム固有の暗号鍵を使用して、前記保護されたボリュームに記憶された前記暗号化データを復号するステップをさらに含む、請求項１に記載の方法。
【請求項３】
前記ボリューム固有の暗号鍵を使用して、前記保護されたボリュームに記憶された前記暗号化データを復号するステップは、
前記ボリューム固有の暗号鍵を使用して、第２のボリューム固有の暗号鍵を復号するステップと、
前記第２のボリューム固有の暗号鍵を使用して、前記保護されたボリュームに記憶された前記暗号化データを復号するステップと
を含む、請求項２に記載の方法。
【請求項４】
前記秘密鍵を取得するステップは、前記秘密鍵を前記第１のコンピュータの前記ローカルメモリから取得するステップを含む、請求項１に記載の方法。
【請求項５】
前記秘密鍵を取得するステップは、ネットワークを通じて第２のコンピュータから前記秘密鍵を取得するステップを含む、請求項１に記載の方法。
【請求項６】
前記ネットワークを通じて前記第２のコンピュータから前記秘密鍵を取得するステップは、チャレンジ－レスポンス対話の実行が成功した後に前記ネットワークを通じて前記第２のコンピュータから前記秘密鍵を取得するステップを含む、請求項５に記載の方法。
【請求項７】
保護されたボリュームを有する第１のコンピュータであって、ローカルメモリにキープロテクタを記憶するように構成され、前記キープロテクタはトラステッドプラットフォームモジュール（ＴＰＭ）のシール動作を行うことにより生成され、前記ＴＰＭのシール動作は、前記保護されたボリュームに記憶された暗号化データを復号するために必要とされるボリューム固有の暗号鍵を暗号化すること、および前記暗号化されたボリューム固有の暗号鍵を、ランダムデータをハッシュ化することによって生成される値にバインドすることである、第１のコンピュータと、
第２のコンピュータと、
前記第２のコンピュータからはアクセスできるが前記第１のコンピュータからはアクセスできない、前記ランダムデータが記憶されるメモリと
を備えるシステムであって、
前記第１のコンピュータはさらに、前記保護されたボリュームにアクセスする試みを検出するのに応答して、前記第２のコンピュータから前記ランダムデータを取得し、前記ランダムデータを利用するＴＰＭのアンシール動作を行うことにより前記ボリューム固有の暗号鍵を取得するように構成され、
前記第２のコンピュータは、前記第２のコンピュータからアクセス可能な前記メモリから前記ランダムデータを削除するように構成される、
システム。
【請求項８】
前記第１のコンピュータはさらに、前記ボリューム固有の暗号鍵を使用して、前記保護されたボリュームに記憶された前記暗号化データを復号するように構成される、請求項７に記載のシステム。
【請求項９】
前記第１のコンピュータは、前記ボリューム固有の暗号鍵を使用して第２のボリューム

固有の暗号鍵を復号し、前記第２のボリューム固有の暗号鍵を使用して、前記保護されたボリュームに記憶された前記暗号化データを復号するように構成される、請求項８に記載のシステム。
【請求項１０】
前記第１のコンピュータは、ＴＰＭを使用して前記ＴＰＭのシール動作を行うことにより前記キープロテクタを生成する、請求項７に記載のシステム。
【請求項１１】
前記第２のコンピュータは、ＴＰＭを使用しない方式で前記ＴＰＭのシール動作を行うことにより前記キープロテクタを生成する、請求項７に記載のシステム。
【請求項１２】
前記第１のコンピュータは、前記第２のコンピュータにチャレンジを提供するように構成され、
前記第２のコンピュータは、前記チャレンジを前記ランダムデータと組み合わせてレスポンスを生成し、前記レスポンスを前記第１のコンピュータに提供するように構成され、
前記第１のコンピュータはさらに、前記レスポンスから前記ランダムデータを抽出するように構成される、
請求項７に記載のシステム。
【請求項１３】
前記第１のコンピュータは、前記第１のコンピュータのユーザに前記チャレンジを発行して、前記チャレンジをアウトオブバンドで前記第２のコンピュータのユーザに提供させ、前記第２のコンピュータに入力させるように構成される、請求項１２に記載のシステム。
【請求項１４】
前記第２のコンピュータは、前記第２のコンピュータのユーザに前記レスポンスを発行して、前記レスポンスをアウトオブバンドで前記第１のコンピュータのユーザに提供させ、前記第１のコンピュータに入力させるように構成される、請求項１２に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データ暗号化技術に関する。
【背景技術】
【０００２】
いわゆる「フルボリューム暗号化」を行うことにより、コンピュータのファイルシステムのボリュームに記憶されたデータの機密性を保護する各種システムが存在する。そのようなシステムは、ボリュームに記憶されたデータのすべてまたはほぼすべてを暗号化し、権限のあるエンティティから要求があった時にそのようなデータを透過に復号する。例えば、特定のＭＩＣＲＯＳＯＦＴ（登録商標）ＷＩＮＤＯＷＳ（登録商標）オペレーティングシステムは、「ＢＩＴＬＯＣＫＥＲ（商標）ドライブ暗号化（「ＢＩＴＬＯＣＫＥＲ」）」と呼ばれる機能の起動を介してフルボリューム暗号化を提供する。
【０００３】
ＢＩＴＬＯＣＫＥＲ（商標）などのフルボリューム暗号化システムは、保護されたボリュームへのアクセスを管理するために各種の認証方法を提供することができる。例えば、保護されたボリュームが、コンピュータのブート時にアクセスされるオペレーティングシステム（ＯＳ）ボリュームである場合は、そのような方法は、コンピュータに内蔵されたトラステッドプラットフォームモジュール（ＴＰＭ）によって行われる特定のシステム起動コンポーネントの完全性検査に依拠することができる。他の認証方法では、起動キーや個人識別番号（ＰＩＮ）などのアクセス資格情報の提供を要求する場合がある。起動キーは、例えば、起動キーを記憶した何らかの形態の携帯型記憶媒体をコンピュータのポートに挿入することを通じて提供することができる。ＰＩＮは、例えばユーザによる手動の入

力を介して提供することができる。さらに他の認証方法では、ＴＰＭに基づく完全性検査と、１つまたは複数のアクセス資格情報の提供を組み合わせるものがある。

【０００４】

場合によっては、一度だけ使用できる認証方法がフルボリューム暗号化システムで提供されると望ましい。そのようなシナリオには例えば復旧のシナリオやシステム管理のシナリオがある。復旧のシナリオに関しては、何らかの正当な理由から、平常使用する認証方法を回避して保護ボリュームにアクセスしなければならない状況があり得る。そのような状況には、例えば、ハードウェア障害や、平常の認証方法に関連付けられたアクセス資格情報を喪失した場合がある。一部の従来のフルボリューム暗号化システムでは、対応する復旧用の認証方法を使用して保護ボリュームへのアクセスを実現できるように、復旧用のアクセス資格情報が供給される。この復旧用の認証方法は、平常の認証方法を回避するために恒久的に使用するものではなく、特定のアクセス事例に限って使用するためのものである。しかし、そのような従来のフルボリューム暗号化システムでは、一度復旧用のアクセス資格情報が提供されると、その復旧用アクセス資格情報に関連付けられた特定の対応する鍵材料が保護ボリュームに存在する限り、その資格情報を継続使用して、保護されたボリュームをロック解除することができる。これは望ましくないセキュリティ上の危険性を呈する。

【０００５】

システム管理に関しては、人間の介在なしにコンピュータを再起動することができると望ましい場合がある。例えば、情報技術（ＩＴ）管理者が、企業ネットワークを介して遠隔のクライアントコンピュータのアプリケーションを更新したり、パッチプログラムをインストールしたい場合があるが、そのような更新やインストールを行うにはクライアントコンピュータを再起動することが必要となる。クライアントコンピュータが、ユーザ対話を必要とする形態の認証で保護されている場合は、再起動を強制すると、クライアントコンピュータは、ブート前の環境でそのようなユーザ対話を待つことになる（例えば、クライアントコンピュータはユーザにＰＩＮの入力を求め、ＰＩＮの入力を待つ）。平常使用している認証方法を変更することなく、その特定のクライアントコンピュータに平常使用している認証形態を回避するために利用できる一度限り使用可能な認証方法があれば、ＩＴ管理者は制約を受けずに必要な更新やパッチを導入することができる。

【発明の概要】

【０００６】

この概要は、以下の発明を実施するための形態でさらに説明する概念のうちいくつかを簡略化した形で紹介するために提供される。この概要は、特許請求される主題の主要な特徴や必須の特徴を明らかにするものでも、特許請求される主題の範囲を限定するために使用すべきものでもない。さらに、本発明は、発明を実施するための形態および／または本文書の他の項に記載される特定の実施形態に限定されないことに留意されたい。そのような実施形態は単に説明の目的で本明細書に提示する。本明細書に含まれる教示に基づいて、当業者にはさらなる実施形態が明らかになろう。

【０００７】

上記の背景技術の項で述べたように、状況によっては、フルボリューム暗号化を使用して保護されたコンピュータのボリュームに緊急アクセスするためのロック解除に使用することができる認証方法を提供することが望まれる。例えば、保護されたボリュームに関連付けられたアクセス資格情報（ｃｒｅｄｅｎｔｉａｌ）を喪失した場合に、そのような認証方法を使用して、保護されたボリュームにアクセスして、障害が発生している保護されたボリュームからデータを抽出する、またはコンピュータを再起動してセキュリティアップデートをインストールするなどの緊急を要する管理機能を行うことができる。そのような認証方法には一部のシステム防御手段を省略させることができるため、一度しか使用できないことが理想的である。これを実現するために、本明細書に記載される実施形態は、コンピュータの保護されたボリュームに記憶された暗号化データにアクセスするための一度限り使用可能な認証方法を提供し、暗号化データへのアクセスは、保護されたボリュー

ムを復号するために必要なボリューム固有の暗号鍵を保持する、コンピュータに記憶されたキープロテクタ（ｋｅｙ　ｐｒｏｔｅｃｔｏｒ）を復号することを要する。以下で説明するように、そのような一度限り使用可能な認証方法は、一般に、一度のみ使用することができ（ｓｉｎｇｌｅ－ｕｓｅ）、かつ／または使用のたびに新しいアクセス資格情報を必要とするキープロテクタの提供に依拠する。特定の実施形態では、認証方法の一部としてチャレンジ－レスポンス処理も使用して、キープロテクタおよび／またはアクセス資格情報の発行を、ユーザを一意に識別することができる特定の情報に結びつける。

【０００８】

本発明のさらなる特徴および利点、ならびに本発明の各種実施形態の構造および動作について、以下で添付図面を参照して詳細に説明する。本発明は、本明細書に記載される特定の実施形態に限定されないことに留意されたい。そのような実施形態は単に説明の目的で本明細書に提示する。本明細書に含まれる教示に基づいて、当業者にはさらなる実施形態が明らかになろう。

【図面の簡単な説明】

【０００９】

本明細書に組み込まれ、本願明細書の一部をなす添付図面は本発明の実施形態を示し、説明と併せて本発明の原理をさらに説明する役割を果たし、当業者が本発明をなし、使用することを可能にする。

【００１０】

【図１】各種実施形態を実施することが可能な例示的動作環境のブロック図である。

【図２】一実施形態による、フルボリューム暗号化機能を提供するように構成された例示的クライアントコンピュータのブロック図である。

【図３】各種実施形態による、コンピュータの保護されたボリュームに記憶された暗号化データへのアクセスを制御する一般的な一度限り使用可能な認証方法のフローチャートである。

【図４】使い捨てのキープロテクタに基づく、コンピュータの保護されたボリュームに記憶された暗号化データへのアクセスを制御する一度限り使用可能な認証方法のフローチャートである。

【図５】トラステッドプラットフォームモジュール（ＴＰＭ）および人間の介在を使用する一度限りのロック解除に基づく、コンピュータの保護されたボリュームに記憶された暗号化データへのアクセスを制御する一度限り使用可能な認証方法のフローチャートである。

【図６Ａ】ＴＰＭおよびサーバの介在を使用する一度限りのロック解除に基づく、コンピュータの保護されたボリュームに記憶された暗号化データへのアクセスを制御する一度限り使用可能な認証方法のフローチャートを示す図である。

【図６Ｂ】ＴＰＭおよびサーバの介在を使用する一度限りのロック解除に基づく、コンピュータの保護されたボリュームに記憶された暗号化データへのアクセスを制御する一度限り使用可能な認証方法のフローチャートを示す図である。

【図７Ａ】ＴＰＭの委任（ｄｅｌｅｇａｔｉｏｎ）を使用する一度限りのロック解除に基づく、コンピュータの保護されたボリュームに記憶された暗号化データへのアクセスを制御する一度限り使用可能な認証方法のフローチャートを示す図である。

