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

特許第4860856号
(P4860856)

(45)発行日　平成24年1月25日(2012.1.25)　(24)登録日　平成23年11月11日(2011.11.11)

(51)Int.Cl.		F I		
G06F 11/34	(2006.01)	G06F	11/34	L
G06F 11/30	(2006.01)	G06F	11/30	305J
G06F 21/22	(2006.01)	G06F	9/06	660N
G06F 21/00	(2006.01)	G06F	15/00	330Z
G06F 9/445	(2006.01)	G06F	9/06	640A

請求項の数 5　(全 38 頁)

(21)出願番号　特願2001-500934 (P2001-500934)
(86)(22)出願日　平成12年5月25日 (2000.5.25)
(65)公表番号　特表2003-501716 (P2003-501716A)
(43)公表日　平成15年1月14日 (2003.1.14)
(86)国際出願番号　PCT/GB2000/002004
(87)国際公開番号　WO2000/073880
(87)国際公開日　平成12年12月7日 (2000.12.7)
審査請求日　平成19年5月25日 (2007.5.25)
(31)優先権主張番号　99304165.6
(32)優先日　平成11年5月28日 (1999.5.28)
(33)優先権主張国　欧州特許庁 (EP)

(73)特許権者　398038580
ヒューレット・パッカード・カンパニー
HEWLETT-PACKARD COMPANY
アメリカ合衆国カリフォルニア州パロアルト　ハノーバー・ストリート　3000
(74)代理人　100087642
弁理士　古谷　聡
(74)代理人　100063897
弁理士　古谷　馨
(74)代理人　100076680
弁理士　溝部　孝彦

最終頁に続く

(54)【発明の名称】コンピュータ装置

(57)【特許請求の範囲】
【請求項１】
コンピュータ装置であって、
データプロセッサと少なくとも１つのメモリ装置を有するコンピュータプラットフォームと、
データプロセッサ及び少なくとも１つのメモリ装置とを有するトラステッドコンポーネントと、
前記コンピュータプラットフォーム上で発生する複数のイベントを監視するためのソフトウェアエージェントを有し、
前記トラステッドコンポーネントの前記データプロセッサ及び前記少なくとも１つのメモリ装置は、前記コンピュータプラットフォームの前記データプロセッサ及び前記少なくとも１つのメモリ装置とは物理的かつ論理的に別個のものであり、前記トラステッドコンポーネントは、前記コンピュータプラットフォームで発生するイベントを記述するイベントデータを前記ソフトウェアエージェントから受け取るためのイベントロギングコンポーネントを有し、
前記ソフトウェアエージェントは、前記コンピュータプラットフォームで発生する少なくとも１つのイベントを監視して、該イベントを前記トラステッドコンポーネントに報告し、前記イベントロギングコンポーネントは、前記イベントデータを暗号化されたセキュアなイベントデータに編集するように構成され、

前記ソフトウェアエージェントは、通常は、前記トラステッドコンポーネントの前記少なくとも１つのメモリ装置に常駐しているプログラムコードを有し、前記コンピュータ装置は、前記コンピュータプラットフォームのプロセッサで該プログラムコードを実行するために該プログラムコードを前記トラステッドコンポーネントから前記コンピュータプラットフォームに送るように構成され、

前記トラステッドコンポーネントは、

i)前記トラステッドコンポーネントの前記少なくとも１つのメモリ装置から前記ソフトウェアエージェントを周期的間隔で再送することと、

ii) 前記コンピュータプラットフォーム上で動作している前記ソフトウェアエージェントが前記トラステッドコンポーネントによる問合せに対して正しく応答しているか否かをチェックすることによって、該ソフトウェアエージェントを定期的に監視すること

とのいずれかまたは両方を行うように構成されてなる、コンピュータ装置。

【請求項２】

前記トラステッドコンポーネントが、対話型表示を生成するためのディスプレイインターフェースを備える、請求項１のコンピュータ装置であって、該ディスプレイインターフェースが、

前記コンピュータプラットフォームの監視されるエンティティを選択するための手段と、

監視される少なくとも１つのイベントを選択するための手段

を備えることからなる、コンピュータ装置。

【請求項３】

前記トラステッドコンポーネントに、ユーザによって前記イベントの監視を開始すべき指示がなされたことを知らせるための、前記トラステッドコンポーネントに接続され、前記コンピュータプラットフォームから独立した、確認キー手段を更に備える、請求項１または２のコンピュータ装置。

【請求項４】

前記ソフトウェアエージェントが前記コンピュータプラットフォームの論理エンティティで発生するイベントを監視するように構成され、該エンティティが、

少なくとも１つのデータファイルと、

少なくとも１つのアプリケーションと、

少なくとも１つのドライバコンポーネント

からなる組から選択される、請求項１乃至３のいずれかのコンピュータ装置。

【請求項５】

前記プログラムコードは、前記コンピュータプラットフォームの前記少なくとも１つのメモリ装置に格納され、該メモリ装置から読み出されて実行される第１のコンピュータプログラムであり、前記トラステッドコンポーネントは、第２のコンピュータプログラムを該トラステッドコンポーネントの前記少なくとも１つのメモリ装置から読み出して、該トラステッドコンポーネントのデータプロセッサにより実行することによって、前記i)とii)のいずれか又は両方を実施するように構成されてなる、請求項１のコンピュータ装置。

【発明の詳細な説明】

【０００１】

［技術分野］

本発明は、コンピュータプラットフォームのセキュリティ監視に関し、特に、コンピュータプラットフォーム上のデータファイル、アプリケーション、ドライバ等のエンティティで発生するイベントおよび動作の監視（これらに限定するわけではないが）に関する。

【０００２】

［背景技術］

今までの従来技術による大量市場コンピューティングプラットフォームには、周知のパーソナルコンピュータ（ＰＣ）およびApple Macintosh（R）等の競合する製品と、急増する周知のパームトップおよびラップトップパーソナルコンピュータなどがある。概して、か

かるマシンの市場は、家庭用すなわち一般消費者向けと法人向けの２つのカテゴリに分類される。家庭用すなわち一般消費者向けのコンピューティングプラットフォームに対する一般的な要件には、比較的高い処理パワー、インターネットアクセス機能、及び、コンピュータゲームを処理するマルチメディア機能がある。このタイプのコンピューティングプラットフォームでは、Microsoft Windows（R）'95および'98オペレーティングシステム製品とIntelプロセッサが、市場で優位を占めている。

【０００３】

一方、ビジネス向けでは、中小企業から多国籍企業までに及び企業をターゲットとした、非常に多くの工業所有権によって保護されたコンピュータプラットフォームが利用可能である。これらのアプリケーションの多くにおいて、サーバプラットフォームは、集中型データ記憶機構と、複数のクライアントステーション用のアプリケーション機能と、を提供する。ビジネス向けでは、他の重要な基準は、信頼性と、ネットワーキング機能と、セキュリティ機能と、である。かかるプラットフォームとして、Microsoft Windows NT 4.0（R） オペレーティングシステムが、Unix（R）オペレーティングシステムと共に一般的である。

【０００４】

「ｅ－コマース(電子商取引)」として知られている、インターネットにより取引が行われる商業活動の増加に伴い、従来技術では、インターネットによりコンピューティングプラットフォーム間のデータのトランザクションを可能にすることに対し多くの関心がもたれてきた。しかしながら、従来方式においては不正行為及び電子データの操作の可能性があるため、十分に透明で効率的な市場が要求されるに従って、広範囲に及ぶ遠隔の未知の相手とのトランザクションを完全に自動化することは、これまでためらわれてきた。基本的な問題は、かかるトランザクションを作成するために対話（または相互作用）するコンピュータプラットフォーム間の信頼の問題である。

【０００５】

コンピュータプラットフォームのセキュリティおよび信頼性を向上させることを目指す、従来技術による方式がいくつかある。大部分、これらは、アプリケーションレベルでセキュリティ機能を付加することに基づいている。すなわち、セキュリティ機能は、オペレーティングシステムのカーネルに本来的に組込まれておらず、コンピューティングプラットフォームの基本ハードウェアコンポーネントに組込まれていない。市場にはすでに、ユーザ固有のデータを有するスマートカードを備えたポータブルコンピュータ装置が現れている。かかるデータは、コンピュータのスマートカードリーダに入力される。目下、かかるスマートカードは、従来からのパーソナルコンピュータに対するアドオンエキストラのレベルにあり、場合によっては、既知のコンピュータのケーシングに組み込まれている。これらの従来技術の方式は、コンピュータプラットフォームのセキュリティを向上させるためにいくらか助けとなるが、従来技術の方式によって得られるセキュリティおよび信頼性のレベルは、コンピュータプラットフォーム間の自動化されたトランザクションの広範な用途を可能にするためには不十分であると考えられる。ビジネスは、非常に価値のあるトランザクションを広い規模で電子商取引に対して晒す前に、基礎をなすテクノロジのにより大きな信頼性を要求するであろう。

