(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6293133号
(P6293133)
(45)発行日　平成30年3月14日(2018.3.14)　(24)登録日　平成30年2月23日(2018.2.23)

(51)Int.Cl.　　F I
G06F 12/14 (2006.01)　　G06F 12/14　５１０Ｄ
G06F 21/62 (2013.01)　　G06F 21/62
G06F 21/57 (2013.01)　　G06F 21/57

請求項の数 9　(全 16 頁)

(21)出願番号　特願2015-518461 (P2015-518461)
(86)(22)出願日　平成25年6月13日 (2013.6.13)
(65)公表番号　特表2015-524128 (P2015-524128A)
(43)公表日　平成27年8月20日 (2015.8.20)
(86)国際出願番号　PCT/US2013/045725
(87)国際公開番号　WO2013/192016
(87)国際公開日　平成25年12月27日 (2013.12.27)
審査請求日　平成28年6月13日 (2016.6.13)
(31)優先権主張番号　13/527,439
(32)優先日　平成24年6月19日 (2012.6.19)
(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　100140109
弁理士　小野　新次郎
(74)代理人　100118902
弁理士　山本　修
(74)代理人　100106208
弁理士　宮前　徹
(74)代理人　100120112
弁理士　中西　基晴

最終頁に続く

(54)【発明の名称】被保護データー集合のネットワーク・ベース管理

(57)【特許請求の範囲】
【請求項１】
システムであって、
複数のエンティティによって出された信頼実行環境コマンドをネットワークを介して受信することができる受信モジュールであって、各信頼実行環境コマンドが、前記コマンドを出したエンティティに対応するセキュリティ・コンテキストに対して動作するコマンドである、受信モジュールと、
前記受信モジュールによって受信された前記信頼実行環境コマンドに応答して、鍵および被保護データー集合に対して複数の暗号プロセスおよびセキュリティ・プロセスを実行するように構成されたセキュリティ・プロセッサー・インスタンスであって、該セキュリティ・プロセッサー・インスタンスが、特定のエンティティと該特定のエンティティの対応する被保護データー集合とに結び付けられ、該セキュリティ・プロセッサー・インスタンスが、他のエンティティからの実行環境コマンドを処理するのを阻止される、セキュリティ・プロセッサー・インスタンスと、
複数の被保護アカウントを維持するように構成されたアカウント管理モジュールであって、前記複数のアカウントの内特定の被保護アカウントが、前記特定のアカウントに割り当てられた前記特定のエンティティに対応し、前記特定のエンティティに対応する複数の鍵を含む被保護データー集合を含み、前記被保護データー集合が、前記システムの外部では読み取り可能ではなく、前記セキュリティ・プロセッサー・インスタンスが、前記複数の鍵の内少なくとも一部を使用して、前記特定のエンティティから受信した１つ以上の信

頼実行環境コマンドに応答して、暗号プロセスを実行する、アカウント管理モジュールと、
を含み、
前記特定のアカウントが、各々前記特定のアカウントに関連するエンティティに対応する複数のデーター集合を含み、前記特定のデーター集合が第１データー集合であり、前記特定のエンティティが第１エンティティであり、前記複数の鍵が第１複数の鍵であり、前記特定のアカウントが、更に、
前記特定のアカウントに割り当てられた第２エンティティに対応し、前記第２エンティティに対応する第２複数の鍵を含む第２被保護データー集合を含み、前記第２被保護データー集合が、前記システムの外部では読み取り可能でなく、前記セキュリティ・プロセッサー・インスタンスが、前記第２エンティティから受信した１つ以上の信頼実行環境コマンドに応答して、前記第２複数の鍵の内少なくとも一部を使用して暗号プロセスを実行する、システム。

【請求項２】
請求項１記載のシステムにおいて、前記信頼実行環境コマンドが、トラステッド・プラットフォーム・モジュール（ＴＰＭ）通信プロトコルに準拠する、システム。

【請求項３】
請求項１記載のシステムにおいて、前記被保護データー集合が、前記セキュリティ・プロセッサー・インスタンスによる場合を除いて、読み取り不可である少なくとも一部を含む、システム。

【請求項４】
請求項１記載のシステムにおいて、前記アカウント管理モジュールが、更に、新たなエンティティが前記アカウントに追加されたとき、新たな被保護データー集合を前記複数のデーター集合に追加するように構成される、システム。

【請求項５】
請求項１記載のシステムにおいて、前記アカウント管理モジュールが、更に、対応するエンティティがもはや動作しなくなった後に、被保護データー集合を前記複数のデーター集合から除去するように構成される、システム。

【請求項６】
請求項１記載のシステムにおいて、前記特定のエンティティが特定のデバイスまたはシステムであり、前記アカウント管理モジュールが、更に、前記被保護データー集合の一部をリセットしたことに応答して、前記特定のデバイスまたはシステムがリブートされたことを検出するように構成される、システム。

【請求項７】
請求項１記載のシステムであって、更に、
前記データー集合に関してポリシーが満たされるか否かに依存して、前記特定のエンティティによるアクションを許可するように構成されたポリシー・モジュールを含む、システム。

【請求項８】
コンピューター・プログラムであって、計算システムに、複数の被保護アカウントを維持するように構成されたアカウント管理モジュールを、インスタンス化させ、前記複数のアカウントの内特定の被保護アカウントが、前記特定のアカウントに割り当てられた特定のエンティティに対応し、前記特定のエンティティに対応する複数の鍵を含む被保護データー集合を含み、前記被保護データー集合が、前記特定のアカウントの外部では読み取り可能ではなく、セキュリティ・プロセッサー・インスタンスが、前記特定のエンティティから受信した１つ以上の信頼実行環境コマンドに応答して、前記複数の鍵の内少なくとも一部および被保護データー集合を使用して暗号プロセスおよびセキュリティ・プロセスを実行し、前記セキュリティ・プロセッサー・インスタンスが、前記特定のエンティティと該特定のエンティティの対応する被保護データー集合とに結び付けられ、前記セキュリティ・プロセッサー・インスタンスが、他のエンティティからの実行環境コマンドを処理す

るのを阻止され、
前記特定のアカウントが、各々前記特定のアカウントに関連するエンティティに対応する複数のデーター集合を含み、前記特定のデーター集合が第１データー集合であり、前記特定のエンティティが第１エンティティであり、前記複数の鍵が第１複数の鍵であり、前記特定のアカウントが、更に、
前記特定のアカウントに割り当てられた第２エンティティに対応し、前記第２エンティティに対応する第２複数の鍵を含む第２被保護データー集合を含み、前記第２被保護データー集合が、前記システムの外部では読み取り可能でなく、前記セキュリティ・プロセッサー・インスタンスが、前記第２エンティティから受信した１つ以上の信頼実行環境コマンドに応答して、前記第２複数の鍵の内少なくとも一部を使用して暗号プロセスを実行する、
コンピューター・プログラム。
【請求項９】
請求項８記載のコンピューター・プログラムであって、更に、前記計算システムに、ネットワークを介して複数のエンティティによって出された前記信頼実行環境コマンドに応答して複数の暗号プロセスおよびセキュリティ・プロセスを鍵に対して実行するように構成された前記セキュリティ・プロセッサー・インスタンスをインスタンス化させ、各信頼実行環境コマンドが、前記コマンドを出したエンティティに対応するセキュリティ・コンテキストに対して動作するコマンドである、コンピューター・プログラム。