【図７Ｂ】ＴＰＭの委任を使用する一度限りのロック解除に基づく、コンピュータの保護されたボリュームに記憶された暗号化データへのアクセスを制御する一度限り使用可能な認証方法のフローチャートを示す図である。

【図８】本明細書に記載の各種実施形態を実施するために使用することができる例示的コンピュータシステムのブロック図である。

【発明を実施するための形態】

【００１１】

本発明の特徴および利点は、図面と併せて以下の詳細な説明を読むことにより明らかになろう。すべての図面で、対応する要素は同様の参照符号で識別する。図面では、概して

、同様の参照符号で、同一の要素、機能的に類似する要素、および／または構造的に類似する要素を示す。要素が最初に登場する図面は、対応する参照符号の一番左の桁で示す。

【００１２】

Ｉ．概要

以下の詳細な説明では、本発明の例示的実施形態を示す添付図面を参照する。しかし、本発明の範囲はそれらの実施形態に制限されず、特許請求の範囲により定義される。したがって、図の実施形態を改変したものなど、添付図面に図示する以外の実施形態も本発明に包含されうる。

【００１３】

本明細書中の「一実施形態」「実施形態」「例示的実施形態」等は、記載されるその実施形態が特定の機能、構造、または特徴を含むことができるが、すべての実施形態が必ずしもその特定の機能、構造、または特徴を含むとは限らないことを意味する。さらに、そのような文言は必ずしも同じ実施形態を指さない。さらに、特定の機能、構造、または特徴をある実施形態との関連で記載する場合、明示的に記載されるか否かに関わらず他の実施形態との関連でその機能、構造、または特徴を実施することは当業者の知識の範囲内であると考える。

【００１４】

Ａ．例示的動作環境

コンピュータの保護されたボリュームに記憶された暗号化データにアクセスするための一度限り使用可能な認証方法を本明細書に記載する。そのような方法の理解を助けるために、以下でそのような方法を実施することが可能な例示的システム１００について図１のブロック図を参照して説明する。ただし、当業者は、本明細書に記載の方法はシステム１００以外の幅広いシステムによって行うことが可能であることを理解されよう。

【００１５】

図１に示すように、システム１００は、複数のクライアントコンピュータ１０４$_1$～１０４$_N$と、サーバ１０６と、管理者用（管理者）コンピュータ１０８とを通信可能に接続するネットワーク１０２を含む。システム１００は、例えば、企業または会社のコンピューティング環境に相当する。ただし、この例は制限的なものではなく、システム１００は他のコンピューティング環境も表すことができる。次にシステム１００の各要素について説明する。

【００１６】

ネットワーク１０２は、各種の通信チャネルで接続されたコンピュータおよび装置（例えばルータ、スイッチ、ブリッジ、ハブ、および中継器）の集合を表す。ネットワーク１０２は、システム１００のユーザ間の通信を容易にし、ユーザが他のユーザと情報およびリソースを共有することを可能にする。ネットワーク１０２は、任意種類の有線技術、無線技術、またはそれらの組み合わせを使用して実施することができる。ネットワーク１０２は、例えば、ローカルエリアネットワーク、ワイドエリアネットワーク、グローバルエリアネットワーク、企業の私設網、仮想私設網などを表すことができる。

【００１７】

各クライアントコンピュータ１０４$_1$～１０４$_N$は、ユーザが各種のコンピューティング動作を行うことができるように構成される。そのようなコンピューティング動作を容易に行えるように、各クライアントコンピュータ１０４$_1$～１０４$_N$は、ローカルにデータを記憶するために使用可能なファイルシステムを備え、ファイルシステムは、「ボリューム」と呼ばれる、１つまたは複数の論理的に定義された記憶領域を備える。各クライアントコンピュータ１０４$_1$～１０４$_N$はさらに、いわゆる「フルボリューム暗号化」を行うことにより、少なくとも１つのファイルシステムボリュームに記憶されたプログラム命令またはデータの機密性を保護するコンポーネントを含む。例示的なクライアントコンピュータ２００については図２を参照してより詳細に説明する。

【００１８】

サーバ１０６は、クライアントコンピュータ１０４$_1$～１０４$_N$のために、またはその代

理として１つまたは複数のサービスを行うように構成され、またシステム１００に関してシステムレベルのタスクを行うように構成することも可能なコンピュータである。サーバ１０６は、システム１００内でネットワーク１０２に接続された任意数のサーバの１つを含みうる。一実施形態では、サーバ１０６は、ＭＩＣＲＯＳＯＦＴ（登録商標）ＡＣＴＩＶＥ　ＤＩＲＥＣＴＯＲＹ（登録商標）で提供されるようなネットワークサービスをシステム１００内のエンティティに提供するように構成されるが、この例は制限的なものではない。これも本明細書で後述するように、各種実施形態で、サーバ１０６は、クライアントコンピュータ104_1～104_Nのうち１つの保護されたボリュームに記憶されたデータへのアクセスを管理するために一度限りの認証方法を実行する際に必要な動作を行うように構成される。サーバ１０６はさらに、特定の実施の要件に応じて各種の他の機能を行うように構成することができる。

【００１９】

指定された機能を行うために、サーバ１０６は、メモリ１１０に通信可能に接続され、メモリ１１０にデータを記憶し、メモリ１１０のデータにアクセスするように構成される。メモリ１１０は、サーバ１０６からアクセス可能な任意種の記憶装置またはシステムを含みうる。メモリ１１０は、ネットワーク１０２または何らかの他のインタフェースを介してサーバ１０６に接続されうる。サーバ１０６がＭＩＣＲＯＳＯＦＴ（登録商標）ＡＣＴＩＶＥ　ＤＩＲＥＣＴＯＲＹ（登録商標）のネットワークサービスを提供するように構成される実施形態では、メモリ１１０はＡＣＴＩＶＥ　ＤＩＲＥＣＴＯＲＹ（登録商標）データベースを記憶することができる。

【００２０】

管理者コンピュータ１０８は、権限を与えられた情報技術（ＩＴ）管理者などの権限ユーザがシステム１００に関する設定および管理作業を行うことを可能にするように構成される。それらの作業には、例えば、ユーザ特権および許可の作成および維持、クライアントコンピュータ104_1～104_N、サーバ１０６、ネットワークの動作およびリソースの監視、クライアントコンピュータ104_1～104_Nまたはサーバ１０６にインストールされたソフトウェアの更新および／またはパッチの適用、リポートの生成、セキュリティおよび監査ポリシーの設定等が含まれる。本明細書で後述するように、各種実施形態で、権限ユーザは管理者コンピュータ１０８を使用して、クライアントコンピュータ104_1～104_Nのいずれか１つの保護されたボリュームに記憶されたデータへのアクセスを制御するための一度限りの認証方法を設定および／または実行することができる。

【００２１】

図２は、一実施形態による、フルボリューム暗号化機能を提供するように構成された例示的なクライアントコンピュータ２００のブロック図である。クライアントコンピュータ２００は、図１に示すクライアントコンピュータ104_1～104_Nのいずれにも相当しうる。実装に応じて、クライアントコンピュータ２００は、デスクトップコンピュータ、ラップトップコンピュータ、タブレットコンピュータ、携帯情報端末（ＰＤＡ）、またはプロセッサを利用した他のシステムもしくは装置を含みうる。図２に示すように、クライアントコンピュータ２００は、ハードウェア層２０２およびソフトウェア層２０４を備える。以下でこれらの各層を説明する。

【００２２】

ハードウェア層２０２は、これらに限定されないが、処理装置２１２、システムメモリ２１４、１つまたは複数の大容量記憶装置２１６、およびトラステッドプラットフォームモジュール（ＴＰＭ）２１８を含む、相互接続された複数のハードウェアコンポーネントを備える。処理装置２１２は、システムメモリ２１４に記憶されたプログラム命令を実行して、クライアントコンピュータ２００に指定された機能を行わせるように設計された１つまたは複数のマイクロプロセッサまたはマイクロプロセッサコアを備える。システムメモリ２１４は、実行時に処理装置２１２に消費されるプログラム命令または生成されるデータを一時的に記憶する１つまたは複数の揮発性記憶装置を備える。大容量記憶装置２１６は、クライアントコンピュータ２００のプログラム命令および／またはデータを恒久的

に記憶するために使用される不揮発性の記憶装置を備える。大容量記憶装置２１６は、１つまたは複数の内蔵ハードディスクドライブなどクライアントコンピュータ２００の一部を形成する装置、および／または、１つまたは複数の携帯型記憶装置やドライブなど、クライアントコンピュータのユーザによってクライアントコンピュータ２００に接続できる装置を含むことができる。ＴＰＭ２１８は、クライアントコンピュータ２００が、Ｔｒｕｓｔｅｄ　Ｃｏｍｐｕｔｉｎｇ　Ｇｒｏｕｐから発行されるトラステッドプラットフォームモジュール仕様の少なくとも１つのバージョンの機能を実施することを可能にするセキュアな暗号処理装置を備える。ハードウェア層２０２に含めることができるが図２に示さない他のハードウェア装置には、これらに限定されないが、ビデオアダプタおよびそれに関連するディスプレイ、１つまたは複数の入力／出力（Ｉ／Ｏ）装置インタフェース、ネットワークインタフェース等がある。

【００２３】

ソフトウェア層２０４は、処理装置２１２などのハードウェア層２０２内の要素によって実行される、特定機能を行う複数のソフトウェア要素を備える。図２に示すように、ソフトウェア層２０４は、システム起動コンポーネント２２２およびオペレーティングシステム２２４を含む。

【００２４】

システム起動コンポーネント２２２は、オペレーティングシステム２２４がシステムメモリ２１４にロードされ、処理装置２１２に実行される前に実行されるコンポーネントからなる。システム起動コンポーネント２２２には、基本入出力システム（ＢＩＯＳ）２３２およびブートマネジャ２３４が含まれる。ＢＩＯＳ２３２は、クライアントコンピュータ２００に電源が投入された時にクライアントコンピュータ２００によって最初に実行されるコードである。諸機能の中でも、ＢＩＯＳ２３２は特に、ハードウェア層２０２に含まれる特定の装置を識別、検査、および初期化する働きをする。クライアントコンピュータ２００が既知の状態に設定されると、ＢＩＯＳ２３２はブートマネジャ２３４を実行させ、ブートマネジャ２３４は処理装置２１２による実行のためにオペレーティングシステム２２４をシステムメモリ２１４にロードする。特定の実装では、ブートマネジャ２３４は、ユーザが複数のオペレーティングシステムの中からロードして実行するものを選択することを可能にする。

【００２５】

オペレーティングシステム２２４は、クライアントコンピュータ２００で実行されるソフトウェアアプリケーション（図２には図示せず）に対するホストとして機能する。例えば、オペレーティングシステム２２４は、クライアントコンピュータ２００で実行される各種アプリケーションによるクライアントコンピュータ２００のリソースの共有を管理し、調整する。オペレーティングシステム２２４は、そのようなソフトウェアアプリケーションに代わってハードウェア層２０２の各種要素とのインタフェースをもとり、それによりアプリケーションがハードウェア動作の詳細を管理せずに済むようにし、アプリケーションへの書き込みを容易にする。オペレーティングシステム２２４は、アプリケーションおよびユーザに複数のサービスを提供することができる。アプリケーションは、アプリケーションプログラミングインタフェース（ＡＰＩ）またはシステムコールを通じてそれらのサービスにアクセスすることができる。そのようなインタフェースを呼び出すことにより、アプリケーションは、オペレーティングシステム２２４にサービスを要求し、パラメータを渡し、結果を受け取ることができる。特定の実装では、ユーザは、コマンドラインインタフェース（ＣＬＩ）やグラフィックユーザインタフェース（ＧＵＩ）などのソフトウェアユーザインタフェース（ＳＵＩ）を介してオペレーティングシステム２２４と対話することができる。

【００２６】

一実施形態では、オペレーティングシステム２２４は、ワシントン州レドモンドのＭｉｃｒｏｓｏｆｔ　Ｃｏｒｐｏｒａｔｉｏｎから公開されるＷＩＮＤＯＷＳ（登録商標）ＶＩＳＴＡ（登録商標）またはＷＩＮＤＯＷＳ（登録商標）７オペレーティングシステムか

らなる。ただしこの例は制限的なものでなく、オペレーティングシステム２２４は、上述の機能の少なくとも１つまたは複数を行うように設計された、従来または今後開発されるオペレーティングシステムから構成されうる。