【０００６】

本出願人による同時係属国際特許出願である、２０００年２月１５日出願の「Trusted Computing Platform」と題されたＰＣＴ／ＧＢ００／００５２８と、２０００年３月３日出願の「Smartcard User Interface for Trusted Computing Platform」と題されたＰＣＴ／ＧＢ００／００７５２において、組込みハードウェアおよびソフトウェアコンポーネントの形態の「トラステッド（信頼された）コンポーネント」を有するコンピューティングプラットフォームからなる「トラステッドコンピューティングプラットフォーム」の概念が開示されている。尚、これらの出願の全開示内容はこの引用をもって本明細書に組み込まれているものとする。このようなトラステッドコンポーネントがそれぞれに提供される２つのコンピューティングエンティティは、高度の「信頼」を持って互いに対話すること

ができる。すなわち、第１および第２のコンピューティングエンティティが互いに対話する場合、トラステッドコンポーネントがまったく存在しない場合に比べて対話のセキュリティが向上される。それは、以下の理由による。
・コンピューティングエンティティのユーザは、自身のコンピュータエンティティの完全性およびセキュリティ、および他のコンピューティングエンティティに属するコンピュータエンティティの完全性およびセキュリティを、より高く信頼する。
・各エンティティは、他方のエンティティが実際にそうであると主張するエンティティであることを確信する。
・トラステッドコンポーネントが組込まれているため、エンティティの一方または両方がトランザクション、例えばデータ転送トランザクションに対するパーティを表す場合、エンティティと対話するサードパーティエンティティは、そのエンティティが実際にかかるパーティを表すことを高く信頼する。
・トラステッドコンポーネントは、それが実施する検査および監視プロセスにより、エンティティ自体の固有のセキュリティを強化する。
・コンピュータエンティティは、予期されるように振舞う可能性がより高い。

【０００７】

従来技術によるコンピューティングプラットフォームには、本出願人の上述したトラステッドコンポーネントの概念を具現化するために、解決する必要のある問題がいくつかある。具体的には、
・コンピュータシステムまたはプラットフォームの動作状態と、プラットフォームまたはシステム内のデータの状態は、動的であり予測することが困難である。コンピュータプラットフォームおよびプラットフォーム上のデータの状態が絶えず変化しており、コンピュータプラットフォーム自体が動的に変化している場合があるため、コンピュータプラットフォームが正しく動作しているかを判断することが困難である。
・セキュリティの観点から、特定のクライアントプラットフォームでは、市販のコンピュータプラットフォームが、無許可の変更を受けやすい環境においてしばしば置かれる。変更を受ける主な範囲には、ユーザによってロードされるソフトウェアによるかまたはネットワーク接続を介してロードされるソフトウェアによる変更が含まれる。限定するわけではないが、具体的には、従来のコンピュータプラットフォームは、悪質の程度によるが、ウイルスプログラムによる攻撃に対して脆弱な場合がある。
・コンピュータプラットフォームがアップグレードされるか、それらの機能が、物理的変更、すなわちハードディスクドライブ、周辺機器ドライバ等のコンポーネントの追加または削除により、拡張または制限される場合がある。

【０００８】

コンピュータシステムにおいて、オペレーティングソフトウェアに組込まれたいくつかのセキュリティ機能を提供することは既知である。これらのセキュリティ機能は、第一に、システムのユーザのコミュニティ内で情報を分配することを目指している。

【０００９】

周知のMicrosoft Windows NT 4.0（R）オペレーティングシステムには、プラットフォーム内で発生するイベントのログを、Windows NTオペレーティングシステムソフトウェアを使用しているシステム管理者が検査することができるイベントログデータファイルに記録する「システムログイベントビューア」と呼ばれる監視機能もある。この機能は、システム管理者が予め選択されたイベントのセキュリティを監視することを可能にするためにいくらか助けになる。Windows NT 4.0(R)オペレーティングシステムのイベントロギング機能は、システム監視の一例である。

【００１０】

しかしながら、コンピュータプラットフォームのセキュリティ全体という意味で、純粋にソフトウェアベースのシステムは、例えばウイルスによる攻撃に対し脆弱である。Microsoft Windows NT 4.0（R）ソフトウェアは、既知のウイルスを捜すよう予め設定された対ウイルス保護ソフトウェアを含む。しかしながら、ウイルス菌は絶えず新たに発生してお

り、対ウイルス保護ソフトウェアは未知のウイルスに対しては役に立たない。

【００１１】

更に、コンピュータエンティティのための従来技術による監視システムは、管理者がネットワーク管理ソフトウェアを使用して複数のネットワークコンピュータのパフォーマンスを監視する、ネットワーク監視機能に焦点を合せる。また、システムの信頼は、システムのコンピュータプラットフォームの各ハードウェアユニットの個々の信頼のレベルでは存在しない。

【００１２】

［発明の概要］

本発明の特定の実施態様は、コンピュータプラットフォームとは物理的かつ論理的に異なるトラステッド（信頼された）コンポーネントを有するコンピュータプラットフォームを提供する。トラステッドコンポーネントは、偽造不可能性(unforgability)とそれが関連するコンピュータプラットフォームからの自律性(autonomy)という特性を有する。トラステッドコンポーネントは、コンピュータプラットフォームを監視し、それにより、ネットワーク監視またはシステム監視レベルより下のレベルで、個々のベースで監視されるコンピュータプラットフォームを提供することができる。複数のコンピュータプラットフォームが、ネットワーク化されるか、またはシステムに含まれる場合、各コンピュータプラットフォームに、別々の対応するそれぞれのトラステッドコンポーネントを設けることができる。

【００１３】

本発明の特定の実施態様は、コンピュータプラットフォームに存在する異質なエージェントによっては、または、コンピュータプラットフォームのユーザによっては破損され得ないようにして、イベントログの破損が発生した場合にそれがただちに明らかとなるような方法で、コンピュータプラットフォームで発生するイベントを監視する安全な方法を提供することができる。

【００１４】

本発明の第１の態様によれば、データプロセッサと少なくとも１つのメモリ装置とを有するコンピュータプラットフォームと、該コンピュータプラットフォームの該データプロセッサおよびメモリとは物理的にかつ論理的に異なるデータプロセッサと少なくとも１つのメモリ装置とを有するトラステッドコンポーネントと、該コンピュータプラットフォーム上で発生する複数のイベントを監視する手段と、を備えるコンピュータエンティティが提供される。

【００１５】

好ましくは、上記監視手段は、上記コンピュータプラットフォーム上で発生する少なくとも１つのイベントを監視し、該イベントを上記トラステッドコンポーネントに報告する、該コンピュータプラットフォーム上で動作するソフトウェアエージェントを備える。上記ソフトウェアエージェントは、上記トラステッドコンポーネントの上記メモリ装置に通常常駐する１組のプログラムコードを備え、該コードは、上記コンピュータプラットフォーム上で監視機能を実行するために該コンピュータプラットフォームに転送される。

【００１６】

好ましくは、上記トラステッドコンポーネントは、上記コンピュータプラットフォーム上で発生する複数のイベントを記述するデータを受取り、該イベントデータをセキュア（安全）なイベントデータに編集（またはコンパイル）する、イベントロギングコンポーネントを備える。好ましくは、上記イベントロギングコンポーネントは、連鎖機能を上記イベントデータに適用することにより上記セキュアなイベントデータを作成する手段を備える。

【００１７】

監視されるイベントおよびエンティティの選択は、監視される上記コンピュータプラットフォームのエンティティを選択する手段と、監視される少なくとも１つのイベントを選択する手段と、を有する対話型表示を生成するディスプレイインタフェースを動作させるこ

とによって、ユーザが行うようにしてもよい。

【００１８】

監視手段は、少なくとも１つの選択されたパラメータの将来値を予測する予測手段を更に備えていてもよい。

【００１９】

好ましくは、コンピュータエンティティは、上記トラステッドコンポーネントに対しユーザの認証信号を確認するための、上記トラステッドコンポーネントに接続され、上記コンピュータプラットフォームから独立した、確認キー（確認鍵）手段を更に備える。

【００２０】

監視されるエンティティには、データファイル、アプリケーションまたはドライバコンポーネントを含めることができる。

【００２１】

本発明の第２の態様によれば、第１のデータプロセッサと第１のメモリ装置を有するコンピュータプラットフォームと、第２のデータプロセッサと第２のメモリ装置を有するトラステッド監視コンポーネントとを備えたコンピュータエンティティであって、上記トラステッド監視コンポーネントは、上記第２のメモリ領域に常駐するエージェントプログラムを格納し、該エージェントプログラムは、上記第１のデータプロセッサの制御の下で上記トラステッドコンポーネントの代りに機能を実行するために上記第１のメモリ領域にコピーされる、コンピュータエンティティが提供される。

【００２２】

本発明の第３の態様によれば、第１のデータプロセッサと第１のメモリ装置とを有するコンピュータプラットフォームと、第２のデータプロセッサと第２のメモリ装置とを有するトラステッド監視コンポーネントと、上記第１のメモリ領域に常駐し上記第１のデータプロセッサを動作させ、上記コンピュータプラットフォームの動作に関するイベントを上記トラステッド監視コンポーネントに報告し返す第１のコンピュータプログラムと、上記トラステッドコンポーネントの上記第２のメモリ領域に常駐し、上記第１のプログラムの完全性を監視するように動作する第２のコンピュータプログラムと、を備えるコンピュータエンティティが提供される。

【００２３】

上記コンピュータプログラムは、上記第１のコンピュータプログラムに複数の問合せメッセージを送信し、該第１のコンピュータプログラムによって作成される該問合せメッセージに対する応答を監視することにより、該第１のコンピュータプログラムの完全性を監視することができる。好ましくは、上記問合せメッセージは、第１のフォーマットで送信され、セキュアなフォーマットである第２のフォーマットで返される。