【発明の詳細な説明】
【背景技術】
【０００１】
[0001] トラステッド・プラットフォーム・モジュール（または「ＴＰＭ」：Trusted Platform Modules）は、計算デバイスの正規な(regular)動作環境から分離された、信頼のおける実行環境である。通例、ＴＰＭは、計算デバイスに物理的に結合されるチップの形態で実現される。正規動作環境は、インターフェースを介してＴＰＭと通信することができ、このインターフェースの一例にＴＰＭベース・サービス（または「ＴＢＳ」）がある。
【０００２】
[0002] ＴＰＭは、暗号鍵生成、ポリシー主導鍵使用（policy-driven key use）、機密記憶(sealed storage)、および証明に最も一般的に使用される範囲の機能を提供する。ＴＰＭは、「被保護エリア」と呼ばれるメモリーの領域を有し、読み取ることができないデーターを収容するが、しかしながら、このようなデーターを使用して動作を実行すること、および／またはこのようなデーターに対して動作を実行することができる。このデーターの一部は、イミュータブルであり、つまり実行されている動作によって読み取られ（しかし変化させられない）、このデーターの一部はミュータブルであり、このような動作によって変化させることができる。尚、これは、データーを読み取っているＴＭＰに対して内部で行われている動作であることを注記しておく。被保護データーは、ＴＰＭ外部では読み取ることができない。
【発明の概要】
【発明が解決しようとする課題】
【０００３】
[0003] このように、ＴＰＭは動作を実行する動作コンポーネントと、ＴＰＭの外部に読み出すことができない被保護データーを保持するメモリー・コンポーネントとを有する。ＴＰＭの動作速度は、ＴＰＭ内部のハードウェアの能力に限定される。また、被保護データーのサイズもＴＰＭ内部の空間に限定される。

【課題を解決するための手段】
【０００４】

[0004] 本明細書において説明する少なくとも１つの実施形態は、被保護アカウントを維持するように構成されたアカウント管理モジュールを含むシステムに関する。例えば、特定の被保護アカウントは、このシステムの外部からアクセスすることができない被保護データー集合を含み、このデーター集合には恐らくアカウントの外部からでもアクセスできない。この特定のデーター集合は、特定のアカウントに割り当てられた特定のエンティティ（例えば、デバイス、システム、ユーザー、コンポーネント、またはこれらの組み合わせ）に対応し、特定のデバイスに対応する鍵を含む。セキュリティ・プロセッサーは、これらの鍵の少なくとも一部を使用して、特定のエンティティから受ける１つ以上の信頼実行環境コマンドに応答して、暗号プロセスおよびセキュリティ・プロセスを実行する。実施形態では、同じアカウントに属する異なるエンティティに対して複数のデーター集合があってもよい。

【０００５】

[0005] この摘要は、詳細な説明において以下で更に説明する概念から選択したものを、簡略化した形態で紹介するために設けられている。この摘要は、特許請求する主題の主要な特徴や必須の特徴を特定することを意図するのではなく、特許請求する主題の範囲を判断するときに補助として使用されることを意図するのでもない。

【図面の簡単な説明】

【０００６】

[0006] 以上で説明したおよびその他の利点ならびに特徴を得ることができる方法について説明するために、添付図面を参照して種々の実施形態の更に特定的な説明を行う。これらの図面は実施形態の見本を図示するに過ぎず、したがって本発明の範囲を限定すると見なされないことを認めた上で、添付図面を使用することによって、更に具体的にそして詳細に、実施形態について説明する(described and explained)。

【図１】図１は、本明細書において説明する実施形態を採用するために使用することができ、管理レベルおよびローカル信頼実行環境レベルを含む計算システム例を示す。

【図２】図２は、複数のクライアントの一部が、トラステッド・プラットフォーム・モジュール（ＴＰＭ）を利用して、ネットワークを介してシステムとインターフェースする環境を示し、本システムは複数のアカウントを含み、各アカウントが、クライアントから受けるローカル信頼実行環境コマンドに応答して実現される暗号プロセスの対象となる１つ以上の被保護データー集合を有する。

【図３】図３は、イミュータブル・データーおよびミュータブル・データーを含む、被保護データー集合を抽象的に示す。

【図４】図４は、信頼実行環境コマンドを管理する方法のフローチャートを示す。

【発明を実施するための形態】

【０００７】

[0011] 本明細書において説明する少なくとも１つの実施形態によれば、アカウント管理モジュールが被保護アカウントを維持するシステムについて説明する。例えば、特定の被保護アカウントは、システムの外部からはアクセスできず、恐らくアカウントの外部からでもアクセスできない被保護データー集合を含む。特定のデーター集合は、特定のアカウントに割り当てられた特定のエンティティ（例えば、デバイス、システム（計算システムのような）、ユーザー、コンポーネント、またはこれらの組み合わせ）に対応し、特定のエンティティに対応する鍵を含む。セキュリティ・プロセッサーは、複数の鍵の内少なくとも一部を使用して、特定のエンティティから受けた１つ以上の信頼実行環境コマンドに応答して、暗号プロセスおよびセキュリティ・プロセスを実行する。実施形態では、複数のデーター集合があってもよく、各々が異なるエンティティに対応する。更に、必須ではないが、１つのアカウント内部に複数の被保護データー集合があってもよい。

【０００８】

[0012] 計算システムは、今日増々多様な形態を取りつつある。例えば、計算システムは、ハンドヘルド・デバイス（スマート・フォンのような）、アプライアンス、ラップトップ・コンピューター、デスクトップ・コンピューター、メインフレーム、分散型計算シ

ステム、または従来では計算システムとは見なされなかったデバイス（腕時計、調理家電、自動車、医療用インプラント等）でもよい。この説明および特許請求の範囲では、「計算システム」という用語は、少なくとも物理的で有形なプロセッサーと、このプロセッサーによって実行することができるコンピューター実行可能命令を有することができる物理的で有形なメモリーとを含む、任意のデバイスまたはシステム（またはこれらの組み合わせ）を含むように、広く定められる。メモリーは、任意の形態を取ることができ、計算システムの性質(nature)および形態に依存してもよい。

【０００９】

[0013] 本明細書において使用する場合、「モジュール」または「コンポーネント」という用語は、計算システムにおいて実行するソフトウェア・オブジェクトまたはルーチンを指すことができる。本明細書において説明する異なるコンポーネント、モジュール、エンジン、およびサービスは、計算システムにおいて実行するオブジェクトまたはプロセスとして実装することができる（例えば、別個のスレッドとして）。

