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

特許第5596029号
(P5596029)

(45)発行日　平成26年9月24日(2014.9.24)　(24)登録日　平成26年8月15日(2014.8.15)

(51)Int.Cl.		F I		
G06F 21/62	(2013.01)	G06F	21/24	165C
G06F 21/45	(2013.01)	G06F	21/20	145
G06K 17/00	(2006.01)	G06K	17/00	S
G06K 19/10	(2006.01)	G06K	19/00	R

請求項の数 11　(全 20 頁)

(21)出願番号	特願2011-516375 (P2011-516375)
(86)(22)出願日	平成21年5月20日 (2009.5.20)
(65)公表番号	特表2011-526028 (P2011-526028A)
(43)公表日	平成23年9月29日 (2011.9.29)
(86)国際出願番号	PCT/US2009/044655
(87)国際公開番号	WO2009/158082
(87)国際公開日	平成21年12月30日 (2009.12.30)
審査請求日	平成24年4月9日 (2012.4.9)
(31)優先権主張番号	12/146,066
(32)優先日	平成20年6月25日 (2008.6.25)
(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　100153028
弁理士　上田　忠

最終頁に続く

(54)【発明の名称】多重認証サイロを用いた一時記憶装置用認証方法

(57)【特許請求の範囲】

【請求項１】

計算機実行可能命令をストアする計算機可読記憶媒体であって、前記命令が、

1つ以上の認証サイロの組み合わせを含む論理式を生成するために、記憶装置上の記憶領域に対応した認証サイロそれぞれに関する認証要件を調整するステップであって、前記論理式が、少なくとも製造者証明書又はプロビジョニング証明書の内の１つの拡張フィールド内の、１つ以上の認証サイロに対する構成設定に基礎をおくものと、

前記認証サイロそれぞれの認証状態が、前記記憶領域に対するアクセスに対し、前記論理式の有効な認証サイロの組み合わせの結果をもたらすか否か決定するステップと、

前記決定に基づいてホスト機器による前記記憶領域に対するアクセスを認可するステップと、

を含む方法を計算機に実行させることを特徴とする、記憶媒体。

【請求項２】

前記記憶領域に対応した前記認証サイロを生成する生成動作が、

認証証明書の拡張フィールドに前記記憶領域の構成可能な設定に関する値を設定するステップと、

前記記憶装置に前記認証証明書をインストールするステップと、を含むことを特徴とする請求項１記載の記憶媒体。

【請求項３】

前記調整するステップが、前記認証サイロそれぞれの認証を試みるための予め決定され

たシーケンスを指定するステップを含むことを特徴とする請求項１記載の記憶媒体。
【請求項４】
前記調整するステップが、
前記認証サイロの少なくとも１つの認証がユーザー入力を利用するか否か決定するステップと、
認証要件を満たすユーザー入力を求めるステップと、を含むことを特徴とする請求項１記載の記憶媒体。
【請求項５】
前記調整するステップが、前記認証サイロそれぞれ及び前記論理式を発見するために、認証証明書に問い合わせを行うステップを含むことを特徴とする請求項１記載の記憶媒体。
【請求項６】
前記調整するステップが、
前記認証サイロそれぞれの認証状態の組合せが、前記論理式内の認証サイロの組み合わせによって特定されているか否か発見するステップを含んでいて、
前記決定するステップが、前記組合せが満足するか否か計算するステップを含むことを特徴とする請求項１記載の記憶媒体。
【請求項７】
前記計算するステップが、前記認証サイロそれぞれの前記認証状態のＭａｘＴｅｒｍ／ＭｉｎＴｅｒｍ値を計算するステップを含むことを特徴とする請求項６記載の記憶媒体。
【請求項８】
プロセッサーと、
記憶領域を有するメモリー記憶ボリュームと、
前記記憶領域に対応した１つ以上の認証サイロを定義する前記記憶領域に関連付けられる認証証明書と、
前記プロセッサー上で実行するファームウェアアプリケーションであって、
1つ以上の認証サイロの組み合わせを含む論理式を生成するために、前記記憶領域に対応した認証サイロそれぞれに対する認証要件を調整し、前記論理式が、少なくとも製造者証明書又はプロビジョニング証明書の内の１つの拡張フィールド内の、１つ以上の認証サイロに対する構成設定に基礎をおくものと、
前記認証サイロの認証状態が、前記記憶領域に対するアクセスに対し、前記論理式の有効な認証サイロの組み合わせの結果をもたらすか否か決定し、
前記決定に基づいてホスト機器による前記記憶領域に対するアクセスを認可するように記憶装置を構成するものと、を含む記憶装置。
【請求項９】
前記ファームウェアアプリケーションが、前記認証サイロそれぞれの認証を試みるための予め決定されたシーケンスを指定するように前記記憶装置を構成することを特徴とする請求項８記載の記憶装置。
【請求項１０】
前記ファームウェアアプリケーションが、
前記認証サイロの少なくとも１つの認証がユーザー入力を利用するか否か決定し、
認証条件を満たすユーザー入力を求めるように前記記憶装置を構成することを特徴とする請求項８記載の記憶装置。
【請求項１１】
前記ファームウェアアプリケーションが、
前記認証サイロそれぞれの認証状態の組合せが、前記論理式内の認証サイロの組み合わせによって特定されているか否か発見し、
前記組合せが満足するか否か計算するように前記記憶装置を構成することを特徴とする請求項８記載の記憶装置。
【発明の詳細な説明】

【技術分野】
【０００１】
本発明は、計算機システムにおける認証に関し、具体的には、一時記憶装置用の認証方法に関する。
【背景技術】
【０００２】
[0001]ポータブルコンピューターデータストレージ用に一時記憶装置（ＴＳＤ）が、近年、広く利用されるようになってきた。ＴＳＤは、携帯電話、デジタルカメラ、携帯情報端末、デジタルミュージックプレーヤー（例えばＭＰ３プレーヤー）、及びその他の携帯機器用のユニバーサルシリアルバス（ＵＳＢ）フラッシュドライブ、及びメモリーカード、及び「スティック」形式を取り得る。大規模な記憶容量かつＴＳＤに入出力する高速データ転送のため、ＴＳＤが接続され得るホスト機器を入出力するデータ転送に関するセキュリティは、認識されている懸案事項である。ＴＳＤに関する米国電気電子技術者学会（ＩＥＥＥ）標準規格１６６７は、認証証明書をストアするための認証データ構造（「サイロ」）定義及びＴＳＤ上のユーザーデータに対するその後のアクセス認可を含むことによってこの懸案事項に対処している。
【０００３】
[0002]ＩＥＥＥ標準規格１６６７は、機器が、多重認証サイロを有することを認めていて、これ等をもとに、ＴＳＤ記憶ボリューム上の単一データ記憶領域（「アドレス可能コマンドターゲット」又はＡＣＴ）に対するアクセスの認可を統制する。しかしながら、この標準規格は、現在、証明書用に対し一タイプの認証サイロを定義しているに過ぎず、その他どんなタイプの認証サイロが使用され得るか提示していない。この標準規格は、１つのＡＣＴに対して複数の認証サイロが存在する状況又は異なる利用環境状況に対し、どの認証サイロを使用すべきかに関するどんな方向性も提供していない。更に、この標準規格は、複数のサイロと共に利用するための一般的な認証構成機構を欠いている。仕様が証明書サイロによって実装されるときの限定した一連の認証及び証明書ストア管理動作を提供しているので現在のＩＥＥＥ標準規格１６６７の制約範囲内でのサイロ階層及び構成の実装は複雑である。しかしながら、どんな構成解決法でも現在のＩＥＥＥ標準規格１６６７のパラメーター及び要件仕様の範囲内で作動する必要がある。
【先行技術文献】
【非特許文献】
【０００４】
【非特許文献１】ＩＥＥＥ標準規格１６６７
【発明の概要】
【発明が解決しようとする課題】
【０００５】
本発明の目的は、一時記憶装置と接続するホスト計算装置が、認証データ構造内の様々なタイプの認証情報を発見し、その一時記憶装置上で作用するように構成される認証方法を提供することである。
【課題を解決するための手段】
【０００６】
[0003]多重認証サイロを有するＴＳＤ装置において、ＴＳＤに接続したホスト計算装置が、サイロ内の様々なタイプの認証情報を発見し、その上で作用するように構成される。ＡＣＴに対するアクセスを許可するためには、認証サイロの１つ以上の論理組合せが認証状態に切り換えられる必要がある。ホストは、ＴＳＤに対するホストのアクセスを認可し得る認証サイロの一連の論理組合せに関しＴＳＤに問い合わせを行う。認証サイロの有効な組合せを達成するために認証サイロの具体的順序付も要求され得る。順序付は、ＴＳＤ内の設定情報によって提示され得る。順序付は、例えば、特定の認証サイロを認証するためのユーザー入力が要求されるか否か、ＴＳＤの利用環境、又は最も信頼される認証サイロから最も信頼されない認証サイロへの階層構造にも基づき得る。