【００２４】

本発明の第４の態様によれば、第１のデータプロセッサと第１のメモリ手段とを備えるコンピュータプラットフォームを監視する方法であって、コンピュータプラットフォームを構成する少なくとも１つの論理または物理エンティティ上で発生するイベントを記述するイベントデータを読出すステップと、関連する第２のメモリ領域を有する第２のデータ処理手段において上記イベントデータを安全なものにするステップとからなり、該第２のデータ処理手段と該第２のメモリ領域は、上記第１のデータ処理手段と上記第１のメモリ領域とは物理的かつ論理的に異なるものであり、該セキュアなイベントデータが変更されると必ずかかる変更が明らかになるようにする方法が提供される。

【００２５】

監視される上記イベントは、データファイルのコピー、データファイルの保存、データファイルのリネーム、データファイルのオープン、データファイルのオーバライト、データファイルの変更、データファイルの印刷、ドライバデバイスの起動、ドライバデバイスの再構成、ハードディスクドライブへの書込み、ハードディスクドライブの読出し、アプリケーションのオープン、アプリケーションのクローズといったイベントの組から選択することができる。監視される上記エンティティは、上記コンピュータプラットフォーム上に

格納される少なくとも１つのデータファイル、該コンピュータプラットフォームのドライバデバイス、該コンピュータプラットフォーム上に常駐するアプリケーションプログラムといった組から選択することができる。

【００２６】

エンティティを、予め選択された期間に亙って連続的に監視するか、または、予め選択されたイベントがエンティティ上で発生する時まで監視することができる。エンティティを、所定の時間が経過するまで選択されたイベントについて監視することができる。

【００２７】

本発明は、第１のデータ処理手段と第１のメモリ手段とを備えるコンピュータプラットフォームを監視する方法であって、上記コンピュータプラットフォームを構成する少なくとも１つのエンティティを選択する選択するための対話型表示を生成するステップと、監視することができるイベントの表示を生成するステップと、上記コンピュータプラットフォームのエンティティの表示を生成するステップと、少なくとも１つの上記エンティティを選択するステップと、少なくとも１つの上記イベントを選択するステップと、該イベントについて上記エンティティを監視するステップとからなる方法を含む。

【００２８】

本発明は、第１のデータ処理手段と第１のメモリ手段とを備えるコンピュータプラットフォームを監視する方法であって、前記第１のメモリ領域とは物理的および論理的に異なる第２のメモリ領域に監視プログラムを格納するステップと、該監視プログラムを該第２のメモリ領域から上記第１のメモリ領域に転送するステップと、上記コンピュータプラットフォーム内部からの該コンピュータプラットフォームの少なくとも１つのエンティティを監視するステップと、上記監視プログラムからのイベントデータを上記第２のデータプロセッサに報告するステップとからなる方法を含む。

【００２９】

本発明は、第１のデータ処理と第１のメモリ手段とを備えるコンピュータプラットフォームを監視する方法であって、該コンピュータプラットフォーム内部からの該コンピュータプラットフォームを構成する少なくとも１つのエンティティを監視するステップと、該コンピュータプラットフォームで発生する複数のイベントを記述するイベントデータを生成するステップと、該イベントデータを、関連する第２のメモリ手段を有する第２のデータ処理手段に報告するステップと、該イベントデータをセキュアなフォーマットに処理するステップとからなる方法を含む。

【００３０】

本発明をよりよく理解するため、および本発明がいかにして実現され得るかを示すために、以下で、添付図面を参照して本発明による特定の実施態様、方法およびプロセスを例示的に説明する。

【００３１】

［本発明を実施するための最良形態の詳細な説明］

本発明者によって考えられた本発明を実施するための最良の形態を、代替的な実施の形態と共に例示的に説明する。以下では、本発明について十分な理解がなされるように、多数の特定の細部について説明する。しかしながら、当業者には、これら特定の細部に限定されることなく本発明を実施できるということは明らかであろう。尚、本発明を不必要に不明瞭にしないように、周知の方法および構成については詳細には説明していない。

【００３２】

本発明の特定の実施態様は、処理手段とメモリ手段とを有するコンピュータプラットフォームと、物理的にコンピュータプラットフォームと関連付けられ、コンピュータプラットフォームからメトリクスデータを収集することにより、コンピュータプラットフォームの動作を監視し、コンピュータプラットフォームと対話している他のエンティティに対し、コンピュータプラットフォームが正しく機能していることを検証することができる、以降「トラステッド（信頼される）コンポーネント」（またはトラステッド装置）と呼ぶ監視コンポーネントと、を備える。かかるシステムは、２０００年２月１５日に出願された、

「Trusted Computing Platform」と題する本出願人の同時係属国際特許出願ＰＣＴ／ＧＢ００／００５２８に記載されている。尚、本出願の全開示内容はこの引用をもって本明細書に組み込まれたものとする。コンピュータプラットフォームのユーザに対して個別的なトークンデバイスは、コンピュータプラットフォームに関連するトラステッドコンポーネントと対話することにより、ユーザに対しコンピュータプラットフォームの信頼性を検証する。適切なトークンデバイスおよびシステムは、２０００年３月３日に出願された、「Smartcard User Interface for Trusted Computing Platform」と題する本出願人の同時係属国際特許出願ＰＣＴ／ＧＢ００／００７５２に記載されている。尚、本出願の全開示内容はこの引用をもって本明細書に組み込まれたものとする。

【００３３】

コンピューティングエンティティのユーザは、かかるトラステッドトークンデバイスを使用することにより、コンピュータエンティティの信頼のレベルを確立した。トラステッドトークンデバイスは、データ処理能力を有しユーザが高レベルで信頼するパーソナルおよびポータブルデバイスである。トラステッドトークンデバイスは、次の機能を実行することができる。

・例えば音声または視覚的表示装置によりユーザに容易に明らかになる方法で、コンピューティングプラットフォームの正しい動作を確認する機能。

・監視コンポーネントに対し、監視コンポーネントが関連するコンピュータプラットフォームの正しい動作の証拠を提供するよう要求する機能。

・監視コンポーネントがコンピューティングエンティティの正しい動作の満足のいく証拠を提供したかに応じて、トークンデバイスのコンピューティングプラットフォームとのあるレベルの対話を確立し、かかる正しい動作の証拠がトークンデバイスによって受取られない場合、コンピュータエンティティとの特定の対話を行わない機能。

【００３４】

トークンデバイスに対して、例えば、コンピューティングプラットフォームに常駐するアプリケーションまたはリモートアプリケーションが、動作を行うよう要求することができ、あるいは、代替的に、トークンデバイス自体が動作を開始することができる。

【００３５】

本明細書では、物理的または論理的コンポーネントに関連して使用される場合の「トラステッド（信頼された）」という語は、物理的または論理的コンポーネントが常に期待されたように振舞うことを意味するために使用される。そのコンポーネントの振舞いは、予測可能であり既知である。トラステッドコンポーネントは、無許可の変更に対する耐性が高い。

【００３６】

本明細書では、「コンピュータエンティティ」という語は、コンピュータプラットフォームおよび監視コンポーネントを示すために使用される。

【００３７】

本明細書では、「コンピュータプラットフォーム」という語は、本質的にではないが通常、関連する通信機能、例えば複数のドライバ、関連するアプリケーションおよびデータファイルを有し、例えばインターネットへの接続、外部ネットワークへの接続により、またはデータ記憶媒体、例えばＣＤ　ＲＯＭ、フロッピーディスク、リボンテープ等に格納されるデータを受取ることが可能な入力ポートを有することにより、外部エンティティ、例えばユーザまたは他のコンピュータプラットフォームと対話することが可能な、少なくとも１つのデータプロセッサと少なくとも１つのデータ記憶システムとを指すために使用される。「コンピュータプラットフォーム」という語には、コンピュータエンティティのメインデータ処理及び記憶機能が含まれる。

【００３８】

本明細書で使用される「ピックスマップ」という語は、モノクロまたはカラー（またはグレイスケール）画像を定義するデータを包含するように広く使用される。「ビットマップ」という語は、例えば、画素が「オン」か「オフ」かにより単一ビットが１かまたは０に

セットされる場合等、モノクロ画像のみに関連すると言えるが、「ピックスマップ」は、より一般的な用語であり、モノクロ画像と、１つの画素の色相、彩度および明度を定義するために２４ビット以上を必要とする可能性のあるカラー画像との両方を含む。

【００３９】

各コンピューティングエンティティにおいてトラステッドコンポーネントを使用することにより、異なるコンピューティングプラットフォーム間にあるレベルの信頼を生じさせることが可能となる。かかるプラットフォームにその状態に関して問合せ、それをリモートで、またはコンピュータエンティティ上のモニタを介して、トラステッド状態と比較することが可能である。かかる問合せによって収集される情報は、プラットフォームのあらゆるパラメータを監視するコンピューティングエンティティのトラステッドコンポーネントによって提供される。トラステッドコンポーネントによって提供される情報は、暗号認証により認証することができ、信頼することができる。