【００２７】

図２に示すように、オペレーティングシステム２２４はファイルシステム２４４を備える。ファイルシステム２４４は、コンピュータプログラムファイルおよびデータファイルを大容量記憶装置２１６に記憶し、大容量記憶装置２１６から取り出し、編成し、その他の形で操作するための操作のセットを提供する。それらの操作は、オペレーティングシステム２２４および／またはオペレーティングシステムで実行されるアプリケーションによって使用されうる。ファイルシステム２４４により記憶されたファイルは、「ボリューム」と呼ばれる、論理的に定義された記憶領域に記憶される。論理ボリュームマネジャ２４８は、そのような論理ボリュームを、大容量記憶装置２１６にある実際の物理記憶領域に対応付ける役割を担う。したがって、論理ボリュームマネジャ２４８は、ファイルシステム２４４によって行われるファイル操作を処理して、大容量記憶装置２１６内の適切な領域がアクセスされることを保証しなければならない。

【００２８】

図２にさらに示すように、オペレーティングシステム２２４はオペレーティングシステム（ＯＳ）暗号化モジュール２４２も含む。ＯＳ暗号化モジュール２４２は、処理装置２１２に実行されるとユーザがファイルシステム２４４のボリュームに選択的にフルボリューム暗号化を適用できるようにするロジックを備える。ボリュームにフルボリューム暗号化が適用されると、そのボリュームに記憶されたすべてのデータ（例外がある場合もある）が暗号化される。そのような暗号化データはその後、権限のあるエンティティから要求があった時に透過に復号される。データの暗号化および復号は、ファイルシステム２４４と論理ボリュームマネジャ２４８との間にインストールされた暗号化フィルタドライバ２４６で処理される。暗号化フィルタドライバ２４６は、保護されたボリュームへの記憶動作の一部としてファイルシステム２４４から論理ボリュームマネジャ２４８に渡されるデータを暗号化し、保護されたボリュームへのアクセス動作の一部として論理ボリュームマネジャ２４８からファイルシステム２４４に渡されるデータを復号するように動作する。本明細書で使用される場合、用語「保護されたボリューム」とは、そのようなフルボリューム暗号化が適用されたボリュームを言う。保護されたボリュームは、オペレーティングシステム２２４の実行に必要なファイルを記憶するオペレーティングシステム（ＯＳ）ボリュームや、実行時（すなわちオペレーティングシステム２２４が立ち上がり、実行されている時）にアクセスされるアプリケーションデータや他のデータを記憶する物理的または仮想的なデータボリュームを含むことができる。

【００２９】

一実施形態では、クライアントコンピュータ２００が提供するフルボリューム暗号化機能は、ＭＩＣＲＯＳＯＦＴ（登録商標）ＷＩＮＤＯＷＳ（登録商標）オペレーティングシステムの１つまたは複数のバージョンに含まれるＢＩＴＬＯＣＫＥＲ（商標）ドライブ暗号化（「ＢＩＴＬＯＣＫＥＲ」）の機能に対応するが、この例は制限的なものではない。

【００３０】

一実施形態によると、保護されたボリュームのセクタは、そのボリュームに関連付けられたフルボリューム暗号化キー（ＦＶＥＫ）を使用して暗号化される。そして、ＦＶＥＫは、ボリュームマスタキー（ＶＭＫ）と呼ばれる鍵で暗号化される。ＶＭＫで暗号化されたＦＶＥＫは、いわゆるボリュームメタデータの一部として、保護されたボリューム自体に記憶される。ＦＶＥＫはローカルに記憶されるが、暗号化されない状態でディスクに書き込まれることは決してない。ＶＭＫも暗号化、すなわち「保護」されるが、ＶＭＫは１つまたは複数の可能な「キープロテクタ」で暗号化される。すなわち、ＶＭＫは、種々の認証方法に対応する各種の異なる方式で暗号化し、記憶することができる。暗号化されたバージョンのＶＭＫすなわちキープロテクタも、保護されたボリューム自体に、ボリュームメタデータの一部として記憶される。

【００３１】
クライアントコンピュータ２００は、復号を通じて保護されたボリュームの暗号化データへのアクセスを得ることをエンティティに許す前に、そのエンティティを認証するために各種の異なる処理のいずれかを行うように構成することができる。エンティティが認証処理に合格すると、暗号化データへのアクセスが許可される。エンティティが認証処理に不合格の場合は、暗号化データへのアクセスが拒否される。上記のように、一実施形態では、暗号化データにアクセスするには、まずキープロテクタで保護されている（すなわち暗号化された）ＶＭＫを入手し、次いで暗号化を解除したＶＭＫを使用してＦＶＥＫを復号し、最後にＦＶＥＫを使用して保護されたボリュームの暗号化セクタを復号することが必要となる。

【００３２】
保護されたボリュームはシステム起動時と実行時にアクセスされる可能性があるため、ソフトウェア層２０４は、そのような認証処理を行うことができる２つの異なるコンポーネントを含む。システム起動時には、ブートマネジャ２３４の一部であるｐｒｅ－ＯＳ暗号化モジュール２６２によって認証が行われ、実行時には暗号化フィルタドライバ２４６内のロジックによって認証が行われる。

【００３３】
例えば、保護されたボリュームが、コンピュータのブート時にアクセスされるＯＳボリュームの場合は、ｐｒｅ－ＯＳ暗号化モジュール２６２は、ＯＳボリュームへのアクセスを許可する前に特定のシステム起動コンポーネントの完全性検査を行うように構成することができる。この認証機構は、ＴＰＭ２１８を使用してＯＳボリュームのＶＭＫをＴＰＭ２１８で計測された特定のシステム起動コンポーネントの状態に「シール（ｓｅａｌ）」することによって初期化される。そして、システムの起動中に同じコンポーネントをＴＰＭ２１８で計測して、コンポーネントの状態が、シール動作が行われた時と同じであるかどうかを判定する。状態が一致する場合は、ＶＭＫが「アンシール（ｕｎｓｅａｌ）」され（非暗号化形態で提供され）、保護されたＯＳボリュームへのアクセスを実現することができる。対して、状態が一致しない場合は、ＶＭＫはシール状態のままにされ、保護されたＯＳボリュームへのアクセスが拒否される。これにより、クライアントコンピュータ２００は、クライアントコンピュータ２００の特定の起動コンポーネントが改ざんされた場合に、保護されたＯＳボリュームへのアクセスを拒否することができる。ＴＰＭ２１８を使用してシールおよびアンシール動作を行う方式は当業者に知られていよう。

【００３４】
ｐｒｅ－ＯＳ暗号化モジュール２６２が備える他の認証機構は、ＶＭＫを復号するために起動キーや個人識別番号（ＰＩＮ）などのアクセス資格情報の提供を要求することができる。起動キーは、例えば、起動キーを記憶した何らかの形態の携帯型記憶装置（例えばＵＳＢサム（ｔｈｕｍｂ）ドライブ）をクライアントコンピュータ２００のポートに挿入することによって提供することができる。ＰＩＮは、クライアントコンピュータ２００の１つまたは複数の入力装置を使用して、ユーザの手動入力を介して提供することができる。さらに他の認証機構は、ＶＭＫを復号するために、ＴＰＭを利用した完全性検査に合格し、かつ１つまたは複数のアクセス資格情報を提供することを求めることができる。

【００３５】
暗号化フィルタドライバ２４６は、上記でｐｒｅ－ＯＳ暗号化モジュール２６２を参照して説明したのと同様の認証処理を行って、実行時にファイルシステム２４４の暗号化されたデータボリュームへのアクセスを制御することができる。

Ｂ．一度限り使用可能な認証方法の利点

【００３６】
場合によっては、緊急のアクセスのためにクライアントコンピュータ２００の保護されたボリュームのロックを解除するために使用できる認証方法があることが望ましい。例えば、保護されたボリュームに関連付けられたアクセス資格情報（例えば起動キーやＰＩＮ）を喪失した場合に、そのような認証方法を使用して保護されたボリュームにアクセスし

て、障害が発生している保護されたボリュームからデータを抽出する、またはクライアントコンピュータ２００を再起動してセキュリティアップデートをインストールするなどの緊急を要する管理機能を行うことができる。そのような認証方法では、ＴＰＭを利用した完全性検査などの一部のシステム防御手段を省略するようにしてよい。したがって、使用のたびにＩＴ管理者または同様の権限者からの明示的な許可を得ないと認証方法を使用することができない場合に有用であると考えられる。これを実現するために、本明細書に記載される実施形態は、保護されたボリュームへのアクセスを管理するための一度限り使用可能な認証方法を提供する。下記で説明するように、そのような一度限り使用可能な認証方法は一般に、一度のみ使用することができ、かつ／または使用のたびに新しいアクセス資格情報を必要とするキープロテクタの提供に依拠する。特定の実施形態では、認証方法の一部としてチャレンジ－レスポンス処理も使用して、キープロテクタおよび／またはアクセス資格情報の発行を、ユーザを一意に識別することができる特定の情報に結びつける。

【００３７】

セキュリティの観点から、一度限り使用可能な認証方法は、権限ユーザの不注意から生じる誤使用、また、いくらかの時間クライアントコンピュータ２００を観察してクライアントコンピュータ２００（および可能性としては他の情報）を捕捉する無許可ユーザによる誤使用を防止しなければならない。攻撃者がロックがかかっていないシステムを危険にさらす攻撃は対象とならない。何故ならば、そのような場合攻撃者は初めから保護されたボリュームの内容を入手することができ、システムのロックを解除する必要がないためである。

【００３８】

特に次のような攻撃から防御すると有益であると考えられる。

【００３９】

（１）認証方法が、ユーザにパスワードの入力を求める場合に、そのパスワードを（例えばユーザがパスワードを書き留めた紙を見つけることにより）知った攻撃者がパスワードの再使用を試みる。

【００４０】

（２）認証方法が、クライアントコンピュータがネットワークを介してサーバと対話することを求める場合に、過去に行われたそのような対話を観察した攻撃者が単に以前のサーバからのレスポンスを再現することにより、クライアントコンピュータに、保護されたボリュームのロックを解除させることを試みる。

【００４１】

（３）認証方法が、クライアントコンピュータがネットワークを通じてサーバと対話することを求める場合に、過去にそのような対話を観察した攻撃者が単に過去のクライアントコンピュータからのレスポンスを再生することにより、サーバに、保護されたボリュームのロックを解除させることを試みる。

【００４２】

（４）認証方法が、クライアントコンピュータがネットワークを通じてサーバと対話することを求める場合に、攻撃者が、クライアントコンピュータで実行されるコードを改変する、または攻撃者の制御下にある悪意あるシステムに対して要求を行う。

【００４３】

（５）過去に緊急アクセスのためにロック解除されたクライアントコンピュータを捕捉した攻撃者がクライアントコンピュータのディスク内容を以前の状態に戻すことにより、ロック解除動作を繰り返すことを試みる。

【００４４】

（６）クライアントで緊急のキープロテクタを作成する際にサーバとの通信が必要とされる場合に、攻撃者がその通信を妨害することによりサービス否定攻撃を行うことを試みる。そのような妨害は、例えばタイミングの悪いネットワーク故障が原因となるなど、悪意ある攻撃者がいない場合にも起こりうることに留意されたい。

【００４５】
以下の項で、上記の攻撃の一部もしくはすべて、またはそれらの組み合わせに対して安全な方法を説明する。
【００４６】
ＩＩ．一度限り使用可能な認証方法の例
以下で、コンピュータの保護されたボリュームに記憶された暗号化データへの制御されたアクセスを提供するために使用できる例示的な認証方法を説明する。この認証方法は一度のみ使用することができる。上記のように、そのような一度限り使用可能な認証方法は、保護されたボリュームに関連付けられた通常使用される認証機構を一度だけ回避できるようにすることが望ましい、復旧のシナリオやシステム管理のシナリオなどの特定のシナリオで有利に使用されうる。
【００４７】
単に説明の目的で、この項で提示する各種の方法ステップは、上記で図１を参照して説明した例示的システム１００内のエンティティ、および／または、上記で図２を参照して説明した例示的クライアントコンピュータ２００のハードウェアまたはソフトウェアコンポーネントによって行われる動作として説明する。ただし、本明細書に提供される教示に基づき、当業者は、そのような方法ステップは、図１および図２に示す以外のエンティティまたはコンポーネントによって行うことも可能であることを容易に理解されよう。
【００４８】
下記の例示的一度限り使用可能な認証方法はすべて、基本的に同じ高レベル処理の流れに従う。それらの方法の理解を助けるために、この高レベル処理の流れについて図３のフローチャート３００を参照して説明する。以下に説明する例示的な一度限り使用可能な認証方法では、フローチャート３００に示す以外の追加的なステップを行うこともでき、またはフローチャート３００の記載とわずかに異なる方式でステップを行うこともできることを理解されたい。したがって、フローチャート３００は、下記の方法に関して制限的なものと見なすべきでない。
【００４９】
図３に示すように、フローチャート３００の方法はステップ３０２で開始し、クライアントコンピュータ２００の保護されたボリュームなど、第１のコンピュータの保護されたボリュームを復号するために必要なボリューム固有の暗号鍵を暗号化することによりキープロテクタが生成される。一実施形態では、ボリューム固有の暗号鍵は、それ自体を使用してフルボリューム暗号化キー（ＦＶＥＫ）を復号することができるボリュームマスタキー（ＶＭＫ）からなる。そして、ＦＶＥＫを使用して、保護されたボリュームの暗号化セクタを復号することができる。
【００５０】
ステップ３０４で、クライアントコンピュータ２００のローカルメモリなど、第１のコンピュータのローカルメモリにキープロテクタを記憶して、後に第１のコンピュータが保護されたボリュームを復号する必要がある時に第１のコンピュータからアクセスできるようにする。一実施形態では、キープロテクタは、いわゆる「ボリュームメタデータ」の一部として、保護されたボリュームの一部分に記憶される。
【００５１】
判定ステップ３０６で、第１のコンピュータが、保護されたボリュームにアクセスする試みが検出されたかどうかを判定する。保護されたボリュームにアクセスする試みが検出されていない場合は判定ステップ３０６を繰り返す。保護されたボリュームにアクセスする試みが検出されている場合は、制御はステップ３０８に進む。
【００５２】
ステップ３０８で、第１のコンピュータが、ローカルメモリに記憶されたキープロテクタを復号するために必要な１つまたは複数のアクセス資格情報を取得する。下記で説明するように、使用する方法に応じて、ステップ３０８で取得されるアクセス資格情報は、キープロテクタを復号するために必要な暗号鍵、ＴＰＭを使用してキープロテクタをアンシ