【００１０】

[0014] 本明細書において説明する実施形態は、以下で更に詳しく説明するように、例えば、１つ以上のプロセッサーおよびシステム・メモリーというようなコンピューター・ハードウェアを含む特殊目的コンピューターまたは汎用コンピューターを含むまたは利用することができる。また、本明細書において説明する実施形態は、コンピューター実行可能命令および／またはデーター構造を伝えるまたは格納するために物理的およびその他のコンピューター読み取り可能媒体も含む。このようなコンピューター読み取り可能媒体は、汎用または特殊目的コンピューター・システム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とすることができる。コンピューター実行可能命令またはデーターを格納するコンピューター読み取り可能媒体は、物理的記憶媒体である。コンピューター実行可能命令またはデーターを伝えるコンピューター読み取り可能媒体は、送信媒体である。したがって、一例として、そして限定ではなく、本発明の実施形態は、少なくとも２つの全く異なる種類のコンピューター読み取り可能媒体、即ち、コンピューター記憶媒体および送信媒体を含むことができる。

【００１１】

[0015] コンピューター記憶媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、ＣＤ－ＲＯＭまたは他の光ディスク・ストレージ、磁気ディスク・ストレージまたは他の磁気記憶デバイス、あるいはコンピューター実行可能命令またはデーター構造の形態で所望のプログラム・コード手段を格納するために使用することができ、汎用または特殊目的コンピューター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。

【００１２】

[0016] 「ネットワーク」は、コンピューター・システムおよび／またはモジュールおよび／または他の電子デバイス間における電子データーの伝送を可能にする１つ以上のデーター・リンクとして定められる。ネットワークまたは他の通信接続（ハードワイヤ接続、ワイヤレス、あるいはハードワイヤまたはワイヤレスの組み合わせ）を介してコンピューターに情報が送られるまたは提供されるとき、コンピューターが接続を送信媒体と見なすのは適正である。送信媒体は、コンピューター実行可能命令またはデーター構造の形態で所望のプログラム・コード手段を伝えるために使用することができ、汎用または特殊目的コンピューターによってアクセスすることができるネットワークおよび／またはデーター・リンクを含むことができる。以上のものの組み合わせも、コンピューター読み取り可能媒体の範囲内に含まれてしかるべきである。

【００１３】

[0017] 更に、種々のコンピューター・システム・コンポーネントに到達したとき、コンピューター実行可能命令またはデーター構造の形態のプログラム・コード手段は、自動的に送信媒体からコンピューター記憶媒体に（またはその逆）送ることができる。例えば、ネットワークまたはデーター・リンクを介して受信されたコンピューター実行可能命令またはデーター構造を、ネットワーク・インターフェース・モジュール（例えば、「ＮＩ

Ｃ」）内にあるＲＡＭにバッファし、次いで最終的にコンピューター・システムのＲＡＭおよび／またはコンピューター・システムにおける揮発性でない(less volatile)コンピューター記憶媒体に送ることができる。したがって、コンピューター記憶媒体は、送信媒体も利用する（または主に利用する）コンピューター・システム・コンポーネントに含むことができることは理解されてしかるべきである。

【００１４】

[0018] コンピューター実行可能命令は、命令およびデーターを含み、プロセッサーにおいて実行されると、汎用コンピューター、特殊目的コンピューター、または特殊目的処理デバイスに、一定の機能または機能の一群を実行させる。コンピューター実行可能命令は、例えば、バイナリー、アセンブリ言語のような中間フォーマット命令、またはソース・コードであってもよい。主題について、構造的特徴および／または方法論的アクトに特定な文言で説明したが、添付する特許請求の範囲において定められる主題はかならずしも説明した特徴や以上で説明したアクトには限定されないことは理解されてしかるべきである。逆に、説明した特徴およびアクトは、特許請求の範囲を実現する形態例として開示される。

【００１５】

[0019] 当業者は、多くのタイプのコンピューター・システム構成を有するネットワーク計算環境において本発明が実施されてもよいことを認めよう。多くのタイプのコンピューター・システム構成には、パーソナル・コンピューター、デスクトップ・コンピューター、ラップトップ・コンピューター、メッセージ・プロセッサー、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・ベースまたはプログラマブル消費者用電子機器、ネットワークＰＣ、ミニコンピューター、メインフレーム・コンピューター、移動体電話機、ＰＤＡ、ページャー、ルーター、スイッチ等が含まれる。

【００１６】

[0020] この説明および特許請求の範囲において、「デバイス」とは分散型でない任意の計算システムとして定義される。しかしながら、本発明は、分散型システム環境において実施することもでき、ネットワークを介してリンクされたローカルおよびリモート・コンピューター・システム（ハードワイヤ結合データー・リンク、ワイヤレス・データー・リンク、またはハードワイヤ結合およびワイヤレス・データー・リンクの組み合わせのいずれかによって）、双方ともタスクを実行する。分散型システム環境では、プログラム・モジュールはローカルおよびリモート双方のメモリー記憶デバイスに配置されてもよい。

【００１７】

[0021] 図１は、計算システム１００の一例を示す。計算システム１００は、管理ドメイン１１０（または「管理レベル」）と、ローカル信頼実行環境ドメイン１２０（または「ローカル信頼実行環境レベル」）とを含む。管理ドメイン１１０は、プロセッサー１１１と主メモリー１１２とを含む。主メモリー１１２は、プロセッサー１１１の使用を介して、計算システム１００のアドミニストレーターにアクセス可能である。主メモリー１１２は、物理システム・メモリーであり、揮発性、不揮発性、またはこれら２つの何らかの組み合わせでもよい。「メモリー」という用語は、本明細書では、物理記憶媒体のような、不揮発性大容量ストレージを指すために使用される場合もある。

【００１８】

[0022] ローカル信頼実行環境ドメイン１２０は、人間のアドミニストレーターによってであっても直接アクセスすることはできない。ローカル信頼実行環境ドメイン１２０は、暗号機能１２２と被保護エリア１２３とを含むトラステッド・プラットフォーム・モジュール（ＴＰＭ）１２１を含む。ＴＰＭのコンテンツに直接アクセスするための何らかの可能な方法があるとすると、この方法は実際にＴＰＭを物理的にばらばらにスライス(slicing)または分解し、複雑な機器を使用してコンテンツを物理的に試験することを伴うであろう。つまり、ローカル信頼実行環境ドメイン１２０のコンテンツは安全である。被保護エリア１２３は、ＴＰＭ外部では読み取りできない少なくともいくつかのコンテンツを含む。しかしながら、暗号機能１２２は、被保護エリア１２３のコンテンツを使用して動