【００４０】

トラステッドコンポーネントの存在により、コンピューティングエンティティに対してリモートなまたはローカルなサードパーティソフトウェアが、その認証および識別のプルーフを取得しそのコンピューティングエンティティの測定された完全性メトリクスを取り出すために、コンピューティングエンティティと通信することが可能になる。そして、サードパーティソフトウェアは、トラステッドコンポーネントから取得されたメトリクスを期待されたメトリクスと比較することにより、サードパーティソフトウェアアイテムがコンピューティングエンティティと行うことを要求する対話、例えば商用トランザクションプロセスに対し、問合されたコンピューティングエンティティの状態が適当であるかを判断する。

【００４１】

コンピューティングエンティティ間のこのタイプの完全性確認は、コンピューティングエンティティのトラステッドコンポーネントと通信するサードパーティソフトウェアのコンテキストではうまく作用するが、人間のユーザが、そのコンピューティングエンティティ、またはそのユーザがユーザインタフェースを用いて対話することができる他のいずれかのコンピューティングエンティティとの信頼できるレベルの対話を取得する手段を提供するものではない。

【００４２】

本明細書で述べる好ましい実施態様では、トラステッドトークンデバイスは、ユーザにより使用されて、コンピューティングエンティティのトラステッドコンポーネントに問合せを行い、トラステッドコンポーネントによって確認されたコンピューティングエンティティの状態に関してユーザに報告する。

【００４３】

ここで、本発明の好ましい実施の形態で使用される「トラステッドプラットフォーム」について説明する。これは、プラットフォームの同一性（または識別）をプラットフォームの完全性メトリクスを提供する確実に測定されたデータに結び付ける、という機能を有する物理的なトラステッド装置のコンピューティングプラットフォームに組込むことによって達成される。同一性（または識別）および完全性メトリクスは、プラットフォームの信頼性を保証するために用意されたトラステッドパーティ（ＴＰ）によって提供される期待値と比較される。一致する場合は、プラットフォームの少なくとも一部が、完全性メトリクスの範囲により、正しく動作している、ということを意味する。

【００４４】

ユーザは、プラットフォームと他のデータを交換する前にプラットフォームの正しい動作を確認する。ユーザは、これを、トラステッド装置にその識別（すなわち、どれであるかの識別）および完全性メトリクスを提供するよう要求することによって行う。（任意選択的に、トラステッド装置は、それ自体がプラットフォームの正しい動作を確認することができなかった場合、識別の証拠を提供することを拒否する）。ユーザは、識別の証拠と識別メトリクスを受取り、それらを、真実であると信じる値と比較する。それらの適正な値

は、ユーザが信頼するＴＰまたは他のエンティティによって提供される。トラステッド装置によって報告されるデータが、ＴＰによって提供されるデータと同じである場合、ユーザはプラットフォームを信頼する。これは、ユーザがエンティティを信頼するためである。エンティティは、事前に識別の妥当性を検査し、プラットフォームの適当な完全性メトリクスを決定しているため、プラットフォームを信頼する。

【００４５】

ユーザは、プラットフォームのトラステッドな（信用できる）動作を確立すると、プラットフォームと他のデータを交換する。ローカルユーザの場合、交換は、プラットフォームで実行中のあるソフトウェアアプリケーションと対話することによって行われる。リモートユーザの場合、交換には、セキュアなトランザクションが含まれる。いずれの場合も、交換されるデータは、トラステッド装置によって「署名」される。そして、ユーザは、挙動を信頼することができるプラットフォームとデータが交換されているということを、より強く確信することができる。

【００４６】

トラステッド装置は、暗号化プロセスを使用するが、必ずしもそれら暗号化プロセスに対する外部インタフェースを提供しない。また、最も望ましい実施態様では、トラステッド装置を不正にいじることができないようにし、他のプラットフォーム機能が秘密にアクセスできないようすることによってその秘密を保護し、無許可の変更に対し実質的に免疫を有する環境を提供する。不正にいじること（すなわち、タンパリング）ができないようにすること（タンパプルーフ）は不可能であるため、これに最も近いものは、不正にいじることができにくい、または、タンパリングを検出するトラステッド装置である。従って、トラステッド装置は、好ましくは、不正にいじることができにくい（すなわち、耐タンパ性を有する）１つの物理的コンポーネントからなる。

【００４７】

耐タンパ性に関する技術は、セキュリティの技術分野における当業者には周知である。これらの技術には、タンパリングに抗する方法（トラステッド装置を適切に封入する等）と、タンパリングを検出する方法（規格外電圧、Ｘ線、またはトラステッド装置のケーシングにおける物理的完全性の喪失の検出等）と、タンパリングが検出された時にデータを削除する方法、が含まれる。適切な技術の更なる説明は、http://www.cl.cam.ac.uk/～mgk25/tamper.htmlにおいて見ることができる。タンパプルーフは本発明の最も望ましい特徴であるが、本発明の通常の動作には入らないため、本発明の範囲を超えるものであり、従って本明細書では詳しくは説明しない。

【００４８】

トラステッド装置は、偽造することが困難でなければならないため、物理的な装置であることが好ましい。それは、模造するすることが困難でなければならないため、耐タンパ性であることが最も好ましい。一般に、それは、ローカルにもある距離をおいても同一性を証明することが要求されるため、暗号化プロセスを使用することができるエンジンを有し、それが関連するプラットフォームのある完全性メトリクスを測定する少なくとも１つの方法を含んでいる。

【００４９】

図１は、好ましい実施の形態によるホストコンピュータシステムを示し、ここでは、ホストコンピュータは、Windows NT 4.0（R）オペレーティングシステムの下で動作するパーソナルコンピュータ、すなわちＰＣである。図１によれば、コンピュータプラットフォーム（ここではホストコンピュータとも呼ぶ）１００は、視覚的表示装置（ＶＤＵ）１０５、キーボード１１０、マウス１１５およびスマートカードリーダ１２０と、ローカルエリアネットワーク（ＬＡＮ）１２５と、に接続されており、後者はインターネット１３０に接続されている。ここでは、スマートカードリーダは独立したユニットであるが、キーボードの一体部分であってもよい。更に、ホストコンピュータは、キーボードに一体化された、トラステッド入力装置、この場合はトラステッドスイッチ１３５を有する。ＶＤＵ、キーボード、マウスおよびトラステッドスイッチは、ホストコンピュータの人間／コンピ

ュータインタフェース（ＨＣＩ）とみなすことができる。より詳細には、トラステッドスイッチと表示装置は、後述するように、トラステッド制御下で動作している時、「トラステッドユーザインタフェース」とみなすことができる。また、図１には、後述するような本実施形態で使用するためのスマートカード１２２も示す。

【００５０】

図２は、図１のホストコンピュータのハードウェアアーキテクチャを示す。

【００５１】

図２によれば、ホストコンピュータ１００は、ＲＡＭ２０５およびＲＯＭ２１０を含むメインメモリとＢＩＯＳメモリ２１９（メインメモリの予約領域であってよい）とに接続された中央処理装置（ＣＰＵ）２００またはメインプロセッサを備え、それらはすべてホストコンピュータ１００のマザーボード２１５上に取付けられている。この場合のＣＰＵは、Pentium(R)プロセッサである。ＣＰＵは、ＰＣＩ（周辺コンポーネント相互接続(Peripheral Component Interconnect)）ブリッジ２２０を介してＰＣＩバス２２５に接続されており、それには、ホストコンピュータ１００の他の主なコンポーネントが取付けられている。バス２２５は、本明細書では詳細に説明しないが、適切な制御、アドレスおよびデータ部分を含む。Pentiumプロセッサおよびｐｃｉアーキテクチャの詳細な説明については、本発明の範囲を超えるが、読み手は、Addison-Wesleyによって出版された、Hans-Peter Messmerによる書籍「The Indispensable PC Hardware Handbook」第３版、ＩＳＢＮ０－２０１－４０３９９－４を参照されたい。当然ながら、本発明は、Pentiumプロセッサ、Windows(R)オペレーティングシステムまたはＰＣＩバスを使用する実施態様に限定されない。

【００５２】

ＰＣＩバス２２５に取付けられたホストコンピュータ１００の他の主なコンポーネントには、ＳＣＳＩバス２３５を介してハードディスクドライブ２４０およびＣＤ－ＲＯＭドライブ２４５に接続されたＳＣＳＩ（小型コンピュータシステムインタフェース(small computer system interface)）アダプタと、ホストコンピュータ１００がファイルサーバ、プリントサーバまたは電子メールサーバ等の他のホストコンピュータ（図示せず）およびインターネット１３０と通信することを可能にするＬＡＮ１２５に、ホストコンピュータ１００を接続するＬＡＮ（ローカルエリアネットワーク）アダプタ２５０と、キーボード１１０、マウス１１５およびスマートカードリーダ１２０を取付けるためのＩＯ（入力／出力）装置２２５と、トラステッド装置２６０と、がある。トラステッド装置は、後に詳細に説明する、すべての標準的な表示機能に加えて多数の他のタスクを処理する。「標準的な表示機能」とは、あらゆる標準的なホストコンピュータ１００、例えばWindows NT(R)オペレーティングシステムの下で動作しているＰＣにおいて装備されていることが通常期待される、オペレーティングシステムまたはアプリケーションソフトウェアに関連する画像を表示するための機能などである。トラステッド装置２６０において「トラステッドディスプレイプロセッサ」の機能を提供することの重要性は、後で更に説明する。なお、キーボード１１０は、トラステッド装置２６０に直接接続されるとともに、ＩＯ装置２５５にも接続される。