【０００７】
[0004]この情報を用いて、ホストは、その後、ＡＣＴに対するアクセス許可をもたらすために最も効率的な認証シーケンスを用いて進め得る。追加するとホストは自らの挙動を最適化し得、例えば、可能であれば、ユーザープロンプトを介して（ユーザー入力のない）静かな認証を支援する。ホストは、以前の組合せが失敗したとき、代替の認証サイロ組合せも試み得る。更に、ホストは、認証の組合せすべてが使い果たされ、認可が不可能なときを、この情報を利用して決定し得る。
【０００８】
[0005] 現在のＩＥＥＥ標準規格１６６７の制約内で作動すると同時にＴＳＤの特定のＡＣＴに対するアクセスに対する認証要件を提供するためにＴＳＤの認証サイロ内の製造者証明書及び／又はプロビジョニング証明書拡張内のフィールドが使用される。一実装において、構成可能なＴＳＤ設定に関する値が、製造者証明書及び／又はプロビジョニング証明書拡張のフィールドに設定される。本方法は、固有の方法でＩＥＥＥ１６６７証明書サイロ仕様書及びＩＴＵ－Ｔ　Ｘ．５０９証明仕様に対する固有の特性を活用する。本方法は、機器構成に関するセキュリティ要件を満たすと同時に、既存の標準規格定義を修正せずにそのまま活用し実装される。とりわけ、本方法は、ＴＳＤファームウェア内の特定の機能を利用可能にし得るか又は利用不可にし得る。
【０００９】
[0006]この明細書に関する用語「一時記憶装置」及び「ＴＳＤ」は、ＩＥＥＥ標準規格１６６７が適用される任意の装置、並びに拡張フィールドをサポートする製造者証明書と同等物及び／又はプロビジョニング証明書と同等なものを許容し得る任意の記憶装置、例えば、アドバンスト・テクノロジー・アタッチメント（ＡＴＡ）機器を包含している。
【００１０】
[0007]この「課題を解決するための手段」は、「発明を実施するための形態」において、更に後述される概念のいくつかを簡易化した形式で紹介するために提供される。この「課題を解決するための手段」は、請求対象項目の重要な機能も本質的な特徴も特定するように意図されておらず、請求対象項目の範囲を限定するように利用されることも意図されていない。請求対象項目の別の特徴、詳細、ユーティリティ、利点は、更に、添付図面に例示し、添付した請求項に定義されているような様々な実施形態及び実装に関し、より具体的に後述される「発明を実施するための形態」から明らかになろう。
【図面の簡単な説明】
【００１１】
【図１】[0008]一時記憶装置のいくつかのプロトコルレイヤの概略図であって、一時記憶装置のあり得る構成の一実装を示している。
【図２】[0009]一時記憶装置の認証サイロ、及び製造者の拡張フィールド又はプロビジョニング証明書を使用し、一時記憶装置を構成する実装の概略図である。
【図３Ａ】[0010]一時記憶装置上の認証サイロの例示的実装、並びに一時記憶装置にアクセスを認可するための階層構造及び要求される認証組合せを決定するための任意の方法を示す概略図である。
【図３Ｂ】[0010]一時記憶装置上の認証サイロの例示的実装、並びに一時記憶装置にアクセスを認可するための階層構造及び要求される認証組合せを決定するための任意の方法を示す概略図である。
【図３Ｃ】[0010]一時記憶装置上の認証サイロの例示的実装、並びに一時記憶装置にアクセスを認可するための階層構造及び要求される認証組合せを決定するための任意の方法を示す概略図である。
【図３Ｄ】[0010]一時記憶装置上の認証サイロの例示的実装、並びに一時記憶装置にアクセスを認可するための階層構造及び要求される認証組合せを決定するための任意の方法を示す概略図である。
【図４】[0011]多重認証サイロを有する一時記憶装置に対するアクセスに関し要求される認可スキームを決定するための必要な実装手順の流れ図である。

【図５】[0012]一時記憶装置に対するホスト機器として作動し得る汎用計算機システムの概略図である。
【発明を実施するための形態】
【００１２】
[0013]ＩＥＥＥ標準規格１６６７は、機器が多重認証サイロを有することを許可しているが、現在、唯一実装されている認証サイロは、証明書サイロである。特定のＡＣＴに対する多重認証サイロが、これらをもとに、単一のデータ記憶領域に対するアクセス認可を統制している。将来、付加的な認証サイロが一時記憶装置（「ＴＳＤ」）上に提供される場合、複数の、ともすれば競合する認証サイロ間の競合及びプライオリティを管理するためのスキームが望まれる。
【００１３】
[0014]一時記憶装置（１００）又はＴＳＤは、機能上、図１に示したような異なるいくつかのコンポーネントに分割される。ＴＳＤ（１００）は、ＴＳＤ（１００）がホスト機器と接続し、通信可能にする物理インターフェース（１０２）を有している。例えば、ユニバーサルシリアルバス（ＵＳＢ）フラッシュドライブ（ＵＦＤ）は、一般に、絶縁体上に置かれた４つの付加接点トレース及び矩形接点によって囲まれる箱形の接点インターフェースを有する。ＴＳＤ（１００）は更に、埋め込みファームウェア（１０６）内で作動するデータ転送、ホスト機器相互認証、及びＴＳＤ（１００）に関するその他の機能性を実行するプロセッサー（１０４）を含む。それぞれＴＳＤ（１００）は、「アドレス可能コマンドターゲット」（ＡＣＴ）レイヤを介しそれぞれアクセスされる少なくとも１つのデータ記憶領域、及び、場合によっては、より個別に認証されたデータ記憶領域（１１６）を有し得、概念において別のストレージシステムの「論理装置」と同様である。図１は、第１のＡＣＴ（１０８ａ）及び第２のＡＣＴ（１０８ｂ）を有するＴＳＤ（１００）を示している。
【００１４】
[0015]ＡＣＴ（１０８ａ，１０８ｂ）それぞれは、ＩＥＥＥ１６６７仕様において「サイロ」と呼ばれるいくつかの機能ユニットを実装していて、少なくとも精査サイロ（１１０ａ，１１０ｂ）及び認証サイロを（１１２ａ，１１２ｂ）含んでいる。ＡＣＴ（１０８ａ，１０８ｂ）それぞれは、付加的な製造者サイロ又はユーザー定義サイロ（１１４ａ，１１４ｂ）を実装し得る。ＡＣＴ（１０８ａ）又は（１０８ｂ）、及び対応したサイロが、ＴＳＤ（１００）上の（１１６ａ）又は（１１６ｂ）に対応したＬＵＮ０又はＬＵＮ１としてアドレス指定される構成及び個別データ領域の認証制御を提供している。
【００１５】
[0016]精査サイロ（１１０ａ，１１０ｂ）は、物理インターフェース（１０２）を介し、接続されるホストによって使用されるＡＣＴ（１０８ａ，１０８ｂ）に問い合わせを行い、利用可能な機能的ユニットを識別する。ＴＳＤ（１００）内の精査サイロ（１１０ａ，１１０ｂ）が、ホスト機器上で実行又は存在しているオペレーティングシステム及びＩＥＥＥ１６６７バージョンの識別を受信する。精査サイロ（１１０ａ，１１０ｂ）が、ＡＣＴ（１０８ａ，１０８ｂ）それぞれにおいて実装されるサイロの数、タイプ、及びバージョンを返却する。精査サイロ（１１０ａ，１１０ｂ）の査問は、更なる任意の動作が実行され得る前に、別の任意のサイロに関しても生じる。
【００１６】
[0017]一旦、精査サイロ（１１０ａ，１１０ｂ）が、必要な装置情報を受信し、返却すると、ＡＣＴ（１０８ａ，１０８ｂ）それぞれに関する認証サイロ（１１２ａ，１１２ｂ）が双方向認証及び認証証明書管理に要求される機能を提供する。認証サイロ（１１２ａ，１１２ｂ）は証明書を使用し、ホスト及びＡＣＴ（１０８ａ，１０８ｂ）それぞれを認証し、証明書の管理も実行する。精査サイロ（１１０ａ，１１０ｂ）、認証サイロ（１１２ａ，１１２ｂ）、及びその他のサイロ（１１４ａ，１１４ｂ）のそれぞれは、ＡＣＴ（１０８ａ，１０８ｂ）それぞれに特有である。一般事項として、データ記憶領域（１１６）は、最初、ＩＥＥＥ標準規格１６６７下の単一の「論理ユニット」又はＡＣＴであると