ールするために必要な計測値、または、ＴＰＭに関連付けられた移動不可能な暗号鍵を利用するために必要な認証コードを含むことができるが、これらの例は制限的なものではない。

【００５３】

ステップ３１０で、第１のコンピュータは、ステップ３０８で取得したアクセス資格情報を使用してキープロテクタを復号し、それによりボリューム固有の暗号鍵を取得する。上記のように、特定の実施形態では、キープロテクタを復号することによりＶＭＫを得ることができ、次いでそのＶＭＫを使用して、保護されたボリュームのセクタを復号するのに必要なＦＶＥＫを復号する。

【００５４】

ステップ３１２で、キープロテクタを削除することにより、および／またはキープロテクタを復号するために必要なアクセス資格情報を削除もしくは変更することにより、認証方法が一度のみ使用されることを保証する。この重要なステップを行う各種方式については、各例示的方法を参照して下記で説明する。

【００５５】

下記の例示的方法の少なくとも１つによると、前述の方法は、新しいキープロテクタおよび／またはアクセス資格情報を自動的に供給することにより、暗号化ボリュームへのアクセスを得るために使用できる一度限り使用可能な認証方法を新たに設定する追加的ステップも含む。そのようなステップは、管理作業を行うために一度限り使用可能な認証方法が使用される場合は必要でない場合もある。管理作業の場合は、ＩＴ管理者などの人間の作業主導者が供給機能を行うことができる。一方、一度限り使用可能な認証方法が緊急作業を行うために使用される場合は、そのような供給を行うことができる時が他にない可能性があるため、そのようなステップが重要となる可能性がある。

【００５６】

第１のコンピュータがクライアントコンピュータ２００である実施形態では、第１のコンピュータによって行われる、保護されたボリュームへのアクセスの検出、および保護されたボリュームに関連付けられたキープロテクタの復号に関連する機能は、ｐｒｅ－ＯＳ暗号化モジュール２６２または暗号化フィルタドライバ２４６のどちらかによって行うことができる。例えば、保護されたＯＳボリュームへのアクセスがシステム起動時に試みられる場合はｐｒｅ－ＯＳ暗号化モジュール２６２がそのような機能を行い、一方、保護されたデータボリュームへのアクセスが実行時に試みられる場合は暗号化フィルタドライバ２４６がそれらの機能を行うことができる。ただし、これらは例に過ぎず、クライアントコンピュータ２００内の他のコンポーネントを使用してそれらの機能を行ってもよい。

【００５７】

下記で提供する例示的方法の説明から明らかにするように、例示的方法とその特定の実施に応じて、ステップ３０２、３０８および３１２を行うために必要とされる動作は、第１のコンピュータ（例えばクライアントコンピュータ２００）、第２のコンピュータ（例えばサーバ１０６）、または第１のコンピュータと第２のコンピュータの組み合わせによって行うことができる。それらのステップを行うために必要な動作は、自動的に、またはＩＴ管理者などのその権限ユーザから提供される入力に応答して管理者用コンピュータ（例えば管理者コンピュータ１０８）によって行われるステップをさらに要する場合もある。また、ステップ３０２および３０８を行うために必要な動作は、チャレンジ－レスポンス機構の実行に関連する人間の介在など、人間の介在を要する場合がある。

【００５８】

機密性のあるデータ（これらに限定されないがランダムノンス（ｎｏｎｃｅ）や権限付与データなど）をコンピュータ間で送信することを要する下記の例示的方法の特定の実施では、そのような通信はセキュアな経路で行って、「中間者（ｍａｎ　ｉｎ　ｔｈｅ　ｍｉｄｄｌｅ）」攻撃などを回避する助けとすることができる。

【００５９】

Ａ．使い捨てのキープロテクタに基づく一度限り使用可能な認証方法

図４に、第１のコンピュータの保護されたボリュームに記憶された暗号化データへのアクセスを制御するための一度限り使用可能な認証方法の第１の例のフローチャート４００を示す。下記の説明から明らかにするように、フローチャート４００の方法は使い捨てのキープロテクタの発想に基づくものである。フローチャート４００の方法は、上記の項Ｉ．Ｂで説明した攻撃タイプ（１）、（３）、および（６）を阻止する。この方法では、第１のコンピュータがＴＰＭを備える必要はない。

【００６０】

図４に示すように、フローチャート４００の方法はステップ４０２で開始し、ランダムの非対称の公開鍵と秘密鍵の対が生成される。非対称の公開鍵と秘密鍵の対は、例えば、ＲＳＡ公開鍵と秘密鍵の対からなることができるが、他の非対称公開鍵と秘密鍵の対を使用してもよい。フローチャート４００の方法がシステム１００で実施される実施形態では、ランダムの非対称公開鍵と秘密鍵の対は、自動的に、またはＩＴ管理者などの権限ユーザの動作に基づいて、管理者コンピュータ１０８で生成することができる。あるいは、非対称の公開鍵と秘密鍵の対は、自動的に、または管理者コンピュータ１０８もしくはクライアントコンピュータ２００から受信される通信に応答して、サーバコンピュータ１０６で生成してもよい。

【００６１】

ステップ４０４で、保護されたボリュームを復号するために必要なボリューム固有の暗号鍵を公開鍵で暗号化することによりキープロテクタを生成する。このステップは、第１のコンピュータ、例えばクライアントコンピュータ２００で行うことができる。フローチャート４００の方法がシステム１００で実施され、システム１００がＡＣＴＩＶＥ　ＤＩＲＥＣＴＯＲＹ（登録商標）を利用するネットワークを備える実施形態では、ＡＣＴＩＶＥ　ＤＩＲＥＣＴＯＲＹ（登録商標）のグループポリシーを介して公開鍵をシステム１００内の１つまたは複数のクライアントコンピュータに配布することができる。ただし、これは一例に過ぎず、多数の他の配布機構を使用することができる。例示的システム１００をさらに参照すると、公開鍵は、管理者コンピュータ１０８、サーバ１０６、またはネットワーク１０２上の何らかの他のエンティティから配布することができる。公開鍵は、使い捨てのキープロテクタ識別子および特定のキープロテクタ属性と共に配布することができる。

【００６２】

実装に応じて、ステップ４０４で生成されるキープロテクタを復号するために必要な秘密鍵は、いくつかの異なる場所の１つに記憶することができる。例えば、秘密鍵は、暗号化されていない状態で第１のコンピュータのローカルメモリに記憶することができる（例えば保護されたボリュームに記憶されたボリュームメタデータの一部として）。あるいは、秘密鍵は、ＡＣＴＩＶＥ　ＤＩＲＥＣＴＯＲＹ（登録商標）サーバからアクセス可能なＡＣＴＩＶＥ　ＤＩＲＥＣＴＯＲＹ（登録商標）データベースなど、企業の社内ネットワーク上にセキュアに記憶し、したがって社内ネットワークへのアクセスを必要としてもよい。さらに、秘密鍵は、アクセスするためにチャレンジ－レスポンス対話を要求する信頼されるサーバにセキュアに記憶することができる。フローチャート４００の方法がシステム１００で実施される実施形態では、サーバ１０６は、ＡＣＴＩＶＥ　ＤＩＲＥＣＴＯＲＹ（登録商標）サーバまたは秘密鍵を記憶するために使用される信頼されるサーバからなることができる。一実施形態では、秘密鍵が記憶される場所は、公開鍵と共に配布されるキープロテクタ属性に基づいて決定される。

【００６３】

ステップ４０６で、キープロテクタを第１のコンピュータのローカルメモリに記憶する。例えば、このステップは、保護されたボリュームのボリュームメタデータの一部としてキープロテクタを記憶することからなることができる。一実施形態では、キープロテクタは、キープロテクタが使い捨てのキープロテクタであることを示すフラグまたは他の識別子、および上記で参照したキープロテクタ属性と共に記憶される。

【００６４】

判定ステップ４０８で、第１のコンピュータは、保護されたボリュームにアクセスする試みが検出されたかどうかを判定する。保護されたボリュームにアクセスする試みが検出されていない場合は、判定ステップ４０８を繰り返す。保護されたボリュームにアクセスする試みが検出された場合は、制御はステップ４１０に進む。

【００６５】

ステップ４１０で、保護された鍵にアクセスする試みが検出されたことに応答して、第１のコンピュータは、以前に記憶した秘密鍵を取得する。一実施形態では、このステップは、秘密鍵がどこに記憶されているかを判定し、次いでその場所にある秘密鍵にアクセスすることからなる。秘密鍵が記憶されている場所の判定は、ステップ４０６でキープロテクタと共に記憶された特定のキープロテクタ属性に基づいて行われる。秘密鍵の記憶場所に応じて、このステップは、第１のコンピュータのローカルメモリ（例えば保護されたボリューム内のボリュームメタデータ）から復号されたバージョンの秘密鍵を取得するか、または、ＡＣＴＩＶＥ　ＤＩＲＥＣＴＯＲＹ（登録商標）サーバもしくは秘密鍵を提供することが可能な社内ネットワーク上の他の信頼されるサーバとのセキュアな通信を確立するか、または第１のコンピュータのユーザにチャレンジで働きかけ、適切なレスポンスを待って、信頼されるサーバから秘密鍵を提供することを伴うことができる。サーバへの接触が伴う場合は、第１のコンピュータのローカルメモリに記憶された属性情報で接触するサーバを一意に識別することができ、第１のコンピュータは、ボリューム識別子または該当する秘密鍵を識別するために使用できる他の一意の識別子をサーバに提供することができる。チャレンジ－レスポンス対話を使用する場合は、チャレンジで所定の情報を要求することができ、それらの情報には、これらに限定されないが、例えばドメインユーザ名およびパスワード、従業員ＩＤ等が含まれる。

【００６６】

ステップ４１２で、秘密鍵を取得した後、第１のコンピュータは、秘密鍵を使用してキープロテクタを復号してボリューム固有の暗号鍵を取得する。そして、そのボリューム固有の暗号鍵を使用して、保護されたボリュームの暗号化データを復号することができる。一実施形態では、ボリューム固有の暗号鍵は第１のボリューム固有の暗号鍵（例えばＶＭＫ）からなり、その暗号鍵を使用して第２のボリューム固有の暗号鍵（例えばＦＶＥＫ）を復号することができ、その第２のボリューム固有の暗号鍵を使用して保護されたボリュームの個々のセクタを復号することができる。

【００６７】

ステップ４１４で、第１のコンピュータは、キープロテクタを１回使用した後に、第１のコンピュータのローカルメモリからキープロテクタを削除する。それにより、フローチャート４００の認証方法が一度のみ使用されることが保証される。一実施形態では、第１のコンピュータは、使い捨てのキープロテクタインディケータとキープロテクタとの関連付けに基づいてこのステップを行うようにプログラムされる。例えば、一実施形態では、第１のコンピュータが、保護されたボリュームのボリュームメタデータにあるすべてのキープロテクタを内部で列挙する。使い捨てのキープロテクタとして指定されたキープロテクタが見つかると、第１のコンピュータは、直ちに自動的に（ユーザへの指示や対話を行わずに）そのキープロテクタを削除する。特定の実装では、この動作は、電源異常が発生した場合には次回の電源切断再投入後にキープロテクタの削除を続けることができるように処理することができる。列挙は、同様の使い捨てのキープロテクタがボリュームメタデータになくなるまで、または完了を必要としている未終了の削除動作がなくなるまで継続する。