作することができる。被保護エリアは、イミュータブル・データー１２３Ａとミュータブル・データー１２３Ｂとを含む。両タイプのデーターは、暗号機能１２２によって読み取ることができる。しかしながら、ミュータブル・データー１２３Ｂのみが、暗号機能１２２によって書き込むことができる。

【００１９】

[0023] イミュータブル・データーの一例に、裏書き鍵(endorsement key)があり、これはＴＰＭに対するパスポートとして機能し、ＴＰＭの識別において製造者レベルのセキュリティを提供する。更に、従来のＴＰＭは物理的に計算システムに接続されるので、裏書き鍵は計算システム１００を安全に識別し、つまり計算システム１００に対して信頼の土台として役割を果たすことができる。

【００２０】

[0024] ミュータブル・データーの例には、他の鍵、単調カウンター(monotonic counter)、および不揮発性メモリーが含まれる。他の鍵は、プロセッサー１１１の要求に対して作られるのでもよい。単調カウンターは、ゼロから開始し、プロセッサー１１１によって要求されるとき、またはある種のイベント（システムに電源を投入するというようなイベント）に応答して増分される。鍵は、移動可能(migratable)または移動不可(non-migratable)とすることができる。移動可能鍵は、任意のＴＰＭにおいて適正な許可によって使用することができ、一方移動不可鍵はＴＰＭ１２１においてのみ使用することができる。

【００２１】

[0025] 計算システム１００は、プロセッサー１１１とＴＰＭ１２１との間で通信するためのインターフェース１３０を含む。従来のインターフェース１３０の一例に、ＴＰＭベース・サービス・モジュール（ＴＢＳ）がある。これは、ＴＰＭコマンドをプロセッサー１１１からＴＰＭ１２１に供給し、しかるべきときには、暗号処理の結果をプロセッサー１１１に供給する（しかし、勿論、ＴＰＭ１２１のコンテンツは供給しない）。

【００２２】

[0026] 図１を参照して説明したこの従来の計算システム１００は、従来通りに配備されたＴＰＭを有するが、ある種の利点および欠点を有する。例えば、従来のＴＰＭは、どちらかと言えば製造が安価であり、ローカル信頼実行環境レベルにおいて被保護エリアを提供する。しかしながら、ＴＰＭの暗号機能は、小型のＴＰＭの能力に処理が限定されるので、非常に遅いことが多い。更に、被保護エリア１２２のメモリー空間も、非常に狭いことが多く、１メガバイトよりも遙かに少ないことが多い。更に、計算システム１００またはＴＰＭ１２１が損傷を受けた場合、ＴＰＭに結合された全ての鍵、またはＴＰＭによって作られた全ての鍵が使用できなくなる。更に、従来の計算システムは、物理的にＴＰＭに結び付けられることによってのみ、ＴＰＭ機能を利用することができる。

【００２３】

[0027] ＴＰＭを含む従来の計算システムは分散されないが、「計算システム」という用語は、本明細書において使用される場合、ネットワーク環境にわたって分散されることもあり、その場合、処理、メモリー、および／または記憶能力も同様に分散されるであろう。

【００２４】

[0028] 以下に続く説明では、１つ以上の計算システムによって実行されるアクトを参照して、実施形態について説明する。このようなアクトがソフトウェアで実現される場合、そのアクトを実行する関連計算システムの１つ以上のプロセッサーが、コンピューター実行可能命令を実行したことに応答して、計算システムの動作を指令する(direct)。このような動作の例は、データーの操作を伴う。コンピューター実行可能命令（および操作されたデーター）は、計算システムのメモリーに格納することができる。

【００２５】

[0029] 図２は、本明細書において説明する原理を採用することができる環境２００を示す。具体的には、環境２００は、複数のクライアント計算システム２０１（以後「クライアント２０１」と呼ぶ）を含む。本明細書において説明する原理は、少なくとも一部の

ローカル信頼実行環境機能を、クライアントからネットワーク２０３を介してシステム２１０にオフロードすることを可能にする。従前では、ＴＰＭモジュールはローカル信頼実行環境レベルにおいて動作し、つまりクライアントに物理的に結び付けられるので、これは反直感的(counterintuitive)である。図２の場合、複数のクライアントがＴＰＭ機能をシステム２１０にオフロードすることができる。ネットワーク２０３の一例はインターネットであるが、本明細書において説明する原理は、恐らくは企業ネットワークのような、他のネットワークにも適用することができる。

【００２６】

[0030] ＴＰＭの機能は、被保護エリアおよびその読み取り不可機構(non-readability feature)をシステム２１０にエミュレートさせることによってオフロードされる。例えば、従前のＴＰＭは当該ＴＰＭの外部では読み取ることができないデーターを含む被保護エリアを有するが、システム２１０はエンティティ毎に被保護エリアを有し、この被保護エリアは、セキュリティ・プロセッサー２１３による場合を除いて、システムの外部から、またはアカウントの外部から読み取ることはできない。システム２１０は容易に侵害されず、これによって他のエンティティが被保護データーを読み取ることを許さないので、システム２１０は、被保護エリアのコンテンツの発見に対して重要なバリアを作るときに、ローカル信頼実行環境セキュリティの同等物を設ける。

【００２７】

[0031] 更に、セキュリティ・プロセッサー２１３は、ローカルＴＰＭが通常信頼実行環境コマンドに応答するのと同様に、このような信頼実行環境コマンドに応答することができる。例えば、セキュリティ・プロセッサー２１３は、鍵および／または被保護データー集合に対して暗号処理および／またはセキュリティ処理を実行することもできる。これによって、ＴＰＭの機能の多くをエミュレートすることができる。クライアントが破壊されても、ＴＰＭは引き続きシステム２１０において利用可能であり、したがって、ＴＰＭから生成された鍵および他のデーター（ＴＰＭに関連する単調カウンター、不揮発性ＲＡＭのコンテンツ等）を引き続き使用することができる。

【００２８】

[0032] 図２において、６つのクライアント２０１Ａから２０１Ｆまでが示されている。しかしながら、楕円２０１Ｇは、本明細書において説明する原理がシステム２１０に接続された特定数のクライアントに限定されるのではないことを表す。特に、ネットワーク２０３がインターネットであり、および／またはシステム２１０がクラウド計算環境である場合、たった１つであっても、潜在的に多くある可能性もある。更に、クライアント２０１の数は時の経過と共に変化することもあり得る。例えば、システム２１０がクラウド計算環境である場合、クライアント２０１の数は秒毎または分毎に変わる可能性がある。

【００２９】

[0033] この説明およびそれに続く特許請求の範囲では、「クラウド・コンピューティング」は、構成可能な計算リソース（例えば、ネットワーク、サーバ、ストレージ、アプリケーション、およびサービス）の共有プールに対してオンデマンドのネットワーク・アクセスを可能にするモデルとして定められる。「クラウド・コンピューティング」の定義は、このようなモデルが適正に配備されたときに得ることができる他の複数の利点のいずれにも限定されない。