【００５３】

主なコンポーネントのすべて、特にトラステッドディスプレイプロセッサ２６０もまた、好ましくは、ホストコンピュータ１００のマザーボード２１５上に組み込まれるが、時に、ＬＡＮアダプタ２５０およびＳＣＳＩアダプタ２３０を、プラグインタイプとすることができる。

【００５４】

コンピュータエンティティは、物理アーキテクチャと共に論理アーキテクチャを有するものとみなすことができる。論理アーキテクチャは、図１および図２において説明する物理アーキテクチャに存在するように、コンピュータプラットフォームとトラステッドコンポーネントに同じ基本的部分を有する。すなわち、トラステッドコンポーネントは、それが物理的に関連するコンピュータプラットフォームとは論理的に異なっている。コンピュー

タエンティティは、コンピュータプラットフォーム（第１のプロセッサおよび第１のデータ記憶手段）に物理的に常駐する論理空間であるユーザ空間と、トラステッドコンポーネントに物理的に常駐する論理空間であるトラステッドコンポーネント空間と、を備える。ユーザ空間には、１つまたは複数のドライバと、１つまたは複数のアプリケーションプログラムと、ファイル記憶領域と、スマートカードリーダと、スマートカードインタフェースと、ユーザ空間において動作を実行しトラステッドコンポーネントに報告を返すことができるソフトウェアエージェントと、がある。トラステッドコンポーネント空間は、トラステッドコンポーネントに基づき、トラステッドコンポーネントに物理的に常駐する、第２のデータプロセッサとトラステッドコンポーネントの第２のメモリ領域とによってサポートされる論理領域である。モニタ１０５は、トラステッドコンポーネント空間から直接画像を受取る。コンピュータエンティティの外部には、ドライバ（１つまたは複数のモデムポートを含んでよい）を介してユーザ空間に接続された、外部通信ネットワーク、例えば、インターネットおよび様々なローカルエリアネットワーク、広域ネットワークがある。外部ユーザスマートカードは、ユーザ空間のスマートカードリーダに入力する。

【００５５】

一般に、パーソナルコンピュータでは、特別な予約メモリ領域にＢＩＯＳプログラムが配置され、最初のメガバイトの上位６４Ｋはシステムメモリであり（アドレスＦ０００ｈ～ＦＦＦＦｈ）、メインプロセッサは、業界基準に従ってこのメモリロケーションを最初に参照するように構成される。

【００５６】

本プラットフォームと従来からのプラットフォームとの重要な相違は、リセット後、メインプロセッサが最初にトラステッド装置によって制御され、その後、トラステッド装置が制御をプラットフォーム固有のＢＩＯＳプログラムに渡し、通常、ＢＩＯＳプログラムがすべての入力／出力装置を初期化する、ということである。ＢＩＯＳプログラムが実行された後、通常、制御はＢＩＯＳプログラムにより、一般にハードディスクドライブ（図示せず）からメインメモリにロードされるWindows NT(R)等のオペレーティングシステムプログラムに渡される。

【００５７】

明らかに、通常の手続きからのこの変更は、業界標準の実施形態に対する変更を必要とし、それによりメインプロセッサ２００は、その第１の命令を受取るためにトラステッド装置２６０をアドレス指定するよう命令される。この変更は、単に異なるアドレスをメインプロセッサ２００にハードコード化することによって行うことができる。代替的には、トラステッド装置２６０には、標準ＢＩＯＳプログラムアドレスを割当てることができ、その場合、メインプロセッサ構成を変更する必要はない。

【００５８】

トラステッド装置２６０内にＢＩＯＳブートブロックが含まれることが非常に望ましい。これにより、完全性メトリクスの取得の破壊（異常なソフトウェアプロセスが存在する場合に発生する可能性がある）が防止され、ＢＩＯＳ（正しい場合であっても）がオペレーティングシステムに対する適切な環境を構築し損なう状況をもたらす異常なソフトウェアプロセスが防止される。

【００５９】

説明する好ましい実施態様では、トラステッド装置２６０は、１つの別個のコンポーネントであるが、トラステッド装置２６０の機能は、代替的にマザーボード上の複数の装置に分割されてよく、あるいはプラットフォームの現存の標準装置の１つまたは複数に組み込まれてもよい、ということが予見される。例えば、トラステッド装置の機能およびそれらの通信が破壊される可能性がない場合、それら機能のうちの１つまたは複数をメインプロセッサ自体に組み込むことが可能である。しかしながら、これには、トラステッド機能による独占的な使用のためにプロセッサ上に個別のリードが必要である可能性が高い。トラステッド装置は、本実施態様ではマザーボード２１５に組み込むために適応されたハードウェア装置であるが、更にまたは代替的に、要求される時にプラットフォームに取付ける

ことができる、ドングル等の「取外し可能な」装置として実施することができる、ということが予測される。トラステッド装置を組み込むか取外し可能とするかは、設計選択の問題である。しかしながら、トラステッド装置が分離可能である場合、トラステッド装置とプラットフォームとの間の論理的結合を提供するメカニズムが存在しなければならない。

【００６０】

システムリセット後、トラステッド装置２６０は、セキュアなブートプロセスを実行することにより、プラットフォーム１００のオペレーティングシステム（システムクロックおよびモニタの表示を含む）が適切にかつセキュアに実行していることを保証する。セキュアなブートプロセス中、トラステッド装置２６０は、コンピューティングプラットフォーム１００の完全性メトリクスを取得する。また、トラステッド装置２６０は、セキュアなデータ転送、例えば、暗号化／復号化および署名／検証を利用して、スマートカードとの間での認証、を実行することができる。また、トラステッド装置２６０は、ユーザインタフェースのロッキング等、様々なセキュリティ制御ポリシーをセキュアに実施することができる。

【００６１】

図３によれば、トラステッド装置２６０は、

トラステッド装置２６０の全体動作を制御し、トラステッド装置２６０の他の要素およびマザーボード２１５上の他の装置と対話するようにプログラムされたマイクロコントローラ３００と、

マイクロコントローラ３００の動作を制御するそれぞれの制御プログラム命令（すなわち、ファームウェア）を含む－かかる制御プログラム命令に含まれる機能には、プラットフォーム１００の完全性メトリクスを取得するための測定機能とスマートカード１２２を認証するための認証機能とが含まれる－不揮発性メモリ３０５、例えばフラッシュメモリ（代替的には、トラステッド装置２６０は、ＡＳＩＣに組込むことが可能であり、それによって一般に、より優れたパフォーマンスと大量生産におけるコスト効率とが提供されるが、概して、開発するためのコストがより高くなり、かつ柔軟性が低くなる）と、

後述するように、トラステッド装置２６０を、ＣＰＵ２００から画像データ（すなわち、グラフィクスプリミティブ）とスマートカード１２２からのトラステッド画像データ等の認証データとを受取るＰＣＩバスに接続するためのインタフェース３１０と、

少なくとも１つのフル画像フレームを格納する十分なＶＲＡＭ（ビデオＲＡＭ）を備えたフレームバッファメモリ３１５（一般的なフレームバッファメモリ３１５は、１６７０万色までをサポートする１２８０×７６８のスクリーン解像度に対し、１～２メガバイトのサイズである）と、

ピックスマップデータを、（アナログ）ＶＤＵ１０５を駆動するためのアナログ信号に変換するビデオＤＡＣ（デジタル-アナログコンバータ）３２０であって、ＶＤＵ１０５は、ビデオインタフェース３２５を介して当該ビデオＤＡＣ３２０に接続することからなる、ビデオＤＡＣ３２０と、

トラステッドスイッチ１３５から直接信号を受取るインタフェース３３０と、　状態情報、特に受取った暗号鍵を格納しマイクロコントローラ３００のためにワークエリアを提供する、揮発性メモリ３３５、例えばＤＲＡＭ（ダイナミックＲＡＭ）またはより高価なＳＲＡＭ（スタティックＲＡＭ）と、

ハードウェア暗号化アクセレレータおよび／またはソフトウェアを備え、後により詳細に説明するように、トラステッド装置２６０に暗号識別を提供すると共に、真正性、完全性および機密性を提供し、リプレイ攻撃（replay attack）から保護し、デジタル署名を作成し、デジタル証明書を使用するように構成された、暗号化プロセッサ３４０と、

トラステッド装置２６０の識別子I_{DP}（例えば、単純なテキストストリング名）、トラステッド装置２６０の秘密鍵S_{DP}、トラステッド装置２６０を署名公開－秘密鍵ペアと機密性公開－秘密鍵ペアに結合し、トラステッド装置２６０の対応する公開鍵を含む、VeriSign Inc.,等のトラステッドサードパーティ認証機関によって署名され提供される証明書$Cert_{DP}$と、を格納する、不揮発性メモリ３４５、例えばフラッシュメモリと、

を備える。

【００６２】

証明書は、一般に、かかる情報を含むが、ＣＡの公開鍵は含まない。その公開鍵は、一般に、「公開鍵インフラストラクチャ(Public Key Infrastructure)」（ＰＫＩ）を使用して利用可能となる。ＰＫＩの動作は、セキュリティの技術分野における当業者に周知である。