【００６８】

第１のコンピュータがクライアントコンピュータ２００である実施形態では、保護されたボリュームへのアクセスの検出、秘密鍵の取得、保護されたボリュームに関連付けられたキープロテクタの復号、およびキープロテクタの削除に関連して上記で述べた機能は、ｐｒｅ－ＯＳ暗号化モジュール２６２または暗号化フィルタドライバ２４６によって行うことができる。例えば、保護されたＯＳボリュームへのアクセスがシステム起動時に試み

られる場合は、ｐｒｅ－ＯＳ暗号化モジュール２６２がそのような機能を行い、保護されたデータボリュームへのアクセスが実行時に試みられる場合は暗号化フィルタドライバ２４６がそれらの機能を行うことができる。ただし、これは例に過ぎず、クライアントコンピュータ２００内の他のコンポーネントを使用してこれらの機能を行ってもよい。

【００６９】

Ｂ．ＴＰＭおよび人間の介在を使用する一度限りのロック解除に基づく一度限り使用可能な認証方法

図５に、第１のコンピュータの保護されたボリュームに記憶された暗号化データへのアクセスを制御する第２の一度限り使用可能な認証方法の例のフローチャート５００を示す。下記の説明で明らかにするように、フローチャート５００の方法は、ＴＰＭおよび人間の介在を使用する一度限りのロック解除の発想に基づく。フローチャート５００の方法は、上記Ｉ．Ｂの項で説明した個々の攻撃タイプすべてとそれらの多数の組み合わせを阻止する。ただし、同項で述べた攻撃タイプ（２）と（４）の組み合わせには無効である可能性がある。

【００７０】

フローチャート５００の方法では、第１のコンピュータにＴＰＭが存在することが必要となる。この方法は、ＴＰＭのエクステンド（ｅｘｔｅｎｄ）およびシール動作がそれぞれハッシュ化と公開鍵による暗号化に相当し、したがってそれらの動作はＴＰＭの支援を受けずに別のエンティティによって行えるのに対し、秘密鍵による復号に相当するＴＰＭのアンシール動作はＴＰＭ自体でしか行うことができないことを利用する。ＴＰＭを使用してエクステンド、シールおよびアンシール動作を行う方式は当業者には知られていよう。

【００７１】

図５に示すように、フローチャート５００の方法はステップ５０２で開始し、ＴＰＭのシール動作を行って、保護されたボリュームをＴＰＭの公開鍵で復号するために必要なボリューム固有の暗号鍵を暗号化し、暗号化したボリューム固有の暗号鍵を、ランダム文字列をハッシュ化する（「Ｓ」と呼ぶ場合がある）ことで生成される値にバインドすることにより、キープロテクタを生成する。実装に応じて、ステップ５０２を行うために必要とされる動作は、ＴＰＭを備える第１のコンピュータが行っても、ＴＰＭを備える第１のコンピュータとＴＰＭを備えない第２のコンピュータとの組み合わせで行ってもよい。第１のコンピュータは例えばクライアントコンピュータ２００であり、第２のコンピュータは例えば、サーバ１０６または管理者コンピュータ１０８である。以下にこのステップを行うための各種手法を説明するが、さらに他の手法を用いてもよい。

【００７２】

例えば、一実施形態では、第１のコンピュータが第２のコンピュータに接触する。第１のコンピュータからの接触に応答して、第２のコンピュータは、ランダム文字列Ｓを生成し、次いでハッシュ関数をＳに適用することにより、ランダム文字列Ｓのハッシュを生成する。そしてハッシュが第１のコンピュータに送られる。第１のコンピュータはハッシュをＴＰＭプラットフォームコンフィギュレーションレジスタ（ＰＣＲ）の値として使用し、ＴＰＭのシール動作を行ってボリューム固有の暗号鍵をＴＰＭの公開鍵に従って暗号化すると共に、暗号化されたボリューム固有の暗号鍵をＰＣＲ値にバインドする。このＴＰＭシール動作の実行によりキープロテクタが生成される。

【００７３】

代替実施形態では、第１のコンピュータがボリューム固有の暗号鍵および第１のコンピュータ内にあるＴＰＭの公開鍵を第２のコンピュータに通信する。第２のコンピュータはランダム文字列Ｓを生成し、ハッシュ関数を適用してＰＣＲ値を生成し、ＴＰＭのシール動作を行ってボリューム固有の暗号鍵をＴＰＭの公開鍵に従って暗号化し、また暗号化されたボリューム固有の暗号鍵をＰＣＲ値にバインドする。上記のように、第２のコンピュータは、第１のコンピュータのＴＰＭにアクセスすることができなくてもＴＰＭのシール動作を行うことができる。このＴＰＭのシール動作の実行によりキープロテクタが生成さ

れ、第２のコンピュータはそのキープロテクタを第１のコンピュータに送り返す。

【００７４】

さらに別の代替実施形態では、第１のコンピュータがランダム文字列Ｓを生成してからＴＰＭのエクステンド動作を行ってＴＰＭのＰＣＲにランダム文字列Ｓのハッシュ化バージョンを書き込む。そして、第１のコンピュータは、ＴＰＭシール動作を行ってボリューム固有の暗号鍵をＴＰＭの公開鍵に従って暗号化すると共に、暗号化されたボリューム固有の暗号鍵をＰＣＲ値にバインドすることにより、キープロテクタを生成する。第１のコンピュータはランダム文字列Ｓのコピーを第２のコンピュータに送信し、自身のランダム文字列Ｓのコピーをローカルメモリから削除する。

【００７５】

さらに別の代替実施形態では、第１のコンピュータは人間による入力を要求する。要求に応答して、第１のコンピュータのユーザがＩＴ管理者または他の権限者に接触し、接触に応じてＩＴ管理者が第２のコンピュータを使用してランダム文字列Ｓを生成し、ハッシュ関数を適用することにより、ランダム文字列Ｓのハッシュを生成する。そして、ＩＴ管理者はアウトオブバンド（ｏｕｔ－ｏｆ－ｂａｎｄ）機構（例えば電話、電子メールなど）を介してユーザにハッシュを伝え、ユーザはハッシュを第１のコンピュータに入力する。第１のコンピュータはハッシュをＰＣＲ値として使用し、ＴＰＭのシール動作を行ってボリューム固有の暗号鍵をＴＰＭの公開鍵に従って暗号化すると共に、暗号化されたボリューム固有の暗号鍵をＰＣＲ値にバインドする。このＴＰＭシール動作の実施によりキープロテクタが生成される。

【００７６】

ステップ５０４で、キープロテクタが第１のコンピュータのローカルメモリに記憶される。例えば、このステップは、保護されたボリュームのボリュームメタデータの一部としてキープロテクタを記憶することからなることができる。

【００７７】

ステップ５０６で、ランダム文字列Ｓが、第２のコンピュータからはアクセスできるが第１のコンピュータからはアクセスできないメモリに記憶される。例えば、第２のコンピュータがランダム文字列Ｓを生成するステップ５０２を実施する上記各種方法にさらに従うと、第２のコンピュータは、ランダム文字列Ｓのコピーを、第２のコンピュータからはアクセスできるが第１のコンピュータからはアクセスできないメモリに記憶し、ランダム文字列Ｓを第１のコンピュータに通信することは決してしない。また、第１のコンピュータがランダム文字列Ｓを生成するステップ５０２を実施する上記方法にさらに従うと、第１のコンピュータは、ランダム文字列Ｓのコピーを第２のコンピュータに送信して、第２のコンピュータからはアクセスできるが第１のコンピュータからはアクセスできないメモリに記憶させ、その後自身のランダム文字列Ｓのコピーをローカルメモリから削除する。

【００７８】

判定ステップ５０８で、第１のコンピュータは、保護されたボリュームにアクセスする試みが検出されたかどうかを判定する。保護されたボリュームにアクセスする試みが検出されていない場合は、判定ステップ５０８を繰り返す。保護されたボリュームにアクセスする試みが検出された場合は、制御がステップ５１０に進む。

【００７９】

ステップ５１０で、保護された鍵にアクセスする試みが検出されたことに対応して、第１のコンピュータが第２のコンピュータからランダム文字列Ｓを取得する。

【００８０】

ステップ５１２で、第１のコンピュータは、ランダム文字列Ｓを利用するＴＰＭのアンシール動作を行うことにより、ボリューム固有の暗号鍵を取得する。詳細には、第１のコンピュータは、ＴＰＭのエクステンド動作を行って、ＴＰＭのＰＣＲに、ハッシュ化されたバージョンのランダム文字列Ｓを書き込む。次いで第１のコンピュータはＰＣＲ値を使用するＴＰＭのアンシール動作を行ってシールされているボリューム固有の暗号鍵を復号する。そして、そのボリューム固有の暗号鍵を使用して保護されたボリュームの暗号化デ

ータを復号することができる。一実施形態では、ボリューム固有の暗号鍵は、第１のボリューム固有の暗号鍵（例えばＶＭＫ）からなり、それを使用して第２のボリューム固有の暗号鍵（例えばＦＶＥＫ）を復号することができ、そして第２のボリューム固有の暗号鍵を使用して保護されたボリュームの個々のセクタを復号することができる。

【００８１】

ステップ５１４で、第２のコンピュータは、第２のコンピュータからアクセス可能なメモリからランダム文字列Ｓを削除する。このステップにより、以後第１のコンピュータがランダム文字列Ｓを取得することができず、したがってキープロテクタを再度アンシールできなくなることが保証される。

【００８２】

上記のように、ステップ５１０で、第１のコンピュータは第２のコンピュータからランダム文字列Ｓを取得する。このステップでランダム文字列Ｓが通常のネットワーク通信を介して第２のコンピュータから直接第１のコンピュータに送信された場合は、その際にランダム文字列Ｓが、そのような通信を盗聴することが可能な攻撃者にさらされることになる。この問題に対処するために、一実施形態では、人間の介在に基づくチャレンジ－レスポンス機構を使用して必要な情報を転送する。この機構によると、保護されたボリュームへのアクセスが要求される時、第１のコンピュータはランダムなチャレンジを生成し、それを第１のコンピュータのユーザに表示する。そして、ユーザは、アウトオブバンド通信経路（電話、電子メールなど）によりＩＴ管理者または第２のコンピュータの他の権限ユーザに接触し、チャレンジを伝える。ＩＴ管理者はチャレンジを第２のコンピュータに入力し、第２のコンピュータは、チャレンジを可逆に（例えばＸＯＲ演算）ランダム文字列Ｓと組み合わせてレスポンスＲを生成し、ランダム文字列Ｓを自身のメモリから削除して再度使用することができないようにする。次いでレスポンスＲが管理者からアウトオブバンド通信経路を通じて第１のコンピュータのユーザに通信され、第１のコンピュータのユーザはレスポンスを第１のコンピュータに入力する。第１のコンピュータはレスポンスＲからランダム文字列Ｓを抽出し、ランダム文字列ＳをＰＲＣの中に展開し、ＰＣＲを使用してボリューム固有の暗号鍵をアンシールする。

【００８３】

第１のコンピュータがクライアントコンピュータ２００である実施形態では、保護されたボリュームへのアクセスの検出、ランダム文字列Ｓの取得、およびＴＰＭアンシール動作の実行に関して上記で説明した機能は、ｐｒｅ－ＯＳ暗号化モジュール２６２または暗号化フィルタドライバ２４６によって行うことができる。例えば、保護されたＯＳボリュームへのアクセスがシステム起動時に試みられる場合はｐｒｅ－ＯＳ暗号化モジュール２６２がそのような機能を行い、一方、保護されたデータボリュームへのアクセスが実行時に試みられる場合は暗号化フィルタドライバ２４６がそれらの機能を行うことができる。ただし、これらは例に過ぎず、クライアントコンピュータ２００内の他のコンポーネントを使用してそれらの機能を行ってもよい。

【００８４】

Ｃ．ＴＰＭおよびサーバの介在を使用する一度限りのロック解除に基づく一度限り使用可能な認証方法

図６Ａおよび図６Ｂに、第１のコンピュータの保護されたボリュームに記憶された暗号化データへのアクセスを制御するための第３の例示的な一度限り使用可能な認証方法のフローチャート６００をまとめて示す。下記の説明で明らかにするように、フローチャート６００の方法は、ＴＰＭおよびサーバの介在を使用する一度限りのロック解除の発想に基づく。フローチャート６００の方法は、項Ｉ．Ｂで説明した個々の攻撃タイプすべてとそれらの攻撃の組み合わせを阻止する。

【００８５】

フローチャート６００の方法では、第１のコンピュータにＴＰＭが存在することが必要となる。先に説明したフローチャート５００の方法と同様に、フローチャート６００の方法は、ＴＰＭのエクステンドおよびシール動作がそれぞれハッシュ化と公開鍵による暗号