【００３０】

[0034] 例えば、クラウド・コンピューティングは、現在構成可能な計算リソースの共有プールに対して遍在的で便利なオンデマンド・アクセスを提供するように、市場において採用されている。更に、構成可能な計算リソースの共有プールは、仮想化によって迅速にプロビジョニングすることができ、少ない管理の手間またはサービス・プロバイダーの介入で放出することができ、次いでしかるべくスケーリングすることができる。

【００３１】

[0035] クラウド・コンピューティング・モデルは、オンデマンド・セルフ・サービス

、ブロード・ネットワーク・アクセス、リソース・プーリング、すばやく(時には自動的に)スケールアウト・スケールインできる(rapid elasticity)、適切な計測により、サービスの透明性が確保される(measured service)等というような種々の特性で構成することができる。また、クラウド・コンピューティング・モデルは、例えば、サービスとしてのソフトウェア（「ＳａａＳ」）、サービスとしてのプラットフォーム（「ＰａａＳ」）、およびサービスとしてのインフラストラクチャ（「ＩａａＳ」）というような種々のサービス・モデルの形態で表すこともできる。また、クラウド・コンピューティング・モデルは、プライベート・クラウド、コミュニティ・クラウド、パブリック・クラウド、ハイブリッド・クラウド等というような、異なる配備モデルを使用して配備することもできる。この説明および特許請求の範囲において、「クラウド・コンピューティング環境とは、クラウド・コンピューティングが採用される環境のことである。

【００３２】

[0036] クライアント２０１の一部はＴＰＭを含んでもよく、一部は含まなくてもよい。例えば、図２の場合、クライアント２０１ＡはＴＰＭ２０２Ａを有し、クライアント２０１ＢはＴＰＭ２０２Ｂを有し、クライアント２０１ＥはＴＰＭ２０２Ｅを有する。クライアントの内、クライアント２０１Ｃ、２０１Ｄ、または２０１Ｆを含む他のものは、ＴＰＭを有さない。ローカル・クライアントＴＰＭが完全にＴＰＭとして実行していなくても、ＴＰＭの存在は、以下で説明するように、そのＴＰＭの一部のマシン特定機能をオフロードすることを可能にする（マシンに関連する信頼イベント履歴を供給する能力というような）。しかしながら、ＴＰＭがなくても、以下で説明するようにＴＰＭ機能の一部をなおもオフロードすることができる。

【００３３】

[0037] システム２１０は、クライアント２０１によって出された信頼実行環境コマンドを受信する受信モジュール２１１を含む。信頼実行環境コマンドは、通常はＴＰＭソフトウェア・インターフェース（ＴＢＳのような）を使用してＴＰＭに出されるが、代わりに傍受されシステム２１０にディスパッチされることによって、受信モジュール２１１によって受信される。例えば、クライアント２０１Ａから２０１Ｆまでは、このような信頼実行環境コマンドを、対応する矢印２０５Ａから２０５Ｆまでによって表されるようにディスパッチする。各信頼実行環境コマンドは、そのコマンドを出したエンティティに対応するセキュリティ・コンテキスト（例えば、キーまたはデーター）に対して動作するコマンドである。本システムは、受信モジュール２１１によって受信された信頼実行環境コマンドに応答して、暗号機能およびセキュリティ機能を実行するセキュリティ・プロセッサー２１３を含む。

【００３４】

[0038] また、システム２１０は、複数の被保護アカウント２２１を含むアカウント管理モジュール２１２も含む。図２において、アカウントは３つのアカウント２２１Ａ、２２１Ｂ、および２２１Ｃを含むが、楕円２２１Ｄは、システム２１０によって管理される任意の数のアカウントがあってもよいことを表す。各アカウントは、クライアント２０１の内１つ以上に対応し、各クライアントに対応する被保護データー集合を含む。各被保護データー集合は、ＴＰＭの被保護エリアがどのようになるか(look like)、クライアント毎にエミュレートする。しかしながら、被保護データー集合はＴＰＭの小さなエリアに限定されないので、被保護データー集合は、はるかに大きくてもよく、恐らくメガバイト、ギガバイト、またはテラバイト範囲となることもあり得る。

【００３５】

[0039] 図２において、アカウント２２１Ａは、クライアント２０１Ａに対応する被保護データー集合２２２Ａを有する。アカウント２２１Ｂは、クライアント２０１Ｂに対応する被保護データー集合２２２Ｂ、およびクライアント２０１Ｃに対応する被保護データー集合２２２Ｃを有する。アカウント２２１Ｂに対するそれぞれのクライアントは、点線のボックスで囲まれている。アカウント２２１Ｃは、クライアント２０１Ｄに対応する被

保護データー集合２２２Ｄ、クライアント２０１Ｅに対応する被保護データー集合２２２Ｅ、およびクライアント２０１Ｆに対応する被保護データー集合２２２Ｆを有する。アカウント２２１Ｃに対するそれぞれのクライアントは、破線のボックスによって囲まれている。

【００３６】

[0040] 被保護データー集合２２２は、そのコンテンツがシステムのコンテキストの外部では読み取りできず、おそらくはセキュリティ・プロセッサー２１３による場合を除いて、おそらくは対応するアカウントの外部でも読み取りできないという意味で「保護される」。一実施形態では、セキュリティ・プロセッサー２１３のインスタンスが、アカウントのコンテキストの内部で実行される。その場合、アカウント２２１Ａの内部にセキュリティ・プロセッサー２１３があり、アカウント２２１Ｂの内部に他のセキュリティ・プロセッサー２１３があり、アカウント２２１Ｃの内部に他のセキュリティ・プロセッサー２１３がある。

【００３７】

[0041] 各データー集合は、そのＴＰＭに対してメモリーの制約がない場合、対応するクライアント２０１がそのＴＰＭにおいて有することができるものの例をエミュレートする。例えば、図３は、イミュータブル・データー３０１およびミュータブル・データー３０２を含む特定のデーター集合３００を示す。例えば、イミュータブル・データー３０１は、移動不可である裏書き鍵３１１を含む。また、イミュータブル・データー３０１は、移動可能鍵３１２と、他のイミュータブル・データー３１３も含む。イミュータブル・データー３０２は、移動可能鍵３２１、移動不可鍵３２２、単調カウンター３２３、および不揮発性メモリー３２４を含む。

【００３８】

[0042] データー集合３００の全ては、以上で述べたように保護される。しかしながら、イミュータブル・データー３０１は、セキュリティ・プロセッサー２１３によってでも、変更することはできない。ミュータブル・データー３０２は、変更することができるが、セキュリティ・プロセッサー２１３の実行に応答してのみである。裏書き鍵３１１は、対応するデーター集合のアカウント内部でのみ使用できることから、移動不可鍵である。しかしながら、移動可能鍵３１２は、アカウントの外部で使用することができるが、移動可能鍵を自由に(in the clear) 読み取ることを防止する、保護された状況（他のＴＰＭまたは他の同様に構成されたアカウントにおいてというような状況）の下でないと使用できない。また、イミュータブル・データー３０１は他のデーター３１３も含むことができる。また、ミュータブル・データー３０２は、移動可能鍵３２１および移動不可鍵３２２というような、移動可能および移動不可鍵を有することもできる。また、ミュータブル・データー３０２は、増分要求に応答しておよび／または他のイベント（マシンの電源投入というような）に応答して不可逆的に増分する単調カウンターも含む。また、ミュータブル・データー３０２は、不揮発性メモリーも含むことができる。