考えられ、かくして、概して任意の製造者証明書又は置かれている元の認証サイロ又は第１の認証サイロ（１１２ａ）によって処理されるプロビジョニング証明書の支配下にある。しかしながら、第１の認証サイロ（１１２ａ）は、ディスク構成物の便宜上、例えば、図１に示したようなＬＵＮ０（１１６ａ）及びＬＵＮ１（１１６ｂ）である論理ユニット番号（ＬＵＮ＃）を用いて識別される個別にアクセス可能な記憶領域を有するデータ記憶領域（１１６）を多くのＡＣＴ（１０８ａ，１０８ｂ）に仕切るように構成され得る。更に、製造者証明書、プロビジョニング証明書、又は双方がＴＳＤ（１００）上のＡＣＴ又はＡＣＴそれぞれに対する認証サイロの１つより多いタイプを提供し得る。

【００１７】

[0018]認証証明書サイロ（２００）のより詳細な機能コンポーネントの実装説明が図２に示されている。ＩＥＥＥ標準規格１６６７下では、認証証明書サイロ（２００）を保持するための異なる５つのタイプの証明書、製造者証明書（２０２）、プロビジョニング証明書（２０４）、認証証明書チェーン（２０６）、ホスト証明書（２０８）、及びユーザー証明書(２１０)によって定義されている。製造者証明書（２０２）は必須であって、ＴＳＤの同一性を証明する。製造者証明書（２０２）は、ＴＳＤにチャレンジするために使用され得る公開鍵に関するＴＳＤ及び固有識別子を含む。認証サイロ（２００）のＡＣＴそれぞれが、固有の公開鍵を用いて固有キーの組から固有の製造者証明書（２０２）それぞれを計算し得る。しかしながら、必要条件は、製造者すべてが、同一の直接の親の製造者証明書に対するチェーンを証明することである。ＴＳＤ上の第１のＡＣＴに対する製造者証明書が使用され、デフォルト証明書サイロ（２００）の域を超えた付加的タイプの認証サイロを利用可能にする。更に後述されるこの新しい状態の詳細を指定するための、プロビジョニング証明書（２０４）の拡張フィールド（２１２）が使用され得る。

【００１８】

[0019]プロビジョニング証明書（２０４）は、認証サイロ（２００）に対する管理アクセスを許可し、残りの証明書を管理する能力を管理者に提供する。ユーザーは、認証サイロ（２００）にストアされているプロビジョニング証明書（２０４）によって署名された証明書に対するアクセスを有するホスト上の認証証明書を追加、削除、又は置換し得るだけである。初期のＡＣＴに対するプロビジョニング証明書（２０４）は不変で、ＴＳＤが初期プロビジョニング証明書（２０４）を用いて供給されるとき、複数のＡＣＴを含む新しい状態へ再初期化するＴＳＤを生成するために使用され得る。ＴＳＤ上の第１のＡＣＴに対する製造者証明書と同様に初期プロビジョニング証明書が使用され、デフォルト証明書サイロ（２００）の域を超えた付加的なタイプの認証サイロを利用可能にする。更に後述されるようにこの新しい状態の詳細を指定するための、プロビジョニング証明書（２０４）の拡張フィールド（２１２）が使用され得る。初期プロビジョニング証明書（２０４）によって生成された付加的なＡＣＴに特有の付加的プロビジョニング証明書が提供され得る。

【００１９】

[0020]一旦、ＡＣＴが供給されると、ＴＳＤは、認証サイロ証明書チェーン（２０６）をストアし得る。ユーザーは、このチェーンを使用し、別の装置すべてから切り離された同一の製造者及び製品識別番号を有しているパーソナライズ機器を生成し得る。ホストは、証明書チェーン（２０６）のコンテンツを使用してＡＣＴを認証し、ＡＣＴにおいて、ストレージに対するアクセスを認可し得る。本明細書に開示した技術の文脈で証明書チェーン（２０６）の使用方法を更に後述する。

【００２０】

[0021]ホスト証明書（２０８）は、ＴＳＤに取り付けられたとき、ＴＳＤに対するホストを認証する。複数のホスト証明書（２０８）が、ＴＳＤに追加され、複数のホスト機器に対応しているＴＳＤが認証され得る。ＩＥＥＥ標準規格１６６７において、１つホスト証明書も認証サイロ（２００）にストアされていない場合、ＴＳＤは、認証されたとき、特定のホストに対する限定したアクセスを意図していないことを示す自動処理をホストに実行し得る。これは、製造者がデータアクセスのための前提条件としてホスト認証を要求

したときのＴＳＤの構成を単純化する。ＡＣＴは、ホストが認証サイロ内のホスト証明書の１つによって署名された証明書を提示したとき、認証状態に状態遷移する。

【００２１】

[0022]ユーザー証明書(２１０)も、認証サイロに配置され得る。ユーザー証明書(２１０)は、認証サイロ（２００）によって管理されない。ＩＥＥＥ標準規格１６６７下において、任意のアプリケーションが、これらの証明書をストアし得るか又は認証サイロ（２００）から削除し得る。ホスト又はユーザー証明書所有者が、プロビジョニング実行者によってＴＳＤ上に置かれたプロビジョニング証明書（２０４）を使用して首尾よく認証しなかった場合、どんなホスト証明書（２０８）もユーザー証明書(２１０)もＴＳＤに追加され得ない。

【００２２】

[0023]ＩＥＥＥ標準規格１６６７においては、ＴＳＤが記憶ボリューム上のデータに対するセキュアアクセスを提供するために使用され得る前にＴＳＤは、それを準備するそのための一連の動作を遂行する必要がある。ＩＥＥＥ標準規格１６６７は、プロビジョニングとしてこのプロセスを指定している。ＴＳＤのプロビジョニング実行者は必ずしもそのＴＳＤのユーザーではない。プロビジョニング実行者は、事実上、ＴＳＤに対する管理者であって、ユーザー、システム管理者、又は製造者であり得る。

【００２３】

[0024]実際問題としてＴＳＤは、認証サイロ（２００）を含む少なくとも１つのＡＣＴ、初期ＡＣＴ（０）を有する非プロビジョニング状態で製造者から届く。このＡＣＴ（０）の第１のプロビジョニング実行者は、ＡＣＴ特有の設定に加えＴＳＤに関するグローバルな機器設定を指定し得る。ＴＳＤのグローバルな設定は、最初のプロビジョニング動作の間に構成され得るだけである。一旦、ＴＳＤ上に配置されると、初期プロビジョニング証明書（２０４）は有効なままであって、機器が明示的に再初期化（すなわち元の製造状態にリセット）されない限り置き換えられ得ない。かくして、一旦、構成設定が特定されるとそれらは、ＴＳＤが元の製造状態にリセットされない限り決して変更され得ない。プロビジョニング証明書（２０４）のこのリセットは、このデータがセキュアなまま保護データすべてを破壊し、どんなＴＳＤ構成設定も製造時点の初期状態へリセットする。最初のプロビジョニングの成功後、ＴＳＤはここで、それが異なるように振る舞う状態か又は元のものに加え付加的なＡＣＴ及び／又はサイロを公開する状態であり得る。更に、別の製造者による別のＡＣＴのプロビジョニング及びプロビジョニング証明書は、初期製造者証明書（２０２）及びプロビジョニング証明書（２０４）によって設定されたＴＳＤのグローバル設定、ＡＣＴに特有の設定に決して影響し得ない。その上のＴＳＤ及びＡＣＴは、初期製造者証明書（２０２）及びプロビジョニング証明書（２０４）の制約によってセキュアなままである。

【００２４】

[0025]国際電気通信連合ＩＴＵ－Ｔ　Ｘ．５０９標準規格に従って証明書を表すために使用される自律システム番号ＡＳＮ．１データタイプが以下に示されている。これは、ＩＥＥＥ標準規格１６６７に従った製造者証明書（２０２）及びＴＳＤ機器のプロビジョニング証明書（２０４）に関し使用されるフォーマットである。示したように、データタイプは、証明書の終わり近くの拡張フィールドを使用するために提供される。しかしながら、拡張は任意と見なされていて、更に定義されていない。証明書内の拡張フィールドの存在を許すためのバージョンフィールドが、バージョン３（ｖ３）に設定される必要があることに留意されたい。