【００６３】

サードパーティが公開鍵のソースを確信し公開鍵が有効な公開－秘密鍵ペアの一部であるように、トラステッド装置２６０の公開鍵をサードパーティに提供するために、証明書$Cert_{DP}$が使用される。従って、サードパーティが、トラステッド装置２６０の公開鍵を事前に知っていたり、取得する必要はない。

【００６４】

トラステッド装置２６０は、その識別およびトラステッドプロセスをホストコンピュータに貸し、トラステッドディスプレイプロセッサは、その耐タンパ性、偽造(forgery）に対する耐性、模倣(counterfeiting)に対する耐性によって、それら特性を有する。適切な認証メカニズムを備えた選択されたエンティティのみが、トラステッド装置２６０内で実行するプロセスに影響することができる。ホストコンピュータの通常のユーザもネットワークを介してホストコンピュータに接続されたいかなる通常のユーザまたはいかなる通常エンティティも、トラステッド装置２６０内部で実行するプロセスにアクセスまたは干渉することができない。トラステッド装置２６０は、「不可侵(inviolate)」であるという特性を有する。

【００６５】

トラステッド装置２６０には、それが関連するコンピューティングプラットフォーム１００の完全性メトリックを確実に測定しまたは取得する少なくとも１つの方法が備えられる。本実施態様では、完全性メトリックは、測定機能により、ＢＩＯＳメモリにおいてＢＩＯＳ命令のダイジェストを生成することによって取得される。かかる取得された完全性メトリックは、上述したように確認（または検証）された場合、プラットフォーム１００の潜在的なユーザに対し、プラットフォーム１００がハードウェアまたはＢＩＯＳプログラムレベルで破壊されなかったことについて高レベルの確信を与える。他の既知のプロセス、例えばウイルスチェッカは、一般に、オペレーティングシステムおよびアプリケーションプログラムコードが破壊されなかったことをチェックするために適所に存在する。

【００６６】

測定機能は、ハッシュプログラム３５４とトラステッド装置２６０の秘密鍵S_{DP}とを格納する不揮発性メモリ３４５と、取得された完全性メトリックをダイジェスト３６１の形態で格納する揮発性メモリ３３５にアクセスすることができる。

【００６７】

１つの好ましい実施態様では、完全性メトリックは、ダイジェストと同様に、ブール値を含み、それは、後に明確になる理由により、測定機能によって揮発性メモリ３３５に格納される。

【００６８】

ここで、完全性メトリックを取得するための好ましいプロセスを、図１５を参照して説明する。

【００６９】

ステップ２４００において、スイッチオン時、測定機能は、メインプロセッサ２００のアクティビティを監視することにより、トラステッド装置２６０が最初にアクセスされたメモリか判断する。従来の動作の下では、メインプロセッサはまず、ＢＩＯＳプログラムを実行するためにＢＩＯＳメモリにまず向けられる。しかしながら、本発明の実施態様では、メインプロセッサ２００は、メモリとして作用するトラステッド装置２６０に向けられる。ステップ２４０５において、トラステッド装置２６０が最初にアクセスされたメモリである場合、ステップ２４１０において、測定機能は、揮発性メモリ３３５に、トラステ

ッド装置２６０が最初にアクセスされたメモリであったことを示すブール値を書込む。そうでない場合、ステップ２４１５において、測定機能は、トラステッド装置２６０が最初にアクセスされたメモリでなかったことを示すブール値を書込む。

【００７０】

トラステッド装置２６０が最初にアクセスされたものでない場合、当然ながら、トラステッド装置２６０がまったくアクセスされない可能性がある。これは、例えば、メインプロセッサ２００がＢＩＯＳプログラムを最初に実行するよう操作された場合である。これらの環境の下で、プラットフォームは動作するが、完全性メトリクスが利用できないため、その完全性を要求時に確認することができなくなる。更に、ＢＩＯＳプログラムがアクセスされた後にトラステッド装置２６０がアクセスされた場合、ブール値は、明らかにプラットフォームの完全性が無いことを示す。

【００７１】

ステップ２４２０において、メインプロセッサ２００によりメモリとしてアクセスされた場合、メインプロセッサ２００は、ステップ２４２５において測定機能から格納されたネイティブハッシュ命令３５４を読出す。ハッシュ命令３５４は、メインプロセッサ２００によって処理されるためにデータバス２２５を介して渡される。ステップ２４３０において、メインプロセッサ２００は、ハッシュ命令３５４を実行し、ステップ２４３５において、それらを使用して、ＢＩＯＳメモリ２１９の内容を読出しハッシュプログラムに従ってそれら内容を処理することにより、ＢＩＯＳメモリ２１９のダイジェストを計算する。ステップ２４４０において、メインプロセッサ２００は、トラステッド装置２６０の適切な不揮発性メモリロケーション３３５に、計算したダイジェスト３６１を書込む。そして、ステップ２４４５において、測定機能は、ＢＩＯＳメモリ２１９のＢＩＯＳプログラムを呼出し、従来からの方法で実行が継続される。

【００７２】

明らかに、要求される信頼の範囲に応じて、完全性メトリックを計算することが可能な多数の異なる方法がある。ＢＩＯＳプログラムの完全性の測定では、プラットフォームの基礎になる処理環境の完全性に関する基本的な検査が行われる。完全性メトリックは、ブートプロセスの妥当性に関し判断を下すことを可能にするような形態でなければならない。すなわち、完全性メトリックの値を使用して、プラットフォームが正しいＢＩＯＳを使用してブートされたか確認することができなければならない。任意選択的であるが、ＢＩＯＳ内の個々の機能ブロックは、それら自体のダイジェスト値を有することができ、全体的なＢＩＯＳダイジェストはこれらの個々のダイジェストのダイジェストである。これにより、ポリシーは、ＢＩＯＳ動作のいずれの部分が意図された目的に対してクリティカルであるか、いずれが無関係であるか（この場合、個々のダイジェストを、ポリシーに基づく動作の妥当性を確立することができる方法で格納しなければならない）を表明することができる。

【００７３】

他の完全性検査は、プラットフォームに取付けられた他の様々なデバイス、コンポーネントまたは装置が存在し正しい動作順序にあることを立証することを含むことができる。１つの例では、ＳＣＳＩコントローラに関連するＢＩＯＳプログラムを検証することにより、周辺装置との通信が信頼できることを保証することができる。他の例では、プラットフォーム上の他の装置、例えばメモリ装置またはコプロセッサの完全性を、一貫した結果を保証する一定の要求（チャレンジ）／応答対話を行うことにより検証することができる。トラステッド装置２６０が分離可能なコンポーネントである場合、かかる形態の対話は、トラステッド装置２６０とプラットフォームとの間の適切な論理結合を提供することが望ましい。また、本実施態様では、トラステッド装置２６０は、データバスをプラットフォームの他の部分との通信の主な手段として利用するが、（それほど都合よくはないものの）配線接続による経路または光学経路等の代替的な通信経路を提供することも可能である。更に、本実施態様では、トラステッド装置２６０は、メインプロセッサ２００に対し完全性メトリックを計算するよう命令するが、他の実施の形態では、トラステッド装置自体

が１つまたは複数の完全性メトリックを測定するよう構成される。

【００７４】

好ましくは、ＢＩＯＳブートプロセスは、ブートプロセス自体の完全性を検証するメカニズムを含む。かかるメカニズムは、例えばＩｎｔｅｌのドラフト「Wired for Management baseline specification v2.0-BOOT Integrity Service」からすでに知られており、ソフトウェアまたはファームウェアをロードする前にそのソフトウェアまたはファームウェアのダイジェストを計算することを含む。かかる計算されたダイジェストは、その公開鍵がＢＩＯＳに既知であるトラステッドエンティティによって提供される証明書に格納された値と比較される。そして、計算された値が証明書からの期待値と一致し、証明書が、トラステッドエンティティの公開鍵を使用することによって有効であることが証明された場合にのみ、ソフトウェア／ファームウェアはロードされる。そうでなければ、適切な例外処理ルーチンが呼出される。

【００７５】

任意に、計算されたＢＩＯＳダイジェストを受取った後、トラステッド装置２６０は、証明書のＢＩＯＳダイジェストの適正な値を検査し、計算されたダイジェストが適正な値と一致しない場合にＢＩＯＳに制御を渡さないようにすることができる。更に、または代替的に、トラステッド装置２６０は、ブール値を検査し、トラステッド装置２６０が最初にアクセスされたメモリでなかった場合にＢＩＯＳに制御を返さないようにすることができる。これらの場合のいずれにおいても、適切な例外処理ルーチンを呼出すことができる。

【００７６】

図１６は、ＴＰと、プラットフォームに組込まれたトラステッド装置２６０と、トラステッドプラットフォームの完全性を検証したい（リモートプラットフォームの）ユーザと、による動作のフローを示す。ユーザがローカルユーザである場合、図１６に示すものと同じステップが実質的に含まれることが理解されよう。いずれの場合も、ユーザは、一般に、検証を行うためにある形態のソフトウェアアプリケーションを使用する。リモートプラットフォームまたはトラステッドプラットフォームでソフトウェアアプリケーションを実行することが可能である。しかしながら、リモートプラットフォームにおいてでさえ、ソフトウェアアプリケーションは何らかの方法で破壊される可能性がある。従って、高レベルの完全性のために、ソフトウェアアプリケーションは、検証の目的でスマートカードを適当なリーダに挿入するユーザのスマートカード上に常駐することが好ましい。本発明の好ましい実施態様は、かかる構成を採用する。