【００３９】

[0043] 任意に、各被保護アカウント２２１Ａから２２１Ｃまでが、対応するアカウント・レベル・データー集合２２３Ａから２２３Ｃまでを含むこともできる。例えば、アカウント２２１Ａはアカウント・レベル・データー集合２２３Ａを有し、アカウント２２１Ｂはアカウント・レベル・データー集合２２３Ｂを有し、アカウント２２１Ｃはアカウント・レベル・データー集合２２３Ｃを有する。各アカウント・レベル・データー集合は、そのアカウントに関連するエンティティのいずれにも特定的ではなく、アカウント自体に対して一般的である。一例として、既存のＴＰＭ通信プロトコルを使用する場合、このようなアカウント・レベル・データーに上位ＰＣＲ（ＰＣＲ２４以上というような）を使用することができる。

【００４０】

[0044] 一例として、アカウント２２１Ｂが特定のユーザーに対応すると仮定し、アカウント・レベル・データー集合２２３Ｂがユーザーのパスワードを列挙するのでもよい。

アカウント・レベル・データー集合２２３Ｂは、アカウントに関連するイミュータブル・イベントを記録するためにも使用することができる。例えば、アカウント・レベル・データー集合２２３Ｂは、オペレーティング・システムにおける高機密機能（アカウントおよびセッション管理というような）の記録を格納するのでもよい。これは、特権を引き上げることまたはアカウントを盗むことを難しくするであろう。更に、アカウントを、例えば、ＰＣＲのような他のトラステッド・プラットフォーム・モジュール（ＴＰＭ）プロパティに結び付けることができると、ユーザーを首尾良く認証し動作状態にするための、システムの暗黙の証明が可能になる。他の例として、ユーザーは、そのユーザーがサイン・アップした一連のライセンスを格納することもできる。この場合も、この一連のライセンスはイミュータブルにすることができ、恐らくこの一連のライセンスを数学的に導くことができる１つのエントリーを使用して作ることができる。その場合、ユーザーが特定の製品に対してライセンスを有するか否かについて質問が出ても、ユーザーは具体的に答えを知ることができる。

【００４１】

[0045] したがって、説明したのは、クラウド・コンピューティング環境においてというように、被保護エリアのコンテンツの保証された不変性(immutability)をローカルＴＰＭからサーバにネットワークを介してオフロードする効果的な方法である。これは、クライアント・プロセッサーからＴＰＭに出される信頼実行環境コマンドを傍受し、これらをネットワークを介して、信頼実行環境コマンドを解釈することができるセキュリティ・プロセッサーを有するシステムにリディレクトすることによって遂行され、クライアント毎のデーター集合は、保護されるべきデーターを含む。

【００４２】

[0046] これは、ローカルな信頼実行環境レイヤのセキュリティを保存する。何故なら、被保護エリア（例えば、データー集合）は、侵入するのか非常に難しいかまたは不可能であり、被保護データーにアクセスするためにはシステム２１０の突破を絶対に(essentially)必要とするからである。システム２１０は非常に精巧であり、高いレベルのセキュリティを有するであろうから、システム２１０の突破は非常に難しいかまたは不可能であろう。このような困難さまたは不可能は、クライアント・マシン自体においてクライアントＴＰＭに侵入しようとすることの困難さまたは不可能も超えるであろう。したがって、ローカルな信頼実行環境セキュリティが保存される。クライアントからシステム２１０に情報が伝達されることもあるが、このような情報は信頼実行環境コマンドだけであり、データー集合において保護された実際のデーターではない。したがって、ある人がこのようなトラフィックを読み取ることができても、被保護データーは保護されたままである。実施形態では、クライアント・プロセッサーとシステム２１０との間に信頼関係が存在すれば、ネットワーク・トラフィックでさえも暗号化されてもよい。このようなことは、コマンドを自由に送信することに関連するセキュリティ問題がある場合にも役に立つであろう。このような信頼関係は、例えば、クライアントがプロビジョニングされる時点で、自動的に開始することができる。

【００４３】

[0047] 追加の利点として、メモリー空間がもはや小さいチップに限定されないので、利用可能なメモリーの量を大幅に増やすことができる。更に、処理パワーはもはや小さいＴＰＭチップに限定されないので、暗号プロセスを遙かに効率的に実行することができ、および／または一層複雑にすることができる。また、被保護エリアはもはやクライアントに物理的に結合されないので、クライアントが破壊された場合、被保護エリアからのデーターを使用して作られた鍵を使用し続けることができる。

【００４４】

[0048] 他の形態について説明する前に、信頼実行環境コマンドの処理に関連する一般的な処理フローについて、ここで説明する。具体的には、図４は信頼実行環境コマンドを処理する方法４００のフローチャートを示す。一例として、信頼実行環境コマンドは、任意のＴＰＭコマンドでよく、任意の既存のプロトコル（ＴＰＭバージョン１．２およびＴ

ＰＭバージョン２．０）に準拠するのでもよく、あるいは今後のＴＰＭプロトコルまたはローカル信頼実行環境レイヤとの通信を容易にする任意のプロトコルに準拠するのでもよい。方法４００のアクトの内一部は、「クライアント」という見出しの下において図４の右側の列に示されるように、クライアント（例えば、クライアント２０１Ａ）によって実行される。これらのアクトの他のものは、「システム」という見出しの下において図４の中央の列に示されるように、システム２１０によって実行される。他のアクトは、「セキュリティ動作」という見出しの下において、図４の左側の列に示されるように、セキュリティ・プロセッサー２１３によって実行される。

【００４５】

[0049] このプロセスは、クライアントが信頼実行環境コマンドを出すときに開始する（アクト４０１）。クライアントにおけるローカルＴＰＭにディスパッチされることの代わりに、またはそれに加えて、信頼実行環境コマンドは、解釈され（アクト４０２）、システムにディスパッチされる（アクト４０３）。

【００４６】

[0050] 次いで、本システムは信頼実行環境コマンドを受信し（アクト４１１）、この信頼実行環境コマンドを出したクライアントに関連するアカウントを識別し（アクト４１２）、クライアントに関連するデーター集合を識別し（アクト４１３）、実行すべき動作を識別する（アクト４１４）。次いで、動作を実行するようにセキュリティ・プロセッサーに命令し（アクト４１５）、次いでセキュリティ・プロセッサーが、識別されたアカウントの識別されたデーター集合に対して動作を実行する（アクト４２１）。