【００２５】

【表１】

```
Certificate ::= SIGNED { SEQUENCE {
        version [0] Version DEFAULT v1,
        serialNumber CertificateSerialNumber,
        signature AlgorithmIdentifier,
        issuer Name,
        validity Validity,
        subject Name,
        subjectPublicKeyInfo SubjectPublicKeyInfo,
        issuerUniqueIdentifier [1] IMPLICIT UniqueIdentifier OPTIONAL,
                                -- if present, version shall be v2 or v3
        subjectUniqueIdentifier [2] IMPLICIT UniqueIdentifier OPTIONAL,
                                -- if present, version shall be v2 or v3
        extensions [3] Extensions OPTIONAL
                                -- If present, version shall be v3 -- } }

        Version ::= INTEGER { v1(0), v2(1), v3(2) }
        CertificateSerialNumber ::= INTEGER
AlgorithmIdentifier ::= SEQUENCE {
        algorithm ALGORITHM.&id ({SupportedAlgorithms}),
        parameters ALGORITHM.&Type ({SupportedAlgorithms}{ @algorithm})
OPTIONAL }
        -- Definition of the following information object set is deferred, perhaps to
standardized
        -- profiles or to protocol implementation conformance statements. The set is
required to
        -- specify a table constraint on the parameters component of AlgorithmIdentifier.
        -- SupportedAlgorithms ALGORITHM ::= { ... }
Validity ::= SEQUENCE {
        notBefore Time,
        notAfter Time }
SubjectPublicKeyInfo ::= SEQUENCE {
        algorithm AlgorithmIdentifier,
        subjectPublicKey BIT STRING }
Time ::= CHOICE {
        utcTime UTCTime,
        generalizedTime GeneralizedTime }
Extensions ::= SEQUENCE OF Extension
Extension ::= SEQUENCE {
        extnId EXTENSION.&id ({ExtensionSet}),
        critical BOOLEAN DEFAULT FALSE,
        extnValue OCTET STRING
        -- contains a DER encoding of a value of type &ExtnType
        -- for the extension object identified by extnId -- }
ExtensionSet EXTENSION ::= { ... }
```

【００２６】

[0026]本技術は、製造者証明書（２０２）内の任意である拡張フィールド（２１２）及び／又はプロビジョニング証明書（２０４）内の拡張フィールド（２２２）を利用し、証明書サイロというよりも付加的なタイプの認証サイロを提供する。ＴＳＤをプロビジョニングする間、製造者又はプロビジョニング実行者は、ＴＳＤの挙動及び性能を統制する様々な機器設定の利用可能又は利用不可の選択をし得る。製造者又はプロビジョニング実行者は、初期製造者証明書（２０２）内のＩＴＵ－Ｔ　Ｘ．５０９証明書拡張フィールド（２１２）及び／又は初期プロビジョニング証明書（２０４）内の拡張フィールド（２２２）を介し、これらの設定を伝達する。ＡＣＴは、一連の証明コマンドの中でこれらの設定を受信する。期待値に一致しないこれら設定の信憑性は、タンパーが生じた場合、証明書署名フィールドによってＴＳＤ上で検証される。

【００２７】

[0027]プロビジョニング実行者は、製造者証明書（２０２）のリトリーブによって、支援されている利用可能なＴＳＤの構成設定を発見し得る。製造者証明書（２０２）は、その証明書の拡張フィールド（２１２）に許容可能な一連の構成設定を示している。プロビジョニング実行者はこれらの設定を解析し、ＴＳＤ上にプロビジョニング証明書（２０４）を配置している間、もしあれば、プロビジョニング実行者証明書（２０４）の拡張フィールド（２２２）に含むべきか決定する。プロビジョニング証明書（２０４）の拡張フィールド（２２２）内の構成設定は、製造者証明（２０２）の拡張フィールド（２１２）内の任意のデフォルト設定の切り札である。拡張フィールド（２１２，２２２）内の構成設定は、それらが、ＴＳＤからのデータ及び証明書すべてを消去した結果としての、製造者証明書（２０２）又は初期プロビジョニング証明書（２０４）の削除を除いて変更され得ないという点において、不変の値である。

【００２８】

[0028]ここで、製造者証明書（２０２）の拡張フィールド（２１２）に配置される例示的構成設定を説明する。最初、付加的なタイプの認証サイロ生成を提供するための多重認証サイロ拡張設定（２１４）が拡張フィールド（２１２）に配置され得る。この拡張設定（２１４）は、ＴＳＤを構成するための製造者又はプロビジョニング実行者によって使用され得、デフォルト証明書認証サイロ（２００）の域を超えた付加的な認証サイロがＴＳＤ上のＡＣＴのどれかに配置されることが許される。付加的な認証サイロタイプは、パスワードサイロ及び生体識別サイロを含む。ＡＣＴ上の多重認証サイロの状況に直面したとき、拡張フィールド（２１２）の製造者証明書（２０２）を使用した、成功認証のための要求される論理的な組合せ、優先順位の順序付、及びユーザーインターフェース要件を示すための例示的多重認証サイロ拡張設定（２１４）は、以下の通りである。

【００２９】

【表２】

extnid = urn:oid:2.25.329800735698586629295641978511506172922

critical = 00

extnValue = 01, 02, 00, 02, 03, 00, 00, 02, 04, 00, 00, 00, 01, 02, 03, 04, 00,

02, 03, 00

【００３０】

ここで最初の文字列の最初の非０の項は、論理的「最小項」とサイロインデックスの組合せ値の論理積を示している。（値００は、それが精査用に予約された定義によって非認証サイロであるセパレーターとして使用され得る。）この項は、００の後、次に出現する「最小項」組合せなどと組合せられる論理和である。

【００３１】

[0029]上記の例において、最初の組合せ項は、（０１　ＡＮＤ　０２）ＯＲ（０２　ＡＮＤ　０３）である。００，００の出現は、１つの組合せの終わりを示す。この後、次の組合せが始まる。上記の例において次の組合せは（０２　ＡＮＤ　０４）である。００，

００，００の文字列は、一連の組合せの終わりを示している。これは、その後、昇順の優先順位で示したサイロインデックスリストが後に続く。最初の００の出現が、このリストを終了し、そのとき、ユーザー入力を要求しているサイロインデックスが一覧され、再度、００によって終わる。それまでどんなユーザー入力も要求されていないＡＣＴの場合、サイロの優先リストのすぐ後にシーケンス００，００が続く。この機能性を構成する製造者証明書（２０２）の代わりにＴＳＤの状態を変更するためのプロビジョニング証明書（２０４）の拡張フィールド（２２２）が、多重認証サイロ拡張設定（２２４）を含み得ることに留意されたい。

【００３２】

[0030]認証シーケンス拡張設定（２１６）は、ＴＳＤ又はホスト機器に対する論理的順序を構成するように使用され得、多重認証サイロからの認可チャレンジに対する問い合わせを行うか又は回答し、特定のＡＣＴにアクセスするための認証を最も効率的に確立する。多重認証サイロ内の認証オプションを試みるシーケンスは同一か又はホスト機器の識別又はその他の動作環境の態様に従って変化し得る。この機能性を構成する製造者証明書（２０２）の代わりにＴＳＤの状態を変更するためのプロビジョニング証明書（２０４）の拡張フィールド（２２２）が、認証シーケンス拡張設定（２２６）を含み得ることに留意されたい。

【００３３】

[0031]提供され得る別の設定は（２１８）である。多重認証サイロが利用されるとき、ユーザーが関連したＡＣＴにアクセス可能になるためにどのサイロが、認証状態に配置されるべきか指定することは重要であり得る。例えば、一実装において、いくつかの認証サイロが提供又は支援され得るが、それらのどれか１つの認証がアクセスを許可する。例を続けると、ユーザーは、即座にＴＳＤを認証し認可する彼女の個人的なホスト計算機上に正しい証明書を有しているが、ユーザーは、対応した証明書なしに、公共のホスト計算機上でＴＳＤを使用することを所望し、別個のパスワードサイロを認証するためのパスワード入力によってＴＳＤにアクセスし得る。ＴＳＤが、証明書又はパスワードのどちらか一方を受け入れるように構成されている場合、正しいパスワードを用いたユーザーに対するアクセスが許可される。代替例においては、上記のシナリオにおいてアクセスを許可するためのホストからの証明書及びユーザーからのパスワード双方の組合せを要求するようにＴＳＤが構成された場合、必要な認証組合せが認可に利用可能でないので、ユーザーは、公共のホスト計算機上のＴＳＤに対するアクセスを許可されない。この機能性を構成する製造者証明書（２０２）の代わりにプロビジョニング証明書（２０４）の拡張フィールド（２２２）が、ＴＳＤ状態を変更するための認証組合せ拡張設定（２２８）を含み得ることに留意されたい。