化に相当し、したがって、それらの動作はＴＰＭの支援を受けずに別のエンティティによって行えるのに対し、秘密鍵による復号に相当するＴＰＭのアンシール動作はＴＰＭ自体でしか行うことができないことを利用する。ＴＰＭを使用してエクステンド、シールおよびアンシール動作を行う方式は当業者には知られていよう。

【００８６】

図６Ａに示すように、フローチャート６００の方法はステップ６０２で開始し、ステップ６０２では、保護されたボリュームを復号するために必要なボリューム固有の暗号鍵を第２のコンピュータに関連付けられた公開鍵で暗号化することにより、第１のキープロテクタが生成される。実装に応じて、このステップは、適切な配布経路を介して第２のコンピュータから公開鍵を受け取った後に第１のコンピュータが行っても、または第２のコンピュータで行い、その後第２のコンピュータから第１のコンピュータにキープロテクタを送信してもよい。さらに他の方法を使用してこのステップを行うことも可能である。

【００８７】

ステップ６０４で、第１のキープロテクタを第１のコンピュータのローカルメモリに記憶する。例えば、このステップは、保護されたボリュームのボリュームメタデータの一部としてキープロテクタを記憶することからなることができる。

【００８８】

図６Ｂに示すように、ステップ６０４の後に判定ステップ６０６が行われる。判定ステップ６０６では、第１のコンピュータが、保護されたボリュームにアクセスする試みが検出されたかどうかを判定する。保護されたボリュームにアクセスする試みが検出されていない場合は、判定ステップ６０６を繰り返す。保護されたボリュームにアクセスする試みが検出された場合は、制御はステップ６０８に進む。

【００８９】

ステップ６０８で、第１のコンピュータで生成された第１の乱数に基づいて第１のコンピュータが第１のＰＣＲ値を生成し、これをＰＣＲｘと表す。このステップは、例えばＴＰＭのエクステンド動作を行って乱数を第１のコンピュータ上のＴＰＭの特定のＰＣＲに展開することによって行うことができ、特定のＰＣＲは事前にゼロに初期化されている。第１の乱数は第１のコンピュータのローカルメモリに記憶される。

【００９０】

ステップ６１０で、第１のコンピュータがキープロテクタ、第１のＰＣＲ値（ＰＣＲｘ）および第１のＰＣＲ値の認証子を第２のコンピュータに送信する。一実施形態では、第１のＰＣＲ値の認証子は、偽造不可能な署名されたＰＣＲ値のセットからなり、これはＰＣＲｘを含み、第１のコンピュータのＴＰＭのクオート（ｑｕｏｔｅ）機能を使用して生成される。この認証子の提供により、第１のコンピュータがＲＣＲｘの生成に使用された乱数に確実にバインドされる。

【００９１】

ステップ６１２で、第２のコンピュータは、第２のコンピュータの公開鍵に対応する秘密鍵を使用して第１のキープロテクタを復号することにより、ボリューム固有の暗号鍵を取得する。

【００９２】

ステップ６１４で、第２のコンピュータは、第１のＰＣＲ値（ＰＣＲｘ）および第２のコンピュータで生成された第２の乱数の両方に基づいて第２のＰＣＲ値を生成する。一実施では、このステップは、ＴＰＭのエクステンド動作を行って、第２の乱数のハッシュ化バージョンをＰＣＲｘに付加することを伴う。上記のように、第２のコンピュータは、第１のコンピュータのＴＰＭにアクセスすることができなくともＴＰＭのエクステンド動作を行うことができる。第２の乱数は、第２のコンピュータからアクセス可能なメモリに記憶される。

【００９３】

ステップ６１６で、第２のコンピュータは、ＴＰＭのシール動作を行ってボリューム固有の暗号鍵を暗号化し、暗号化されたボリューム固有の暗号鍵を第２のＰＣＲ値にバイン

ドすることにより第２のキープロテクタを生成する。上記のように、第２のコンピュータは、第１のコンピュータのＴＰＭにアクセスすることができなくともＴＰＭのシール動作を行うことができる。

【００９４】

ステップ６１８で、第２のコンピュータは第２のキープロテクタおよび第２の乱数を第１のコンピュータに送信する。

【００９５】

ステップ６２０で、第１のコンピュータは第１のＰＣＲ値および第２の乱数の両方に基づいて第２のＰＣＲ値を生成する。一実施形態では、このステップは、ＴＰＭのエクステンド動作を行って第２の乱数のハッシュ化バージョンをＰＣＲｘに付加することからなる。

【００９６】

ステップ６２２で、第１のコンピュータは、第２のＰＣＲ値を利用するＴＰＭのアンシール動作を第２のキープロテクタに行うことにより、ボリューム固有の暗号鍵を取得する。このＴＰＭアンシール動作は、第１のコンピュータのＴＰＭを使用してしか行うことができない。そして、そのボリューム固有の暗号鍵を使用して、保護されたボリュームの暗号化データを復号することができる。一実施形態では、ボリューム固有の暗号鍵は、第１のボリューム固有の暗号鍵（例えばＶＭＫ）からなり、その暗号鍵を使用して第２のボリューム固有の暗号鍵（例えばＦＶＥＫ）を復号することができ、その第２のボリューム固有の暗号鍵を使用して保護されたボリュームの個々のセクタを復号することができる。

【００９７】

ステップ６２４で、第１のコンピュータは、第１のコンピュータのローカルメモリから第１の乱数および第２の乱数を削除し、第２のコンピュータは、第２のコンピュータからアクセス可能なメモリから第２の乱数を削除する。このようにして第１の乱数および第２の乱数を削除することにより、ボリューム固有の暗号鍵をアンシールするために必要なＰＣＲ値を再作成することができなくなる。

【００９８】

前述のフローチャート６００の方法は、それ単独では、第１のコンピュータにある認証コードが改ざんされていないという保証は提供しない。そのような保証が望まれる場合は、以下のようなこの方法の拡張を使用することができる。

【００９９】

第１のコンピュータのシステム起動時に、第１のコンピュータにある認証コードを計測してＴＰＭのＰＣＲに書き込む（ｍｅａｓｕｒｅ）。このＰＣＲ値をＰＣＲｙと呼ぶ。ステップ６０８で、第１のコンピュータで生成された乱数を計測してＴＰＭの別のＰＣＲに書き込むことにより、上記のように値ＰＣＲｘが生成される。

【０１００】

ステップ６１０で、第１のコンピュータはキープロテクタ、ＰＣＲｘ、ＰＣＲｙ、およびＰＣＲｘとＰＣＲｙの認証子を第２のコンピュータに送信する。一実施形態では、ＰＣＲｘおよびＰＣＲｙの認証子は、偽造不可能な署名されたＰＣＲ値のセットからなり、これはＰＣＲｘおよびＰＣＲｙを含み、第１のコンピュータのＴＰＭのクオート機能を使用して生成される。

【０１０１】

第２のコンピュータは、ＰＣＲｙを既知の合格値のデータベースと比較するか、または事前に第１のコンピュータから取得した信頼される値と比較することにより、ＰＣＲｙを検証する。この検証が不合格の場合、第２のコンピュータは認証要求を拒否する。

【０１０２】

一方、検証が合格の場合は、ステップ６１４で、第２のコンピュータが、第１のＰＣＲ値（ＰＣＲｘ）および上記の要領で第２のコンピュータで生成された第２の乱数の両方に基づいて第２のＰＣＲ値を生成する。そして、ステップ６１６で、第２のコンピュータが、ＴＰＭのシール動作を行ってボリューム固有の暗号鍵を暗号化し、暗号化されたボリュ

ーム固有の暗号鍵を第２のＰＣＲ値およびＰＣＲｙにバインドすることにより第２のキープロテクタを生成する。

【０１０３】

ステップ６２２で、第１のコンピュータが、第２のＰＣＲ値およびＰＣＲｙを利用するＴＰＭアンシール動作を第２のキープロテクタに行うことによりボリューム固有の暗号鍵を取得する。

【０１０４】

前述の説明では、第１のコンピュータにある認証コードを計測して、ＰＣＲｙと呼ばれる、ＴＰＭの１つのＰＣＲに書き込むと述べた。しかし、この方法は、認証コードを計測してＴＰＭの複数個のＰＣＲに書き込むように一般化することができる。複数のＰＣＲを第２のコンピュータに送信し、検証し、使用して、上記で１つのＰＣＲ値ＰＣＲｙを参照して説明したのと同様にして第２のキープロテクタを生成することができる。

【０１０５】

第１のコンピュータがクライアントコンピュータ２００である実施形態では、保護されたボリュームへのアクセスの検出、第１のキープロテクタの生成と第２のコンピュータへの送信、第２のキープロテクタの取得とアンシール、および第１のコンピュータのローカルメモリからの乱数の削除に関連して上記で述べた機能は、ｐｒｅ－ＯＳ暗号化モジュール２６２または暗号化フィルタドライバ２４６によって行うことができる。例えば、保護されたＯＳボリュームへのアクセスがシステム起動時に試みられる場合は、ｐｒｅ－ＯＳ暗号化モジュール２６２がそのような機能を行い、保護されたデータボリュームへのアクセスが実行時に試みられる場合は暗号化フィルタドライバ２４６がそれらの機能を行うことができる。ただし、これは例に過ぎず、クライアントコンピュータ２００内の他のコンポーネントを使用してこれらの機能を行ってもよい。

【０１０６】

Ｄ．ＴＰＭの委任を使用する一度限りのロック解除に基づく一度限り使用可能な認証方法

図７Ａおよび図７Ｂに、第１のコンピュータの保護されたボリュームに記憶された暗号化データへのアクセスを制御するための第４の例示的な一度限り使用可能な認証方法のフローチャート７００をまとめて示す。下記の説明で明らかにするように、フローチャート７００の方法は、ＴＰＭの委任を使用する一度限りのロック解除の発想に基づく。ＴＰＭの委任、および本明細書でＴＰＭ委任に関連して記載する機能、動作および性質は当業者に知られていよう。フローチャート７００の方法は、上記のＩ．Ｂの項で説明したリプレー攻撃のタイプに強い。

【０１０７】

図７Ａに示すように、フローチャート７００の方法はステップ７０２で開始し、ステップ７０２では、第１のコンピュータが、保護されたボリュームを復号するために必要とされるボリューム固有の暗号鍵を、第１のコンピュータのＴＰＭから提供される移動不可能な暗号鍵で暗号化することによりキープロテクタを生成する。特定の実装では、移動不可能な暗号鍵は、秘密使用権限（ｕｓａｇｅＡｕｔｈ）を有し、これもボリューム固有の暗号鍵である。

【０１０８】

ステップ７０４で、第１のコンピュータは、ＴＰＭに移動不可能な暗号鍵の鍵委任エントリを生成し、鍵委任エントリは、単調増加のみが可能な、エントリに関連付けられた検証カウンタを有する。

【０１０９】

ステップ７０６で、第１のコンピュータは、第１のコンピュータで生成された乱数Ｘおよび検証カウンタの現在の値に基づいて使い捨ての認証文字列を生成する。使い捨ての認証文字列は、ＨＭＡＣ（検証用カウント値Ｘ）と定義することができるＨＭＡＣ演算を行うことによって生成することができる。当業者には理解されるように、ＨＭＡＣ演算は、ＴＰＭで行うことができる鍵付きハッシュを利用するメッセージ認証コード（ＭＡＣ）演算である。