【００４７】

[0051] 未だ述べていないＴＰＭの機能の内の１つは、対応するクライアントのパワー・サイクル（power cycle）を検出する能力を拠り所とする。これは、ＴＰＭが停電および給電の復旧を検出することができるように、ＴＰＭが対応するクライアント内部で結合され、クライアントの電源にハードワイヤ接続される理由の１つである。パワー・サイクルを検出する理由の１つは、ＴＰＭが、停電および給電の復旧を体験したときに、被保護データー内部にあるデーターの一部をリセットすることができるようにすることである。場合によっては、ＴＰＭ内部におけるマシン特定データーの一部の信頼性が、パワー・サイクルについて知ることを拠り所とする。

【００４８】

[0052] パワー・サイクルによってリセットすべきデーターの一例に、プラットフォーム・イベント・ログがある。典型的なＴＰＭでは、イベント・ログは１つのエントリーとして表される。新たな対象イベント（例えば、ソフトウェアのロード、ソフトウェアの実行開始）が発生したときにはいつでも、このイベントは直前のエントリーと結び付けられ、ハッシュされ、次いでエントリーの新たな値として格納される。古いエントリーからの情報（即ち、以前のイベント）が保存されるようにこれが行われる場合、プラットフォームにおいて発生した一連のイベントを再生するために、エントリーを数学的に評価することができる。これから、プラットフォームの完全性を証明することができる。

【００４９】

[0053] しかしながら、システム２１０は物理的にクライアント２０１のいずれとも結合されていないが、代わりにネットワークを介して通信するので、それぞれのクライアント２０１の内いずれかがパワー・サイクルを体験したか否か判断するのは、システム２１０には難しい。それにもかかわらず、クライアントがＴＰＭを有する場合、このＴＰＭは、パワー・サイクルが起こったことを推論できるのに丁度十分な情報を追跡することができる。これは、信頼実行環境コマンドがローカルＴＰＭに与えられず、代わりに傍受されてシステム２１０にディスパッチされるのであれば、ローカル・クライアントＴＰＭが完全に機能していなくても可能である。例えば、図２において、クライアント２０１Ａは、ＴＰＭ２０２Ａを含むように示され、クライアント２０１ＢはＴＰＭ２０２Ｂを含むように示され、クライアント２０１ＥはＴＰＭ２０２Ｅを含むように示されている。

【００５０】

[0054] この場合、アカウント管理モジュール２１２および／またはシステム２１０は、全体として、所与のクライアントにインストールされたローカル・クライアントＴＰＭと通信することによって、そのクライアントがリブートされたことを検出することができる（例えば、クライアント２０１Ａの場合、ＴＰＭ２０２Ａと通信する）。例えば、システム２１０は、パワー・サイクルが起こったことを示す暗号文(cryptographic statement)をクライアント２０１Ａから受信することができる。これを行うことができる方法は複数ある。

【００５１】

[0055] 第１の例では、システム２１０およびローカル・クライアントＴＰＭは、パワー・サイクル時にリセットされるレジスタに関連するＰＣＲ値をシステム２１０が受信するように、通信することができる。次いで、システム２１０は、システムにおける被保護データー内にあるＰＣＲの現在値を、ローカル・クライアントＴＰＭにおけるＰＣＲの値と比較し、パワー・サイクルが生じたか否か推論することができる。

【００５２】

[0056] 第２の例では、ローカル・クライアントＴＰＭが、クライアントの電力投入毎に、短期鍵 (ephemeral key)を作り、次いで通信するためにこの短期鍵の使用をクライアント・プロセッサーとネゴシエートすることができる。システム２１０は、通信を追跡しているので、この短期鍵を把握している。システム２１０がもはや通信を理解できないことを検出した場合、短期鍵が変化したに違いなく、クライアントにパワー・サイクルが生じたことを暗示する。

【００５３】

[0057] 代替実施形態では、システム２１０におけるＴＰＭがなくても、システム２１０のパワー・サイクルを検出することができる。例えば、これは、クライアント・システムのパワー・サイクル(cycling)を監視することができるシステム・モニターを有することによって遂行することができる。このようなシステム・モニターの非限定的な例に、MICROSOFT（登録商標）のSystem Center Virtual Machine Monitor（または SCVMM）がある。

【００５４】

[0058] システム２１０は、新たなクライアントがアカウントに追加されたときはいつでも、被保護データー集合を所与のアカウントに追加することができる。例えば、特定のアカウントに関連して通信が検出され、この通信が認識されていないクライアントからであることをこの通信が何らかの方法で示すとき、新たなデーター集合をそのアカウントに追加することができる。つまり、例えば、クライアントが暗号鍵を使用してシステムと通信すると仮定すると、認識されていない暗号鍵を使用する通信が到達した場合、恐らく新たなクライアントが追加されている(has been added)。同様に、あるアカウントの被保護データー集合は、対応するクライアントがもはやそのアカウントにおいて動作しなくなった後には削除してもよい。例えば、ある時間期間（恐らく年単位）使用されていない被保護データー集合がアカウントから削除されるガベージ・コレクション・アクションがあってもよい。

【００５５】

[0059] ポリシー・モジュール２１４は、クライアントに対応する被保護データー集合の１つ以上のデーター・フィールドに関して判断基準が満たされたか否かに依存して、クライアントによるアクションを許可する役割を担うことができる。あるいはまたは加えて、ポリシー・モジュール２１４は、アカウント・レベルのデーター集合の１つ以上のデーター・フィールドに関して判断基準が満たされたか否かに依存して、アカウントに関連する任意のクライアントによるアクションを許可する役割を担うこともできる。被保護データー集合に関連するメモリーは、ローカルＴＰＭと比較すると著しく増大させることができるという事実と組み合わせて、これはかなりの発展性(significant possibilities)を実現可能にする(enable)。

【００５６】

[0060] 例えば、所与のクライアントの被保護データー集合が、当該クライアントの復元状態のイメージ全体を含むと仮定する（例えば、オペレーティング・システム、任意の標準的アプリケーション、標準的構成設定等）。このクライアントが失われたまたは損傷を受けた場合、そのアカウントにおける他のクライアントがこのイメージにアクセスし、一定のポリシーが満たされることを条件に、新たなクライアントにこのイメージをインストールすることができる。このようなポリシーは、不正にクライアントの復元状態を得ることに対して保護されることを意図している。

【００５７】

[0061] また、システム２１０は、移動不可鍵（例えば、アカウント外部では使用することができない鍵）を使用して、そのアカウントに特定的であり、したがってそのアカウントに関連するクライアントの内任意のものによって使用することができる証明書を生成する証明書管理モジュール２１５も含むことができる。つまり、各クライアントは証明書に基づく認証に関与するためにそれ自体の証明書を作る必要がない。