【００３４】

[0032]製造者証明書（２０２）の拡張フィールド（２１２）に配置する、別の認証サイロに関連した設定は、特定のサイロに対するユーザー対話要件を構成するためのユーザー対話要求拡張設定（２２０）であり得る。この設定は、サイロを認証状態へ変更するためのＴＳＤとホストとの間の証明書の単なる比較というよりもむしろ、サイロがユーザー入力を要求しているか否か示している。例えば、認証サイロは、パスワード認証、又は顔認識若しくは別の生体認証を要求し、その双方は、対応した認証ファイルか又はＴＳＤ上にストアされている関連するセキュアなハッシュ値と比較するためのホスト機器へのユーザー入力を要求する。代替として証明書認証サイロは、ユーザー入力を要求しない。この機能性を構成する製造者証明書（２０２）の代わりにプロビジョニング証明書（２０４）の拡張フィールド（２２２）が、ＴＳＤの状態を変更するためのユーザー対話要求拡張設定（２３０）含み得ることに留意されたい。

【００３５】

[0033]ＴＳＤ自身か又はホスト機器上で作動中の（例えば、ソフトウェア又は装置に特有の構成ファイル形式の）ＴＳＤのソフトウェアエージェント又はその２つの組合せのどちらか一方が、製造者証明書又はプロビジョニング証明書の拡張フィールド内の多重認証

サイロに関する構成設定に基づく、１つ以上の「認可ポリシー定義式」（ＡＰＥ）を有し得る。ＡＰＥは、以下のコンポーネント、
・認証シーケンスの順番に従って格付けされたサイロ識別の順序付きリストを含む文字列式
・認可されたＡＣＴに対するアクセスが対応した認証サイロが認証状態にあるとき、ＴＳＤによってホスト機器に許可される（例えば、後述されるＭａｘＴｅｒｍｓ／ＭｉｎＴｅｒｍｓから構成される）認証組合せに関する論理式
・どの認証サイロがユーザー対話を要求するか示している文字列式
のうち１つ以上を含み得る。
ホスト機器が、ＡＰＥ内の情報を使用し、ＡＣＴを許可状態にするための最も効率的パスを計算する。可能な認証サイロの任意の論理組合せ及びシーケンスが承諾され得る。ＡＰＥは、グループポリシー執行を考慮すると同時に、認証及び認可プロセスを最適化し統制するための誘導もホスト機器に提供し得る。

【００３６】

[0034]例示的認証サイログループが図３Ａに提示されている。認証サイロＡが、デフォルト証明書サイロ（３０２）として示されている。認証サイロＢが、ユーザーの正しいパスワード入力提示のときのホスト機器から認証されるパスワードサイロ（３０４）として示されている。パスワードサイロ（３０４）は、ユーザー名をリクエストすることによって、特定のパスワードに相互に関連する複数のＴＳＤユーザーを承諾し得るか、又はそれは、それが受け入れるように構成されている複数のパスワードのうちどれかを単に認証する。

【００３７】

[0035]認証サイロＣは、ホスト機器へ取り付けられた指紋読取装置への入力をユーザーが提示したときに認証される指紋サイロ（３０６）として示されている。入力指紋ハッシュが、指紋サイロ（３０６）上にストアされているハッシュと比較され、認証を実行する。指紋サイロ（３０６）は、特定の指紋ハッシュに相互に関連するユーザー名をリクエストすることによって複数のＴＳＤユーザーを承諾し得るか又はそれは、それが受け入れるように構成されている複数の指紋のうちどれかを単に認証する。

【００３８】

[0036]認証サイロＤが、ホスト機器に取り付けられた声紋読取器への入力のユーザーの提示時に認証される声紋サイロ（３０８）として示されている。入力声紋ハッシュが、声紋サイロ（３０８）上にストアされているハッシュと比較され得、認証を実行し得る。声紋サイロ（３０８）は、特定の声紋ハッシュに相互に関連するユーザー名をリクエストすることによって、複数のＴＳＤユーザーを承諾し得るか又はそれは、それが受け付けられるように構成されている複数の声紋のうちどれかを単に認証する。

【００３９】

[0037]認証サイロＥは、ユーザーの網膜スキャン入力提示時、ホスト機器に取り付けられた光学式読取装置において認証される光学式スキャンサイロ（３１０）として示されている。入力された網膜スキャンハッシュが、光学式スキャンサイロ（３１０）上にストアされているハッシュと比較され得、認証を実行し得る。声紋サイロ（３１０）は、特定の網膜スキャンハッシュに相互に関連するユーザー名をリクエストすることによって複数のＴＳＤユーザーを承諾し得るか、又はそれは単に、それが受け付けられるように構成されている複数の網膜スキャンのどれかを認証する。

【００４０】

[0038]図３Ｂは、認証シーケンスの順番に従って、格付けされたサイロ識別の順序付きリスト覧を含む例示的文字列式を図的に示している。サイロＢは、優先される認証方法として最初に格付けされている。故に、この場合、ＡＰＥによって対象とされるホスト機器は、最初にサイロＢを使用した認証を試みる。図３Ａの例においてこれは、ホスト機器がパスワード形式のユーザー入力を求めていて、別の認証サイロのどれかを試みる前にサイロＢにパスワードを提示し、機器をホスト認証することを意味している。示したように認

証の優先シーケンスにおいて、サイロＣが２番目に格付けされ、サイロＤが第３番目に格付けされ、サイロＡが４番目に格付けされ、サイロＥが５番目に格付けされる。ホスト機器は、ＡＰＥに準じこの順番でサイロに対する承認を試みる。しかしながら、ホスト機器は、（例えば動作環境に基づく）決定を実行し得、認証プロセスを早める。例えば、特定のユーザー入力が利用可能でない（例えば、ホスト機器が、図３Ａのようなキーボードも指紋読取装置も装備していない）場合、ホスト機器は、この事実を認識し、認証用のユーザーの声紋入力を求めるために直接スキップする。

【００４１】

[0039]図３Ｃは認証組合せのための論理表現の一例示的実装を図的に示していて、対応した認証サイロが認証状態にあるとき、ＡＣＴに対する認可されたアクセスが、ＴＳＤによってホスト機器に許可される。この例においてＴＳＤは、非常に高いセキュリティを要求しているＡＣＴに対するアクセス認可を提供することが理解され得る。この場合、ＡＰＥは、ＴＳＤ上のＡＣＴに対するアクセスを認可するために、証明書（サイロＡ）及びパスワード（サイロＢ）双方の組合せを要求し、かつ、証明書及びパスワードを組合せた指紋一致（サイロＣ）か又は声紋一致（サイロＤ）のどちらか一方を要求する。代替として、（例えば、光学式読取装置環境の精度又は既知のセキュリティどちらか一方における）光学的網膜スキャン（サイロＥ）のより大きな信頼性により、この認証単独でＴＳＤ上のＡＣＴに対するアクセスを許可する。

【００４２】

[0040]図３Ｄは、ＭａｘＴｅｒｍｓ／ＭｉｎＴｅｒｍｓ構造を使用した認証組合せのための論理式の代替の例示的実装を図的に示していて、対応した認証サイロが認証状態にあるとき、ＡＣＴに対する認可アクセスが、ＴＳＤによってホスト機器に許可される。図３Ｄに示したように、証明書認可（サイロＡ）がパスワード認証（サイロＢ）、指紋認証（サイロＣ）、又は声紋認証（サイロＤ）のどれかと同時に起こった場合、ＴＳＤ上のＡＣＴに対するアクセスが認可される。代替として、光学的スキャン認証（サイロＥ）の提供だけがアクセスを認可する。

【００４３】

[0041]ＴＳＤ（又はＡＰＥに準じたホスト機器）は、標準のＭａｘＴｅｒｍｓ／ＭｉｎＴｅｒｍｓの比較実行によって、これらの特定の組合せのうちどれかが存在しているか決定し得る。最小項は、サイロＡとＢ、サイロＡとＣ、サイロＡとＤ、及びサイロＥの組合せである。サイロのどれかが認証された場合、その状態が１によって示され得る。サイロが認証されない場合、その状態は０によって示され得る。ＭｉｎＴｅｒｍ演算子へのこれら状態値の組合せは、状態値を一緒に乗ずることによって実行される。かくして、１つの項の状態が０の場合、ＭｉｎＴｅｒｍが０になり、項の状態双方が１の場合、その組合せに対するＭｉｎＴｅｒｍは１になる。ＭｉｎＴｅｒｍの組合せすべての合計ＭａｘＴｅｒｍが０より大きいときに限り、適切な認証及び認可となる。ＭｉｎＴｅｒｍｓすべてが０の場合、ＭａｘＴｅｒｍは０になり、ＡＣＴに対するアクセスが拒否される。ＭｉｎＴｅｒｍのどれかが０より大きい場合、ＭａｘＴｅｒｍは０より大きくなり、ＡＣＴに対するアクセスが許可される。