【０１１０】
ステップ７０８で、第１のコンピュータは、乱数Ｘをその識別子と共に第２のコンピュータにセキュアに送信し、第２のコンピュータからアクセス可能なメモリに記憶させる。
【０１１１】
ステップ７１０で、第１のコンピュータが、使用権限（ｕｓａｇｅＡｕｔｈ）が使い捨ての認証文字列に設定された鍵委任ブラブ（ｂｌｏｂ）をＴＰＭ内に生成する。
【０１１２】
ステップ７１２で、第１のコンピュータは、キープロテクタ、乱数識別子、および鍵委任ブラブをローカルメモリに（例えば保護されたボリュームのボリュームメタデータに）記憶し、同時に第１のコンピュータのローカルメモリから使い捨ての認証文字列を削除する。第１のコンピュータは、乱数Ｘをボリューム固有の暗号鍵で暗号化し、暗号化した乱数をその一意の識別子と共にローカルメモリに記憶することもできる。
【０１１３】
図７Ｂに示すように、ステップ７１２の後に判定ステップ７１４が行われる。判定ステップ７１４で、第１のコンピュータが、保護されたボリュームにアクセスする試みが検出されたかどうかを判定する。保護されたボリュームにアクセスする試みが検出されていない場合は、判定ステップ７１４を繰り返す。保護されたボリュームにアクセスする試みが検出されている場合は、制御はステップ７１６に進む。
【０１１４】
ステップ７１６で、第１のコンピュータは、検証カウンタの現在の値と乱数識別子を第２のコンピュータに送信する。ステップ７１８で、第２のコンピュータは、乱数識別子を使用して、第２のコンピュータからアクセス可能なメモリから乱数を取得する。
【０１１５】
ステップ７２０で、第２のコンピュータは、取得した乱数と検証カウンタの現在の値に基づいて使い捨ての認証文字列を生成し、ステップ７２２で、第２のコンピュータは使い捨ての認証文字列を第１のコンピュータに送信する。
【０１１６】
ステップ７２４で、第１のコンピュータは、使い捨ての認証文字列を使用してキープロテクタを復号することによりボリューム固有の暗号鍵を取得する。詳細には、このステップは、まず使い捨ての認証文字列を使用して移動不可能な鍵をロック解除し、次いでその移動不可能な鍵を使用してキープロテクタを復号することを伴う。そして、ボリューム固有の暗号鍵を使用して、保護されたボリュームの暗号化データを復号することができる。一実施形態では、ボリューム固有の暗号鍵は第１のボリューム固有の暗号鍵（例えばＶＭＫ）からなり、その暗号鍵を使用して第２のボリューム固有の暗号鍵（例えばＦＶＥＫ）を復号することができ、その第２のボリューム固有の暗号鍵を使用して保護されたボリュームの個々のセクタを復号することができる。ボリューム固有の暗号鍵が第１のコンピュータからアクセスできるようになるため、第１のコンピュータは、このステップで乱数Ｘの暗号化バージョンを復号することもできることに留意されたい。
【０１１７】
ステップ７２６で、第１のコンピュータは、第１のコンピュータによる検証カウンタを増分し、それにより委任ブラブを無効化する。これにより、その使い捨ての認証文字列を使用して、キープロテクタを復号するために必要な移動不可能な鍵をロック解除できなくなることが保証される。ステップ７２６は、保護されたボリュームが実際に復号される前に行わなければならないことに留意されたい。
【０１１８】
ステップ７２６の後、第１のコンピュータは、乱数Ｘ（ステップ７２４で復号されている）と新しい検証用カウント値を使用して、第２のコンピュータに送信する新しい使い捨ての認証文字列と新しい鍵委任ブラブを生成し、それにより認証機構を再整備することができる。この手法により、乱数Ｘは一度のみ第２のコンピュータに通信すればよいことが保証され、それにより、乱数が潜在的な攻撃者にさらされることを抑制する。代替実施形

態では、認証機構が再整備されるたびに第１のコンピュータで新しい乱数を生成できることに留意されたい。

【０１１９】

第２のコンピュータは、複数の連続した検証カウント値のための使い捨ての認証文字列を事前に要求する、または、所与の識別子による要求の回数や順序外れの要求を制限する、または、すべての要求をログに記録、監視し、同じ識別子が２度使われた場合は警告を発する等により、追加的な保護を得ることができる。また、第２のコンピュータは、操作者不在の再起動が予想される計画された保全期間外は利用できないようにしてもよい。

【０１２０】

第１のコンピュータがクライアントコンピュータ２００である実施形態では、保護されたボリュームへのアクセスの検出、第２のコンピュータへの検証カウンタの現在の値と乱数識別子の送信、ボリューム固有の暗号鍵の取得、および検証カウンタの増分に関連して上記で述べた機能は、ｐｒｅ－ＯＳ暗号化モジュール２６２または暗号化フィルタドライバ２４６によって行うことができる。例えば、保護されたＯＳボリュームへのアクセスがシステム起動時に試みられる場合は、ｐｒｅ－ＯＳ暗号化モジュール２６２がそのような機能を行い、保護されたデータボリュームへのアクセスが実行時に試みられる場合は暗号化フィルタドライバ２４６がそれらの機能を行うことができる。ただし、これは例に過ぎず、クライアントコンピュータ２００内の他のコンポーネントを使用してこれらの機能を行ってもよい。

【０１２１】

ＩＩＩ．例示的なコンピュータシステムの実施

図８に、本明細書に記載される各種の実施形態を実施するために使用できる例示的なコンピュータシステム８００を示す。例えば、コンピュータシステム８００を使用して、図１のクライアントコンピュータ104_1～104_N、サーバ１０６、または管理者コンピュータ１０８、または図２のクライアントコンピュータ２００を実施することができる。同様に、上記で図３、４、５、６Ａ、６Ｂ、７Ａ、および７Ｂを参照したフローチャート３００、４００、５００、６００、または７００を参照して説明した第１のコンピュータまたは第２のコンピュータに備わるとした機能も、コンピュータシステム８００を使用して行うことができる。

【０１２２】

コンピュータシステム８００は、例えば従来のパーソナルコンピュータ、モバイルコンピュータ、またはワークステーションの形態の汎用コンピューティング装置であるか、またはコンピュータシステム８００は特殊目的のコンピューティング装置であってもよい。本明細書に提供するコンピュータシステム８００の記述は説明のために提供され、制限的なものではない。当業者に知られるように、実施形態はさらに別の種類のコンピュータシステムで実施することも可能である。

【０１２３】

図８に示すように、コンピュータシステム８００は、処理装置８０２、システムメモリ８０４、およびシステムメモリ８０４を含む各種のシステムコンポーネントを処理装置８０２に結合するバス８０６を含む。処理装置８０２は、１つまたは複数のプロセッサまたは処理コアを備えることができる。プロセッサ８０６は、数種のプロセッサ構造の１つまたは複数に相当し、それらの種類には、メモリプロセッサまたはメモリコントローラ、ペリフェラルバス、アクセラレーテッドグラフィクスポート、および各種のバスアーキテクチャを使用したプロセッサバスまたはローカルバスが含まれる。システムメモリ８０４は、ＲＯＭ（読出し専用メモリ）８０８およびＲＡＭ（ランダムアクセスメモリ）８１０を含む。基本入出力システム８１２（ＢＩＯＳ）がＲＯＭ８０８に記憶される。

【０１２４】

コンピュータシステム８００は、以下のドライブの１つまたは複数も有する。ハードディスクの読み書きを行うためのハードディスクドライブ８１４、取り外し可能磁気ディスク８１８の読み書きを行うための磁気ディスクドライブ８１６、および、ＣＤ　ＲＯＭ、

ＤＶＤ　ＲＯＭ、または他の光学媒体などの取り外し可能光学ディスク８２２の読み書きを行うための光学ディスクドライブ８２０。ハードディスクドライブ８１４、磁気ディスクドライブ８１６、および光学ディスクドライブ８２０は、それぞれハードディスクドライブインタフェース８２４、磁気ディスクドライブインタフェース８２６、光学ドライブインタフェース８２８によりバス８０６に接続される。これらのドライブとそれに関連するコンピュータ可読媒体は、コンピュータのコンピュータ可読命令、データ構造、プログラムモジュール、および他のデータの不揮発性の記憶を提供する。ハードディスク、取り外し可能磁気ディスクおよび取り外し可能光学ディスクを記載するが、データの記憶には他の種類のコンピュータ可読媒体も使用することができ、それらには、フラッシュメモリカード、デジタルビデオディスク、ランダムアクセスメモリ（ＲＡＭ）、読出し専用メモリ（ＲＯＭ）等がある。

【０１２５】

ハードディスク、磁気ディスク、光ディスク、ＲＯＭ、またはＲＡＭには、複数のプログラムモジュールを記憶することができる。それらのプログラムには、オペレーティングシステム８３０、１つまたは複数のアプリケーションプログラム８３２、他のプログラムモジュール８３４、およびプログラムデータ８３６が含まれる。これらのプログラムは、実行されると、コンピュータシステム８００に、上記で図３、４、５、６Ａ、６Ｂ、７Ａ、および７Ｂを参照したフローチャート３００、４００、５００、６００、または７００を参照して説明した、第１のコンピュータまたは第２のコンピュータに備わる機能を行わせる。

【０１２６】

ユーザは、キーボード８３８やポインティングデバイス８４０等の入力装置を通じてコンピュータシステム８００にコマンドと情報を入力することができる。他の入力装置（図示せず）には、マイクロフォン、ジョイスティック、ゲームコントローラ、スキャナ等がある。一実施形態では、ディスプレイ８４４と併せてマルチタッチ可能なタッチスクリーンを提供して、ユーザがタッチスクリーン上の１つまたは複数の点への接触（例えば指やスタイラスで）の適用を通じてユーザ入力を行えるようにする。上記および他の入力装置は、多くの場合、バス８０６に結合されたシリアルポートインタフェース８４２を通じて処理装置８０２に接続されるが、パラレルポート、ゲームポート、またはユニバーサルシリアルバス（ＵＳＢ）等の他のインタフェースで接続してもよい。

【０１２７】

ディスプレイ８４４も、ビデオアダプタ８４６などのインタフェースを介してバス８０６に接続される。ディスプレイの他に、コンピュータシステム８００は、スピーカやプリンタなどの他の周辺出力装置（図示せず）も含むことができる。

【０１２８】

コンピュータシステム８００は、ネットワークインタフェースもしくはアダプタ８５０、モデム８５２、またはネットワークを通じて通信を確立するための他の手段を通じて、ネットワーク８４８（例えばローカルエリアネットワークや、インターネットなどのワイドエリアネットワーク）に接続される。モデム８５２は内蔵型の場合も外付けの場合もあり、シリアルポートインタフェース８４２を介してバス８０６に接続される。

【０１２９】

本明細書で使用する用語「コンピュータプログラム媒体」および「コンピュータ可読媒体」は、一般に、ハードディスクドライブ８１４に関連するハードディスク、取り外し可能磁気ディスク８１８、取り外し可能光ディスク８２２等の非一時的媒体、ならびに、フラッシュメモリカード、デジタルビデオディスク、ＲＡＭ（ランダムアクセスメモリ）、ＲＯＭ（読出し専用メモリ）等の他種の媒体を意味するものとして使用する。

【０１３０】

上記のように、コンピュータプログラムおよびモジュール（アプリケーションプログラム８３２および他のプログラムモジュール８３４を含む）は、ハードディスク、磁気ディスク、光ディスク、ＲＯＭ、またはＲＡＭに記憶することができる。それらのコンピュー

タプログラムは、ネットワークインタフェース８５０またはシリアルポートインタフェース８４２を介して受け取ることもできる。それらのコンピュータプログラムは、アプリケーションによって実行またはロードされると、コンピュータ８００に本明細書に述べる実施形態の機能を実施させる。したがって、そのようなコンピュータプログラムは、コンピュータシステム８００のコントローラに相当する。

【０１３１】

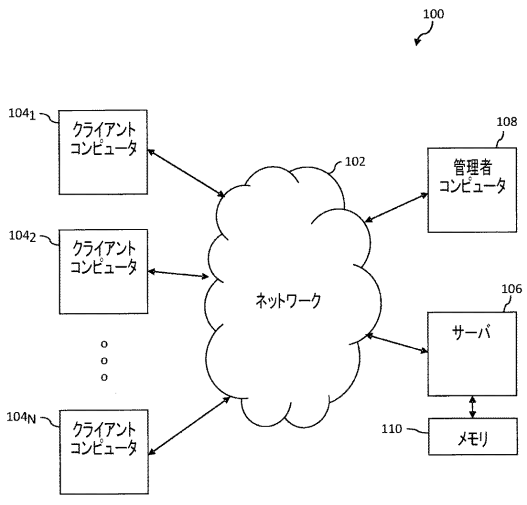
実施形態は、任意のコンピュータ可読媒体に記憶されたソフトウェアを含むコンピュータプログラム製品も対象とする。そのようなソフトウェアは、１つまたは複数のデータ処理装置で実行されると、データ処理装置を本明細書に記載されるように動作させる。実施形態は、現在または今後知られる、任意のコンピュータによる使用が可能な媒体またはコンピュータ可読媒体を用いることができる。コンピュータ可読媒体の例には、これらに限定されないが、ＲＡＭ、ハードドライブ、フロッピー（登録商標）ディスク、ＣＤ　ＲＯＭ、ＤＶＤ　ＲＯＭ、ｚｉｐディスク、テープ、磁気記憶装置、光学記憶装置、ＭＥＭＳを利用した記憶装置、ナノ技術を利用した記憶装置などの記憶装置が含まれる。