【００７７】

最初の例では、トラステッドプラットフォームに対し保証を行うＴＰは、プラットフォームのタイプを検査してそれに対して保証すべきか否かを決定する。これは、ポリシーの問題である。すべてが良好である場合、ステップ２５００において、ＴＰは、プラットフォームの完全性メトリックの値を測定する。そして、ステップ２５０５において、ＴＰは、プラットフォームに対する証明書を作成する。証明書は、ＴＰにより、トラステッド装置の公開鍵と、オプションとしてそのＩＤラベルとを測定された完全性メトリクスに添付し、ストリングにＴＰの秘密鍵で署名することによって、作成される。

【００７８】

その後、トラステッド装置２６０は、その秘密鍵を使用してユーザから受け取った入力データを処理することによりその同一性を証明し、秘密鍵を知らずに入力／出力ペアを作成することが統計的に不可能であるように、出力データを作成することができる。このため、秘密鍵を知ることが、この場合の（同一性の）識別の基礎を形成する。明らかに、対称暗号化（symmetric encryption）を使用して識別の基礎を形成することが可能である。しかしながら、対称暗号化を使用する欠点は、ユーザがその秘密をトラステッド装置と共有する必要がある、ということである。更に、ユーザと秘密を共有する必要のある結果、対称暗号化は、原則としてユーザに対する識別を提供するためには十分であるが、トラステッド装置またはユーザからもたらされる確認を完全には信じることができないサードパーティに識別を証明するためには不十分である。

【００７９】
ステップ２５１０において、トラステッド装置２６０は、証明書$Cert_{DP}$をトラステッド装置２６０の適切な不揮発性メモリロケーションに書込むことによって初期化される。これは、好ましくは、マザーボード２１５にインストールされた後のトラステッド装置２４とのセキュアな通信によって行われる。トラステッド装置２６０に証明書を書込む方法は、秘密鍵を書込むことによりスマートカードを初期化するために使用される方法と類似している。セキュアな通信は、ＴＰのみに知られている「マスタ鍵」によってサポートされる。それは、製造中にトラステッド装置（またはスマートカード）に書込まれ、トラステッド装置２６０へのデータの書込みを可能にするために使用される。マスタ鍵を知らずにトラステッド装置２６０にデータを書込むことは不可能である。

【００８０】
プラットフォームの動作中における後のある時点、例えば、スイッチオンされるかリセットされる時、ステップ２５１５において、トラステッド装置２６０は、プラットフォームの完全性メトリック３６１を取得して格納する。

【００８１】
ユーザは、プラットフォームと通信することを望む場合、ステップ２５２０において、乱数等の一時的なもの（ナンス：nonce）を生成し、ステップ２５２５において、トラステッド装置２６０に要求する（プラットフォームのオペレーティングシステム、または適切なソフトウェアアプリケーションは、その要求を認識し、それを適切な方法で、一般的にはＢＩＯＳタイプのコールを介してトラステッド装置２６０に引渡すように構成される）。ナンスは、信頼できないプラットフォームによる古いが真正の署名の反復（「リプレイ攻撃」と呼ばれる）によってもたらされる欺きから、ユーザを保護するために使用される。ナンスを提供し応答を確認するプロセスは、周知の「要求（チャレンジ）／応答」プロセスの一例である。

【００８２】
ステップ２５３０において、トラステッド装置２６０は、要求（チャレンジ）を受取り、適切な応答を作成する。これは、測定された完全性メトリクスとナンス、及びオプションであるそのＩＤラベルのダイジェストであってよい。そして、ステップ２５３５において、トラステッド装置２６０は、その秘密鍵を使用してダイジェストに署名し、署名したダイジェストに証明書$Cert_{DP}$を添付してユーザに返す。

【００８３】
ステップ２５４０において、ユーザは、要求（チャレンジ、以下同じ）応答を受取り、ＴＰの周知の公開鍵を使用して証明書を確認する。そして、ユーザは、ステップ２５５０において、証明書からトラステッド装置２６０の公開鍵を抽出し、それを使用して要求応答から署名されたダイジェストを復号化する。次に、ステップ２５６０において、ユーザは要求応答内部のナンスを確認する。次に、ステップ２５７０において、ユーザは、要求応答から抽出した計算された完全性メトリックを、証明書から抽出した適正なプラットフォーム完全性メトリクスと比較する。ステップ２５４５、２５５５、２５６５または２５７５において、上記確認ステップのいずれかが失敗した場合、プロセス全体がステップ２５８０において終了し、更なる通信は発生しない。

【００８４】
すべてが良好な場合は、ステップ２５８５および２５９０において、ユーザおよびトラステッドプラットフォームは、他のプロトコルを使用して他のデータに対するセキュアな通信をセットアップする。この場合、プラットフォームからのデータはトラステッド装置２６０によって署名されるのが好ましい。

【００８５】
この確認プロセスの更なる改善が可能である。チャレンジャが、要求（チャレンジ）を通して、プラットフォーム完全性メトリクスとそれが取得された方法との値の両方を知ることが望ましい。これらの両方の情報により、チャレンジャがプラットフォームの完全性に関する適切な判断を行うことが可能になることが望ましい。また、チャレンジャは、多く

の異なるオプションを利用することができる。すなわち、チャレンジャは、完全性メトリクスがトラステッド装置２６０において有効であると認識されることを認めてよく、あるいは代替的に、完全性メトリクスの値がチャレンジャが保持する値と等しい場合に、プラットフォームが適切なレベルの完全性を有する、ということのみを認めてよい（または、これら２つの場合に異なるレベルの信頼があるとしてもよい）。

【００８６】

署名、証明書と要求／応答との使用、およびそれらを使用して同一性を証明する技術は、セキュリティの当業者には周知であるため、本明細書ではこれ以上詳細には説明する必要はない。

【００８７】

ユーザのスマートカード１２２は、コンピューティングエンティティから分離したトークンデバイスであり、スマートカードリーダポート１２０を介してコンピューティングエンティティと対話する。ユーザは、いくつかの異なるベンダまたはサービスプロバイダによって発行されるいくつかの異なるスマートカードを有することができ、トラステッドコンポーネントおよびスマートカードリーダによって提供される、本明細書で説明するような複数のコンピューティングエンティティのうちのいずれか１つから、インターネットまたは複数のネットワークコンピュータへのアクセスを取得することができる。ユーザが使用している個々のコンピューティングエンティティにおけるユーザの信頼は、ユーザのトラステッドスマートカードトークンとコンピューティングエンティティのトラステッドコンポーネントとの間の対話から得られる。ユーザは、それらのトラステッドスマートカードトークンにより、トラステッドコンポーネントの信頼性を確認する。

【００８８】

好ましい実施態様に従う使用に適したスマートカードの処理エンジンを、図４に示す。処理エンジンは、標準的な暗号化および復号化（暗号解読）機能を行うと共に、後述するようにスマートカード１２２の認証およびプラットフォーム１００の検証のための単純な要求／応答動作を行うプロセッサ４００を備える。本実施態様では、プロセッサ４００は８ビットマイクロコントローラであり、組込みオペレーティングシステムを有し、ＩＳＯ７８１６－３、４、Ｔ＝０、Ｔ＝１およびＴ＝１４規格によって指定される非同期プロトコルを介して外部と通信するように構成されている。また、スマートカードは、スマートカード１２２の識別子I_{SC}と、データにデジタル的に署名するために使用される秘密鍵S_{SC}と、スマートカードを公開－秘密鍵ペアと結合しスマートカード１２２の対応する公開鍵を含む、トラステッドサードパーティ認証機関によって提供される証明書$Cert_{SC}$（トラステッドディスプレイプロセッサ２６０の証明書$Cert_{DP}$と本質的に同じ）とを含む、不揮発性メモリ４２０、例えばフラッシュメモリも備える。更に、スマートカードは、不揮発性メモリ４２０内に「シール(seal)」データＳＥＡＬを含むが、その重要性については後で説明する。

【００８９】

ここで、ユーザスマートカード１２２とプラットフォーム１００との間の認証のための好ましいプロセスを、図１７のフローチャートを参照して説明する。後述するように、プロセスは、うまい具合に要求／応答ルーチンを実施する。多くの利用可能な要求／応答メカニズムが存在する。本実施態様で使用される認証プロトコルは、ＩＳＯ／ＩＥＣ９７９８－３に記載されている相互（または３ステップ）認証を実施する。当然ながら、ＩＳＯ／ＩＥＣ９７９８－３に記載されている、他の認証手続き、例えば２ステップまたは４ステップを使用することができない理由はない。

【００９０】

最初に、ユーザは、ステップ２７００において、プラットフォーム１００のスマートカードリーダ１２０にユーザのスマートカード１２２を挿入する。予め、プラットフォーム１００は、一般にその標準オペレーティングシステムの制御下で動作し、認証プロセスを実行しており、ユーザがユーザスマートカード１２２を挿入するのを待っている。このようにアクティブであるスマートカードリーダ１２０を除けば、プラットフォーム１００は一