【００４４】

[0042]多重認証サイロを有する環境において、ＴＳＤユーザーによるＡＣＴに対するアクセスを認可するための例示的認証プロセス（４００）が図４に提示されている。アクセス動作（４０２）において、ＴＳＤ上の精査サイロがホストによってアクセスされ、サイロの数、タイプ、及びバージョンに関し精査サイロに問い合わせを行われる。同時にホストは、特定のオペレーティングシステム及びＩＥＥＥ１６６７のバージョン情報をホスト機器に提供する。第２番目のアクセス動作（４０４）において、次にホストは、サイロ情報を使用し、精査サイロによって提供される識別情報に基づき認証サイロ（単数又は複数）をアクセスする。特定のＡＣＴに対し複数の認証サイロが存在していることを精査サイロが示している場合、認証プロセス（４００）において支援するＡＰＥが構築され得、認証要件を調整し、認証サイロの状態を報告し、アクセス認証に要求される集合的状態が獲

得されたか否か決定する。プロセス（４００）は次に、ＡＰＥに準じ、最初の決定動作（４０６）に示した認可に要求される認証組合せが存在するか否か決定する。動作（４０８）において、プロセス（４００）は更に、機器の優先傾向又はホストの最適化決定に従って、多重サイロの論理組合せ認証に関する論理的なシーケンス又は順番を決定する。動作（４１０）において、優先傾向及び／又はホスト最適化に従って、最初に発生する認証サイロの論理組合せが選択される。

【００４５】

[0043]ＡＰＥが更に、特定の認証サイロがユーザー入力を要求しているか否かに関する情報を提供する。クエリー動作（４１２）において、プロセス（４００）は、シーケンス内の最初の認証サイロに関しユーザー入力が、サイロを認証するために要求されているか否かクエリーする。ユーザー入力が要求されていない場合、プロセスは、認証動作（４１８）へ移り、自動認証組合せ（例えばホスト機器によって提供されている証明書）の認証を試みる。プロセス（４００）はクエリー動作（４２０）へ移り、認証の組合せが、ＴＳＤに要求されているＡＣＴに対する認可アクセスの認証すべてが成功した結果をもたらしたか否か決定する。要求されている認証の組合せが満たされた場合、ホストは権限を与えられ、許可動作（４２２）に示したようにＡＣＴに対するアクセスが許可される。

【００４６】

[0044]ユーザー入力のクエリー動作（４１２）に戻ると、ユーザー入力（例えば、パスワード又は生体認証）が要求された場合、リクエスト動作（４１４）において、ホスト機器が要求されているユーザー入力をリクエストする。クエリー動作（４１６）において、その後、ホスト機器が、リクエストされた入力情報が利用可能であるか否か決定する。ホスト機器が、リクエストされたユーザー入力が利用可能でない（例えば、ホスト機器が特定の入力インターフェース機器へ接続されない）場合か又は適正な期間後、ユーザー入力が何も供給されていないか決定した場合、プロセス（４００）は、クエリー動作（４２４）の一部として試みられ得る更なる任意の論理組合せが残っているか否か決定する。動作（４２６）に示したように、更なる組合せが残っていない場合、ホストは、更なる任意の認証の試みを終了する。しかしながら、更に組合せが残っている場合、プロセス（４００）が動作（４１０）へ戻ったとき次の組合せが選択され、利用可能な次の組合せを選択する。

【００４７】

[0045]代替としてクエリー動作（４１６）が、ユーザー入力が利用可能かつ適切であることを決定した場合、プロセスは動作（４１８）へ移って、別に必要なデータを用いたユーザー入力が、論理的なＡＣＴ組合せ認証の試みの際に使用される。プロセス（４００）は、その後、クエリー動作（４２０）へ移って要求される認証組合せのどれかが満足しているか否か決定する。認証サイロの認証状態が、要求される認証組合せの達成が集合的結果になる場合、ホストは、権限を与えられ、許可動作（４２０）に示したように、ＡＣＴに対するアクセスが許可される。

【００４８】

[0046]代替として、クエリー動作（４１６）が認証証明書又は受信した入力が無効であることを決定した場合か又はクエリー動作（４２０）が要求されている認証サイロの組合せが満足していないことを決定した場合かどちらか一方のとき、プロセス（４００）は、クエリー動作（４２４）において、任意の論理的な試みられる組合せが残っているか否か決定する。どんな組合せも残っていない場合、実行されるＡＣＴに対するアクセスを認証するどんな試みも、動作（４２６）に示したように実行されない。代替として、更なる組合せが利用可能な場合、選択動作（４１０）において示したように、プロセス（４００）は、試みられる認証に関する次の認証サイロの組合せを選択し得、既に説明したようなＴＳＤに対するホスト機器の認可を試み得る。

【００４９】

[0047]ＴＳＤに対しホスト計算機装置として作動する汎用計算装置（５００）の概略図が、図５に示されている。ホスト計算装置に関する例示的ハードウェア及び動作環境は、

処理ユニット（５０２）、システムメモリー（５０４）、及びシステムメモリー（５０４）を含む様々なシステムコンポーネントを処理ユニット（５０２）と接続するシステムバス（５１８）を含み得る。計算機（５００）のプロセッサーは、単一の中央演算処理ユニット（ＣＰＵ）、又は並列処理環境として一般的に参照される複数の処理ユニットを含む１つ以上の処理ユニット（５０２）があり得る。計算機（５００）は、従来のコンピューター、分散コンピューター、又はその他任意のタイプのコンピューターである。

【００５０】

[0048]システムバス（５１８）は、メモリーバス、又はメモリーコントローラー、周辺バス、スイッチ型ファブリックバス、二地点間接続バス、及び様々な任意のバスアーキテクチャを使用したローカルバスを含むいくつかのタイプのバス構造のどれかであり得る。システムメモリー（５０４）は、単にメモリーとしても参照され得、読み出し専用メモリー（ＲＯＭ）（５０６）及びランダムアクセスメモリー（ＲＡＭ）（５０５）を含む。計算機（５００）内のエレメント間の情報の始動中の送信を援助する基本ルーチンを含む基本入力／出力システム（ＢＩＯＳ）（５０８）は、ＲＯＭ（５０６）にストアされている。計算機（５００）は更に、示されていないハードディスクから読み出し、それに書き込むためのハードディスクドライブ（５３０）、取外し可能磁気ディスク（５３６）から読み出すか又はそれに書き込むための磁気ディスクドライブ（５３２）、及びＣＤ－ＲＯＭ若しくはその他の光学式媒体のような取外し可能光ディスク（５３８）から読み出すか又はそれに書き込むための光ディスクドライブ（５３４）を含む。

【００５１】

[0049]ハードディスクドライブ（５３０）、磁気ディスクドライブ（５３２）、及び光ディスクドライブ（５３４）は、それぞれハードディスクドライブインターフェース（５２０）、磁気ディスクドライブインターフェース（５２２）、及び光ディスクドライブインターフェース（５２４）によってシステムバス（５１８）へ接続される。ドライブ及びそれらに関連する計算機可読媒体が、計算機可読命令、データ構造、プログラムモジュール、及びその他の計算機（５００）用データの不揮発性記憶装置を提供する。計算機によってアクセス可能なデータをストアし得る任意のタイプの計算機可読媒体、例えば、磁気カセット、フラッシュメモリーカード、デジタルビデオディスク、ＲＡＭ、ＲＯＭが例示的動作環境において使用され得ることを当業者は十分理解されよう。

【００５２】

[0050]オペレーティングシステム（５１０）、１つ以上のアプリケーションプログラム（５１２）、その他のプログラムモジュール（５１４）、及びプログラムデータ（５１４）を含む多くのプログラムモジュールが、ハードディスク（５３０）、磁気ディスク（５３２）、光ディスク（５３４）、ＲＯＭ（５０６）、又はＲＡＭ（５０５）にストアされ得る。例示的実装において、ＴＳＤとの通信用プログラム及びデータ転送用プログラムが、（例えば、アプリケーションプロトコルインターフェース（ＡＰＩ）の一部のように）オペレーティングシステム（５１０）、アプリケーションプログラム（５１２）、又はその他のプログラムモジュール（５１４）（例えば、認証プロセス間のＡＰＥを処理するモジュール）の一部として組み込まれる。