【０１３２】

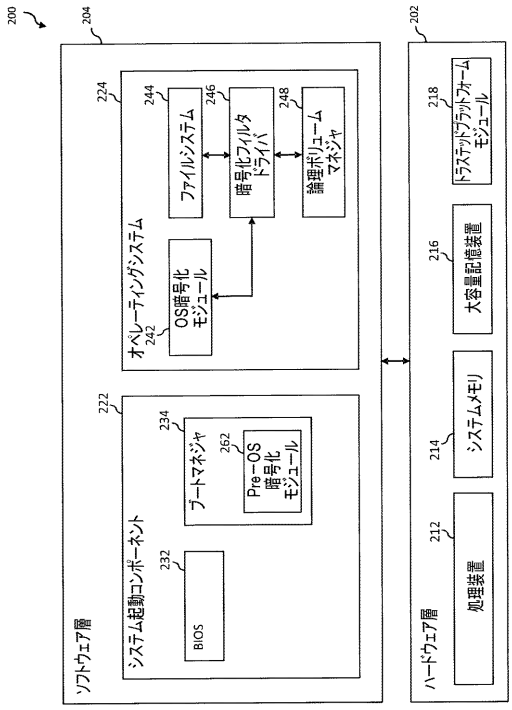
ＩＶ．結び

上記で各種実施形態を説明したが、それらは単なる例として提示したものであり、制限ではないことを理解されたい。当業者には、本発明の主旨から逸脱しない範囲内で形態および詳細への各種変更を行うことが可能であることが明らかであろう。したがって、本発明の範囲は上記の例示的実施形態によっては制限されず、特許請求の範囲およびその均等物に従ってのみ定義すべきである。

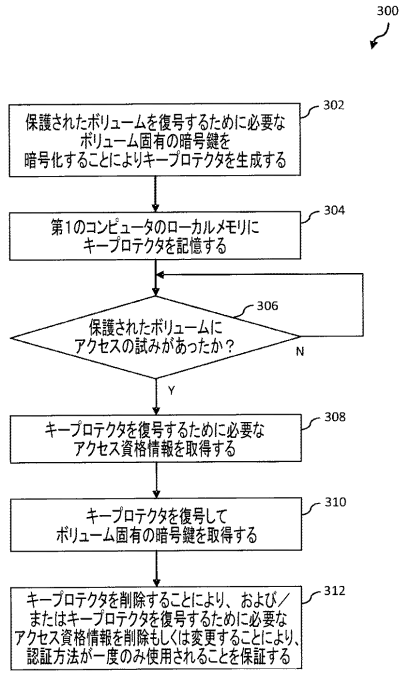
【図１】



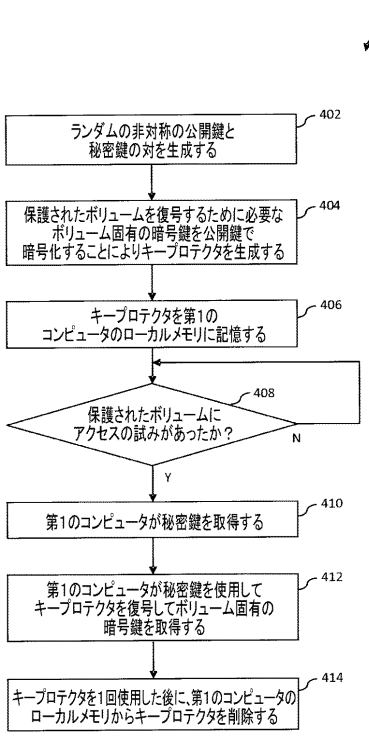
【図２】



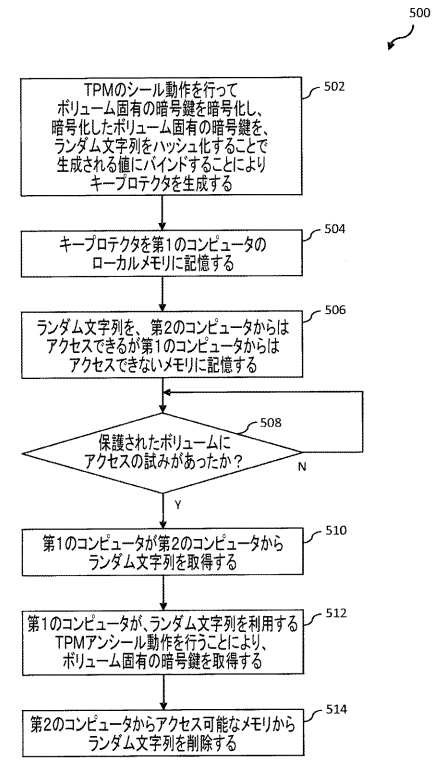
【図３】


300
保護されたボリュームを復号するために必要な
ボリューム固有の暗号鍵を
暗号化することによりキープロテクタを生成する
302
第1のコンピュータのローカルメモリに
キープロテクタを記憶する
304
保護されたボリュームに
アクセスの試みがあったか？
306
N
Y
キープロテクタを復号するために必要な
アクセス資格情報を取得する
308
キープロテクタを復号して
ボリューム固有の暗号鍵を取得する
310
キープロテクタを削除することにより、および／
またはキープロテクタを復号するために必要な
アクセス資格情報を削除もしくは変更することにより、
認証方法が一度のみ使用されることを保証する
312

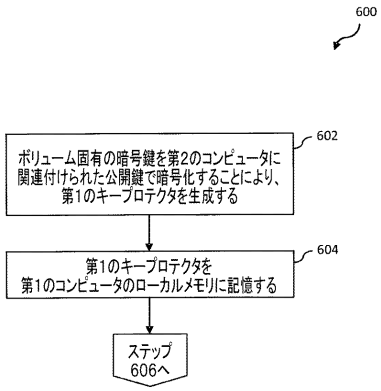
【図４】


400
ランダムの非対称の公開鍵と
秘密鍵の対を生成する
402
保護されたボリュームを復号するために必要な
ボリューム固有の暗号鍵を公開鍵で
暗号化することによりキープロテクタを生成する
404
キープロテクタを第1の
コンピュータのローカルメモリに記憶する
406
保護されたボリュームに
アクセスの試みがあったか？
408
N
Y
第1のコンピュータが秘密鍵を取得する
410
第1のコンピュータが秘密鍵を使用して
キープロテクタを復号してボリューム固有の
暗号鍵を取得する
412
キープロテクタを1回使用した後に、第1のコンピュータの
ローカルメモリからキープロテクタを削除する
414

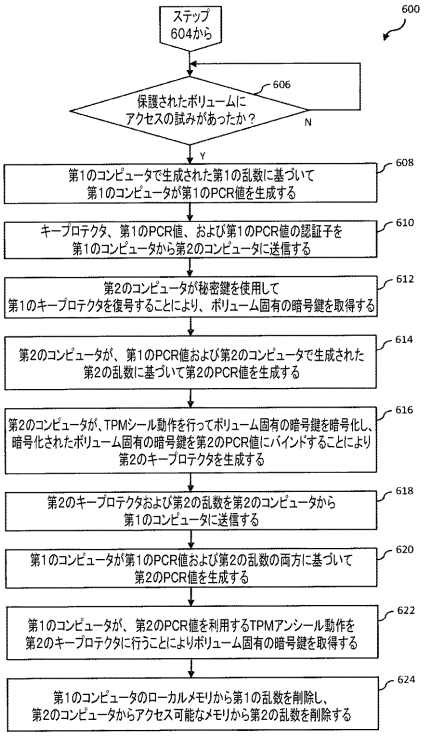
【図５】


500
TPMのシール動作を行って
ボリューム固有の暗号鍵を暗号化し、
暗号化したボリューム固有の暗号鍵を、
ランダム文字列をハッシュ化することで
生成される値にバインドすることにより
キープロテクタを生成する
502
キープロテクタを第1のコンピュータの
ローカルメモリに記憶する
504
ランダム文字列を、第2のコンピュータからは
アクセスできるが第1のコンピュータからは
アクセスできないメモリに記憶する
506
保護されたボリュームに
アクセスの試みがあったか？
508
N
Y
第1のコンピュータが第2のコンピュータから
ランダム文字列を取得する
510
第1のコンピュータが、ランダム文字列を利用する
TPMアンシール動作を行うことにより、
ボリューム固有の暗号鍵を取得する
512
第2のコンピュータからアクセス可能なメモリから
ランダム文字列を削除する
514

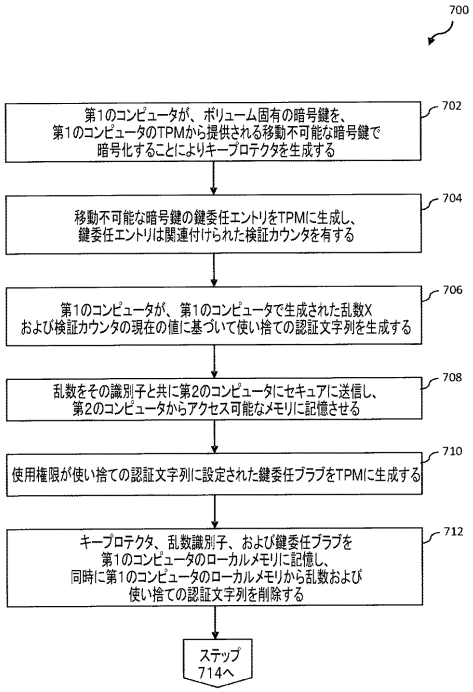
【図６Ａ】


600
ボリューム固有の暗号鍵を第2のコンピュータに
関連付けられた公開鍵で暗号化することにより、
第1のキープロテクタを生成する
602
第1のキープロテクタを
第1のコンピュータのローカルメモリに記憶する
604
ステップ
606へ

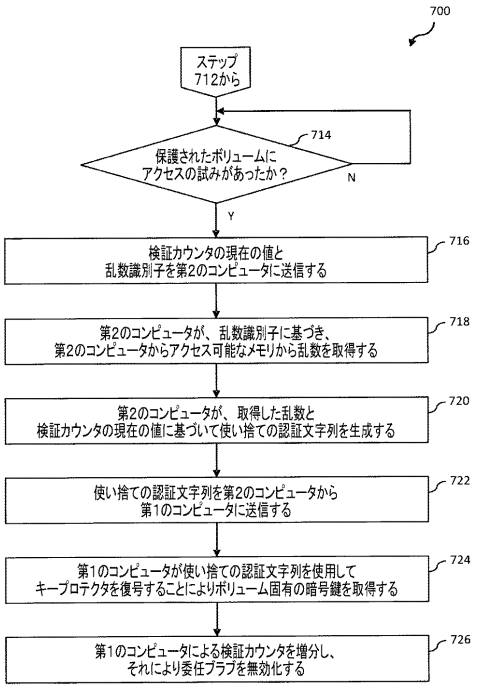
【図６Ｂ】



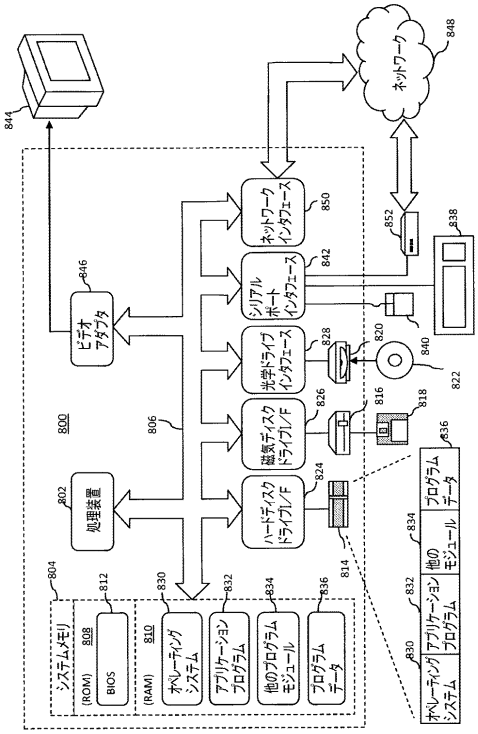
【図７Ａ】



【図７Ｂ】



【図８】



フロントページの続き

(72)発明者 オクタビアン ティー．ウレケ
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ内
(72)発明者 ニルス デュサール
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ内
(72)発明者 チャールズ ジー．ジェフリーズ
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ内
(72)発明者 クリスティアン エム．アイラック
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ内
(72)発明者 ビジャ ジー．バラドワジ
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ内
(72)発明者 インノケンティー バスモブ
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ内
(72)発明者 ステファン トム
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ内
(72)発明者 ソン ヴォバ
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ内

審査官 打出 義尚

(56)参考文献 特開２００９－００４９０１（ＪＰ，Ａ）
米国特許出願公開第２００７／０３０００８０（ＵＳ，Ａ１）
米国特許出願公開第２００５／０２４６７７８（ＵＳ，Ａ１）
PGP(R) Desktop:Enterprise Whole Disk Encryption Only Edition - Security Target, ２０１０年 3月３０日, Version 1.0, pp. 6-8, 21-23, 57-58, 62-63, ＵＲＬ, https://www.commoncriteriaportal.org/files/epfiles/pgp-desktop-v9100-sec-eng.pdf

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／０８
Ｈ０４Ｌ ９／３２