【００５８】

[0062] 本発明は、その主旨や本質的な特性から逸脱することなく、他の具体的な形態で具体化することもできる。以上で説明した実施形態は、いかなる観点においても、限定ではなく例示として見なされてしかるべきである。したがって、本発明の範囲は、以上の説明ではなく、添付する特許請求の範囲によって示されるものとする。特許請求の範囲の意味および均等の範囲に該当する全ての変更は、その範囲内に含まれるものとする。

【図１】

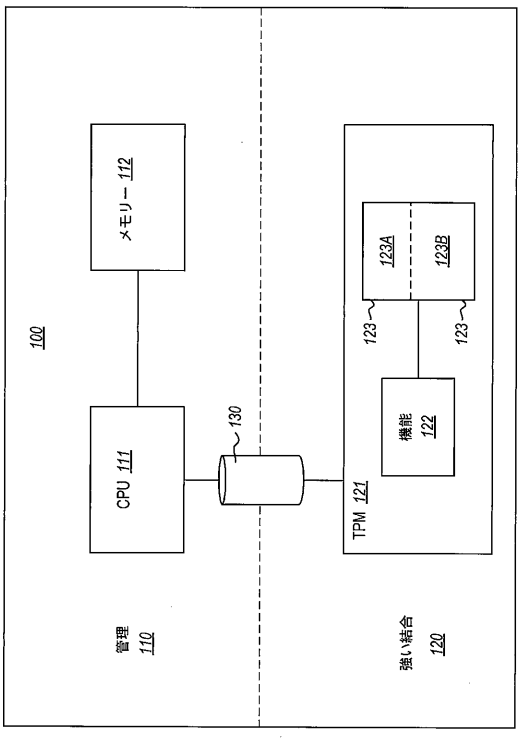

Figure 1

【図２】

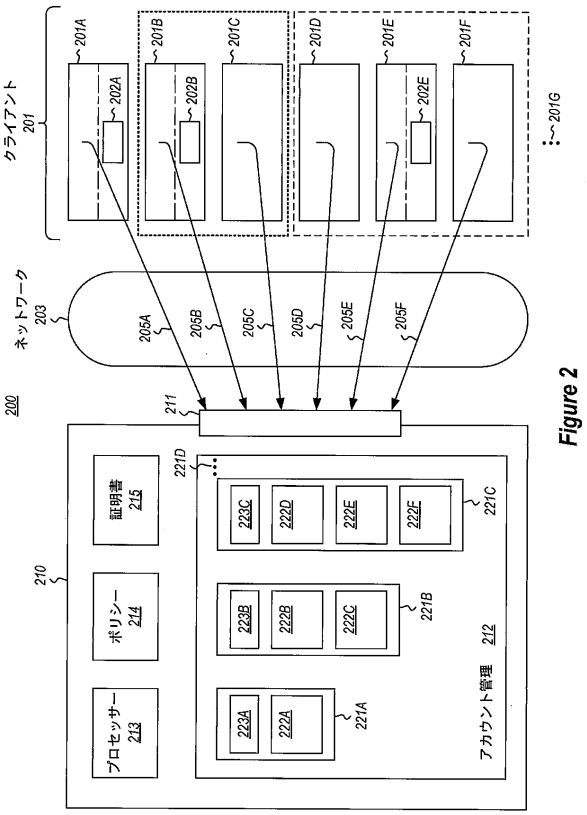

Figure 2

【図３】

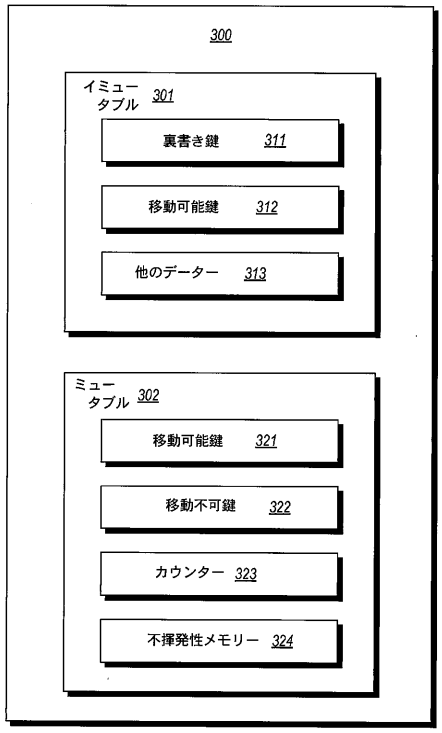

Figure 3

【図４】

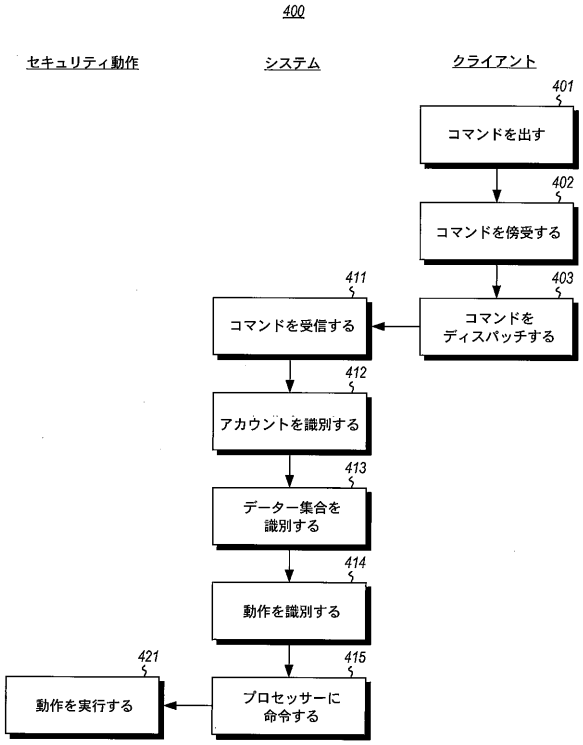

Figure 4

フロントページの続き

(72)発明者　ノヴァック，マーク・エフ
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　レイマン，アンドリュー・ジョン
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，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　ナイストローム，マグナス
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　トム，ステファン
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，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　青木　重徳

(56)参考文献　米国特許出願公開第２００７／０３０００６９（ＵＳ，Ａ１）
特表２００２－５１３９６１（ＪＰ，Ａ）
特開２０１１－２５８１９９（ＪＰ，Ａ）
米国特許出願公開第２００８／００４６８９８（ＵＳ，Ａ１）
米国特許出願公開第２００７／００７９１２０（ＵＳ，Ａ１）
田坂　和之　ほか，ネットワークサービスを非常時にも継続提供するためのアカウント提供・管理方式の実装と評価，情報処理学会第７３回（平成２３年）全国大会講演論文集（３），日本，一般社団法人情報処理学会，２０１１年　３月　２日，１Ｅ－４，ｐ．３－５９～３－６０

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１２／１４
Ｇ０６Ｆ　２１／５７
Ｇ０６Ｆ　２１／６２