【００５３】

[0051]ユーザーは、キーボード（５４０）及びポインティングデバイス（５４２）、例えばマウスのような入力装置を介しパーソナルコンピューター（５００）へコマンド及び情報を入力し得る。別の（示されていない）入力装置は、例えばマイクロフォン、ジョイスティック、ゲームパッド、タブレット、タッチスクリーン装置、衛星放送受信アンテナ、スキャナー、ファクシミリ機器、及びビデオカメラを含み得る。これらの入力装置及びその他の入力装置は、多くの場合、システムバス（５１８）へ接続されるシリアルポートインターフェース（５２６）を介し処理ユニット（５０２）へ接続されるが、パラレルポート、ゲームポート、又はユニバーサルシリアルバス（ＵＳＢ）のような別のインターフェースによって接続され得る。

【００５４】

[0052]モニター（５４４）又はその他のタイプの表示装置もビデオアダプター（５４６）のようなインターフェースを介しシステムバス（５１８）へ接続される。モニター（５４４）に加えて計算機は、典型的に、プリンター（５５８）及び（示されていない）スピーカーなど別の周辺出力装置を含む。これらの装置及びその他の出力装置は、多くの場合、システムバス（５１８）へ接続されるシリアルポートインターフェース（５２６）を介し処理ユニット（５０２）へ接続されるが、パラレルポート、ゲームポート、又はユニバーサルシリアルバス（ＵＳＢ）のような別のインターフェースによって接続される。メディアチューナーモジュール（５６０）もシステムバス（５１８）に関連付けられ得、ビデオアダプター（５４６）又はその他の出力提示モジュールを介した出力用音声及び映像プログラム（例えばテレビ番組）に合わせる。

【００５５】

[0053]計算機（５００）は、１つ以上のリモートコンピューター（５５４）のようなリモートコンピューターとの論理接続を使用したネットワーク接続環境において作動し得る。これらの論理接続は、計算機（５００）と接続され得るか又は統合され得る通信装置によって達成され得、本発明は特定タイプの通信装置に限定されない。リモートコンピューター（５５４）は、別の計算機、サーバー、ルーター、ネットワークパーソナルコンピューター、クライアント、ピア装置、又はその他の一般的なネットワークノードであり得、計算機（５００）に関し前述した多くのエレメント又はエレメントすべてを典型的に含むが、図５にはメモリー記憶装置（５５６）だけが例示されている。図５に示した論理接続は、ローカルエリアネットワーク（ＬＡＮ）（５５０）及び広域ネットワーク（ＷＡＮ）（５５２）を含む。そのようなネットワーク環境は、オフィスネットワーク、企業コンピューターネットワーク、イントラネット、及びインターネット、すべてのタイプのネットワークにおいて一般的である。

【００５６】

[0054]ＬＡＮ（５５０）環境において使用されるとき、計算機（５００）は、ネットワークインターフェース（５２８）又はアダプター、例えばイーサネット（登録商標）又はその他の通信インターフェースを介しローカルネットワーク（５５０）へ接続され得る。ＷＡＮ（５５２）環境において使用されるとき、計算機（５００）は、典型的に、モデム（５４８）、ネットワークアダプター、又はその他任意タイプの広域ネットワーク（５５２）上の通信を確立するための通信装置を含む。内蔵又は外付けがあり得るモデム（５４８）が、シリアルポートインターフェース（５２６）を介しシステムバス（５１８）へ接続される。ネットワーク接続環境において、パーソナルコンピューター（５００）又はその一部に関し示されているプログラムモジュールが、リモートメモリー記憶装置にストアされ得る。示したネットワーク接続が例示的であって、計算機間の通信リンクを確立する別の手段及び通信装置が使用され得ることを十分に理解されよう。

【００５７】

[0055]本明細書に記載した技術は、１つ以上のシステムにおいて論理動作及び／又はモジュールとして実装され得る。論理動作は、１つ以上の計算機システムにおいて実行している、プロセッサーに実装されるステップシーケンスとして実装され得、１つ以上の計算機システム内部で相互接続された計算機又は回路モジュールとして実装され得る。同様に、様々なコンポーネントモジュールの記述が、モジュールによって実行される動作によって提供され得るか又は作用され得る。結果として生じる実装は、選択事項であって、記載した技術を実装している基本システムの性能要件に依存する。したがって、本明細書に記載した技術の実施形態を作り出す論理動作は、動作、ステップ、オブジェクト、又はモジュールとして様々に参照される。更に、明示的に請求した別の方法でも特定の順番が請求言語によって本質的に必要とされていない場合、論理動作が任意の順番で実行され得ることを理解されよう。

【００５８】

[0056]実装の中には、製造品が計算機プログラム製品として提供されるものもある。一実装において、計算機プログラム製品は、コンピューターシステムによって実行可能な符

号化された命令をストアしている計算機可読媒体として提供される。別の計算機プログラム製品の実装は、計算システムによって搬送波で具現化された計算機プログラムを符号化している計算機データ信号の中に提供され得る。本明細書において、別の実装も記載され、示されている。

【００５９】

[0057]上記の仕様、例、及びデータは、本発明の例示的実施形態の構造及び使用に関する完全な記述を提供している。本発明の様々な実施形態が、ある程度特殊性又は個別の１つ以上の実施形態とともに前述されているが、当業者は、この発明の趣旨及び範囲から逸脱せずに開示した実施形態に対し、多くを変更し得る。具体的に、記載した技術は、パーソナルコンピューターと独立して使用され得ることが理解されよう。故に別の実施形態が想定される。上記説明に含まれ、添付図面に示したすべての事項が、例示的特定の実施形態に過ぎず、限定しないように解釈されるべきであることを意図している。以下の請求項に定義されているような詳細変更又は構造的変更が、本発明の基本要素から逸脱せずに実施され得る。

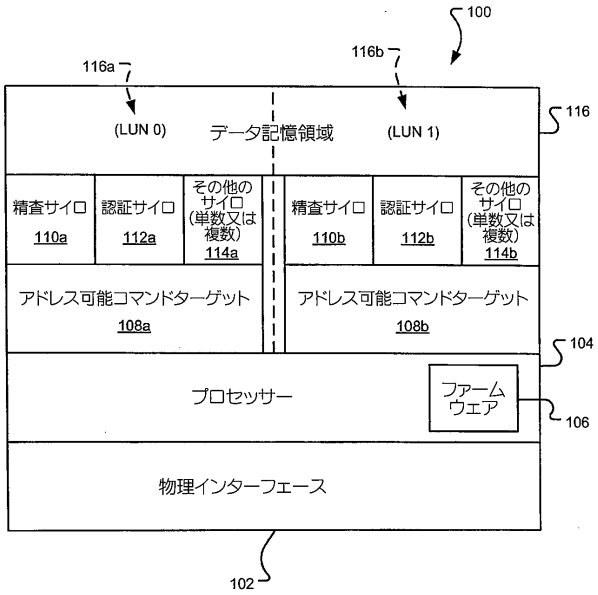
【符号の説明】

【００６０】

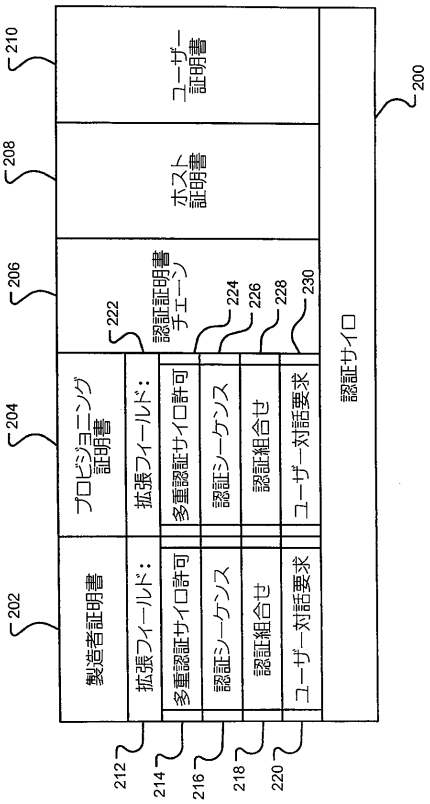
１００　一時記憶装置
１０２　物理インターフェース
１０４　プロセッサー
１０６　ファームウェア
１０８ａ　第１のアドレス可能コマンドターゲット（ＡＣＴ）
１０８ｂ　第２のアドレス可能コマンドターゲット（ＡＣＴ）
１１０ａ　精査サイロ
１１０ｂ　精査サイロ
１１２ａ　認証サイロ
１１２ｂ　認証サイロ
１１４ａ　ユーザー定義サイロ
１１４ｂ　ユーザー定義サイロ
１１６　記憶領域
１１６ａ　データ記憶領域
１１６ｂ　データ記憶領域
２００　認証証明書サイロ
２０２　製造者証明書
２０４　プロビジョニング証明書
２０６　認証証明書チェーン
２０８　ホスト証明書
２１０　ユーザー証明書
２１２　拡張フィールド
２１４　多重認証サイロ拡張設定
２１６　認証シーケンス拡張設定
２１８　認証組合せの拡張設定
２２０　ユーザー対話要求拡張設定
２２２　拡張フィールド
２２４　多重認証サイロ拡張設定
２２６　認証シーケンス拡張設定
２２８　認証組合せ拡張設定
２３０　ユーザー対話要求拡張設定
３０２　デフォルト証明書サイロ
３０４　パスワードサイロ
３０６　指紋サイロ

３０８　声紋サイロ
３１０　光学式スキャンサイロ
５００　汎用計算装置
５０２　処理ユニット
５０４　システムメモリー
５０５　ランダムアクセスメモリー（ＲＡＭ）
５０６　読み出し専用メモリーＲＯＭ
５０８　基本入力／出力システム（ＢＩＯＳ）
５１０　オペレーティングシステム
５１２　１つ以上のアプリケーションプログラム
５１４　その他のプログラムモジュール
５１６　プログラムデータ
５１８　システムバス
５２０　ハードディスクドライブインターフェース
５２２　磁気ディスクドライブインターフェース
５２４　光ディスクドライブインターフェース
５２６　シリアルポートインターフェース
５２８　ネットワークインターフェース
５３０　ハードディスクドライブ
５３２　磁気ディスクドライブ
５３４　光ディスクドライブ
５３６　取外し可能磁気ディスク
５３８　取外し可能光ディスク
５４０　キーボード
５４２　ポインティングデバイス
５４４　モニター
５４６　ビデオアダプター
５４８　モデム
５５０　計算機
５５２　広域ネットワーク
５５４　リモートコンピューター
５５６　メモリー記憶装置
５５８　プリンター
５６０　メディアチューナーモジュール

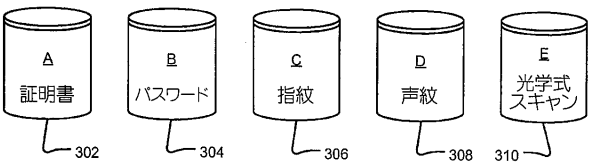
【図１】



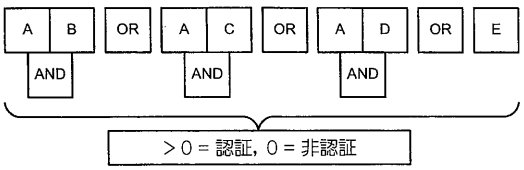
【図２】



【図３Ａ】



【図３Ｄ】



【図３Ｂ】

A	B	C	D	E
4	1	2	3	5

Fig. 3B

【図３Ｃ】

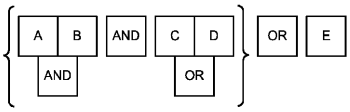
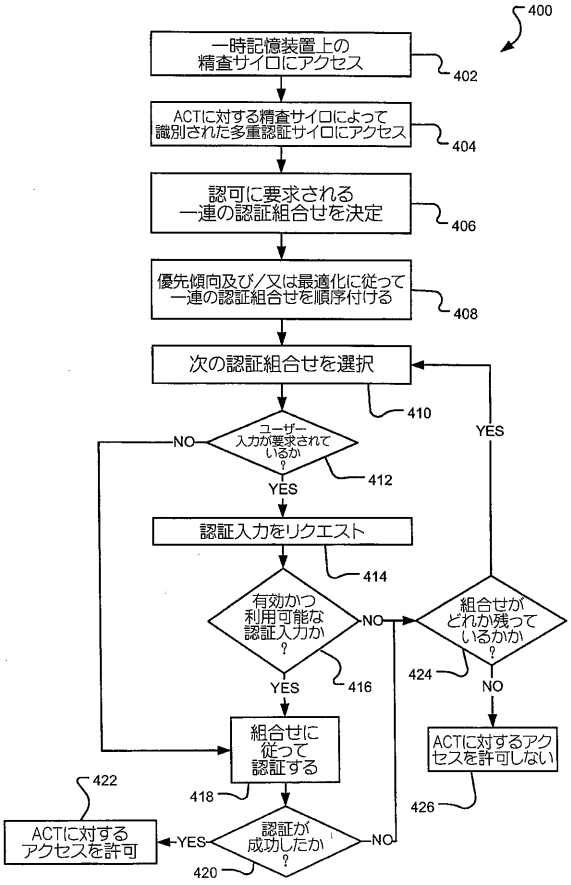
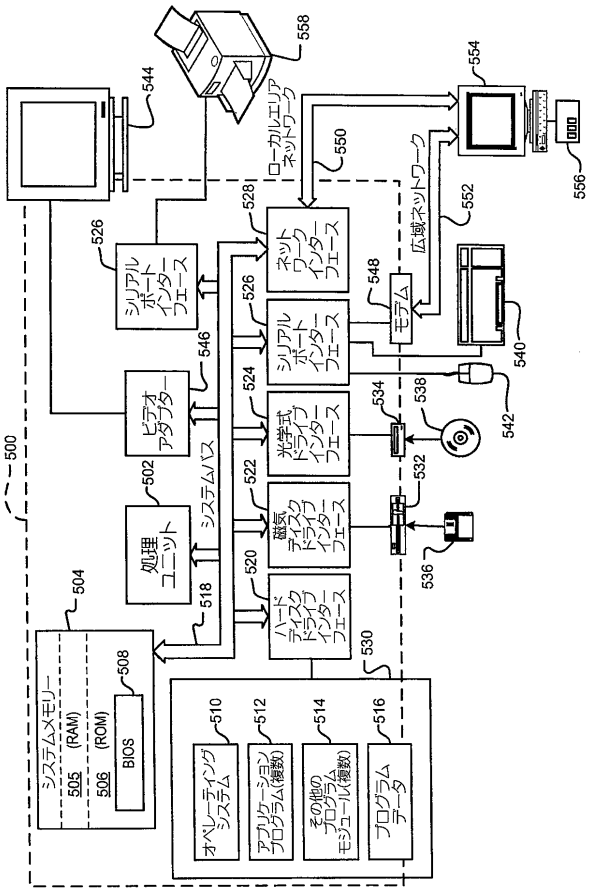


Fig. 3C

【図４】


400
一時記憶装置上の精査サイロにアクセス
402
ACTに対する精査サイロによって識別された多重認証サイロにアクセス
404
認可に要求される一連の認証組合せを決定
406
優先傾向及び/又は最適化に従って一連の認証組合せを順序付ける
408
次の認証組合せを選択
410
ユーザー入力が要求されているか？
412
NO
YES
認証入力をリクエスト
414
有効かつ利用可能な認証入力か？
416
NO
YES
組合せがどれか残っているか？
424
YES
NO
組合せに従って認証する
418
ACTに対するアクセスを許可しない
426
ACTに対するアクセスを許可
422
認証が成功したか？
420
YES
NO

【図５】


500
システムバス
処理ユニット
502
システムメモリー
504
505 (RAM)
506 (ROM)
BIOS
508
オペレーティングシステム
510
アプリケーションプログラム(複数)
512
その他のプログラムモジュール(複数)
514
プログラムデータ
516
518
ビデオアダプター
526
シリアルポートインターフェース
526
ネットワークインターフェース
528
ローカルエリアネットワーク
550
広域ネットワーク
552
モデム
548
シリアルポートインターフェース
524
光学式ドライブインターフェース
534
磁気ディスクドライブインターフェース
522
ハードディスクドライブインターフェース
520
530
532
536
538
540
542
544
546
554
556
558

フロントページの続き

(72)発明者　ボヴィー，ジェームズ
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　岸野　徹

(56)参考文献　特開平０９－０３５０３０（ＪＰ，Ａ）
特開平１１－０６５９３８（ＪＰ，Ａ）
特開２００３－１４３１３６（ＪＰ，Ａ）
特開２００３－２４８６６２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６２
Ｇ０６Ｆ　２１／４５
Ｇ０６Ｋ　１７／００
Ｇ０６Ｋ　１９／１０