般に、ユーザインタフェース（すなわち、画面、キーボードおよびマウス）を「ロックする」ことによりユーザにはアクセス不能となる。

【００９１】

ユーザスマートカード１２２がスマートカードリーダ１２０に挿入されると、トラステッド装置２６０は、ステップ２７０５においてナンスＡを生成してユーザスマートカード１２２に送信することにより、歩調を合わせて相互認証を試みるようにトリガされる。乱数等のナンスは、信頼されないサードパーティによる古いが真正の応答の反復（「リプレイ攻撃」と呼ばれる）によってもたらされる欺きから、発信者を保護するために使用される。

【００９２】

これに応答して、ステップ２７１０において、ユーザスマートカード１２２は、以下の連結からなる応答を生成して返す。すなわち、ナンスＡ、ユーザスマートカード１２２によって生成される新たなナンスＢ、トラステッド装置２６０のＩＤおよび幾分かの冗長性のプレーンテキスト（plain text）と、ユーザスマートカード１２２の秘密鍵によりプレーンテキストに署名することによって生成されたプレーンテキストの署名と、ユーザスマートカード１２２のＩＤおよび公開鍵を含む証明書を連結したものである。

【００９３】

トラステッド装置２６０は、ステップ２７１５において、証明書の公開鍵を使用してプレーンテキストの署名を検証することによって、応答が真正のものであるかどうかを確認する。応答が真正でない場合、プロセスはステップ２７２０で終了する。応答が真正である場合、ステップ２７２５において、トラステッド装置２６０は以下の連結を含む更なる応答を生成して送信する。すなわち、ナンスＡ、ナンスＢ、ユーザスマートカード１２２のＩＤおよび取得された完全性メトリックのプレーンテキストと、トラステッド装置２６０の秘密鍵を使用してプレーンテキストに署名することにより生成されたプレーンテキストの署名と、ＴＰの秘密鍵によって署名された、トラステッド装置２６０の公開鍵と真正の完全性メトリックとを含む証明書を連結したものである。

【００９４】

ステップ２７３０において、ユーザスマートカード１２２は、ＴＰの公開鍵を使用し、取得した完全性メトリックを認証された完全性メトリックと比較することにより、この応答が真正のものであるかどうかを確認する。ここで一致は、確認が成功したことを示す。応答が真正でない場合、プロセスはステップ２７３５で終了する。

【００９５】

手続きが成功した場合、トラステッド装置２６０がユーザスマートカード１２２を認証したと共に、ユーザスマートカード１２２がトラステッドプラットフォーム１００の完全性を確認しており、ステップ２７４０において、認証プロセスはユーザに対してセキュアプロセスを実行する。そして、ステップ２７４５において、認証プロセスは、インターバルタイマをセットする。その後、認証プロセスは、ステップ２７５０において、適切なオペレーティングシステム割込みルーチンを使用して、インターバルタイマを定期的に点検することにより、いつタイマが所定のタイムアウト期間を満たしたか、または、超過したかを検出する。

【００９６】

明らかに、認証プロセスとインターバルタイマとは、セキュアプロセスと平行して動作する。

【００９７】

タイムアウト期間が満たされるかまたは超過された時、認証プロセスは、ステップ２７６０において、ユーザスマートカード１２２に対しそれ自体を識別するために要求（チャレンジ）を送信することにより、ユーザスマートカード１２２を再度認証するようにトラステッド装置２６０をトリガする。ユーザスマートカード１２２は、ステップ２７６５において、そのＩＤとその公開鍵とを含む証明書を返す。ステップ２７７０において、応答がない（例えば、ユーザスマートカード１２２が取外された結果として）かまたは、証明書

が何らかの理由によりもはや有効でない（例えば、ユーザスマートカードが異なるスマートカードと交換されたことにより）場合、ステップ２７７５においてトラステッド装置２６０により、セッションが終了される。そうでない場合、ステップ２７７０において、インターバルタイマをリセットすることによってステップ２７４５からのプロセスが繰返される。

【００９８】

この好ましい実施態様では、モニタ１０５は、トラステッドコンポーネント自体に含まれるモニタサブシステムによって直接駆動される。この実施態様では、トラステッドコンポーネント空間に、トラステッドコンポーネント自体と、モニタ１０５上のトラステッドコンポーネントによって生成される表示とが存在する。この構成は、「System for Digitally Signing a Document」と題する１９９９年５月２８日に出願された、本出願人の同時係属欧州特許出願第９９３０４１６４．９号（およびこれに基づいて優先権を主張している、本出願と同一日付の国際特許出願を含む全ての特許出願）に更に記載されている。尚、この出願の内容はこの引用をもって本明細書に組み込まれたものとする。

【００９９】

後で明らかになるが、トラステッド装置のこの形態を使用することにより、特にホストコンピュータの表示機能の少なくとも一部を制御することによってセキュアなユーザインタフェースが提供される。より詳細には、トラステッド装置（これらの目的のためにトラステッドディスプレイプロセッサと呼ぶ）または同様の特性を有する装置は、標準的なホストコンピュータソフトウェアによってデータを処理することができるポイントを超えるビデオ処理のある段階でビデオデータに関連付けられる。これにより、トラステッドディスプレイプロセッサは、ホストコンピュータソフトウェアによる干渉または破壊を受けることなく表示面にデータを表示することができる。このため、トラステッドディスプレイプロセッサは、何の画像が現在ユーザに表示されているかを確定することができる。これは、ユーザが署名している画像（ピックスマップ）を明白に識別するために使用される。この副次的効果は、トラステッドディスプレイプロセッサが、例えば従来の特許出願の完全性メトリック、またはユーザステータスメッセージあるいはプロンプトを含む、それの任意のデータを表示面に確実に表示することができる、ということである。

【０１００】

ここで、トラステッド装置がトラステッドディスプレイプロセッサである場合の「トラステッド表示」の要素および機能を、図３および図４を参照して更に説明する。

【０１０１】

図３から、フレームバッファメモリ３１５が、トラステッドディスプレイプロセッサ２６０自体のみによりアクセス可能であって、ＣＰＵ２００によってアクセス可能でないことが明らかとなろう。これは、ＣＰＵ２００、またはより重要なことには破壊的なアプリケーションプログラムまたはウイルスが、トラステッド動作中にピックスマップを変更することができないということは必須であるため、好適な実施態様の重要な特徴である。当然ながら、ＣＰＵ２００がフレームバッファメモリ３１５にアクセスすることができる場合に、トラステッドディスプレイプロセッサ２６０が最終的な制御を有するよう構成されている限りは、ＣＰＵ２００がフレームバッファメモリ３１５に直接アクセスすることができる場合であっても、同じレベルのセキュリティを提供することが可能である。明らかに、この後者の方式は実施するのがより困難である。

【０１０２】

ここで、グラフィクスプリミティブがホストコンピュータ１００によって生成される一般的なプロセスを、背景として説明する。最初に、特定の画像を表示したいアプリケーションプログラムが、グラフィカルＡＰＩ（アプリケーションプログラミングインタフェース）を介してオペレーティングシステムに対し適切なコールを行う。ＡＰＩは、一般に、アプリケーションプログラムが、画像を表示する目的でWindows NT(R)によって提供されるような基礎となる特定の表示機能にアクセスするための標準インタフェースを提供する。ＡＰＩコールにより、オペレーティングシステムは各グラフィクスドライバライブラリル

ーチンコールを行い、その結果、この場合はトラステッドディスプレイプロセッサ２６０であるディスプレイプロセッサに特有のグラフィクスプリミティブが生成される。これらのグラフィクスプリミティブは、最後に、ＣＰＵ２００によってトラステッドディスプレイプロセッサ２６０に渡される。グラフィクスプリミティブの例としては、「幅ｚで点ｘから点ｙに線を引く」かまたは「点ｗ、ｘ、ｙおよびｚで囲まれる領域を色ａで塗りつぶす」といったものがある。

【０１０３】

マイクロコントローラ３００の制御プログラムは、マイクロコントローラを制御して、受取ったグラフィクスプリミティブを処理する標準表示機能を提供する。具体的には、
グラフィクスプリミティブをＣＰＵ２００から受取って処理することにより、ＶＤＵ１０５画面に表示される画像を直接的に表すピックスマップデータを形成する。ここで、ピックスマップデータは、一般的に、ＶＤＵ１０５画面上のアドレス指定可能な各画素の赤、緑および青のドットの各々の明度値（輝度値）を含んでいる。そして、
ピックスマップデータをフレームバッファメモリ３１５に格納し、
定期的に、例えば１秒間に６０回、フレームバッファメモリ３１５からピックスマップデータを読出し、ビデオＤＡＣを使用してそのデータをアナログ信号に変換し、アナログ信号をＶＤＵ１０５に送信して、画面上に所望の画像を表示する。

【０１０４】

制御プログラムは、標準表示機能の他に、ＣＰＵ２００から受け取った表示画像データをトラステッド画像データと混合して１つのピックスマップを形成する機能を有する。また、制御プログラムは、暗号化プロセッサおよびトラステッドスイッチ１３５との対話も管理する。

【０１０５】

トラステッドディスプレイプロセッサ２６０は、ホストコンピュータ１００の全「表示システム」の一部を形成し、その他の部分は、一般に、アプリケーションプログラムによって「呼ばれる」ことが可能でありグラフィクスプロセッサの標準表示機能にアクセスする、オペレーティングシステムと、ＶＤＵ１０５と、の表示機能である。言い換えれば、ホストコンピュータ１００の「表示システム」は、画像の表示に関するハードウェアまたは機能のすべての部分を含む。

【０１０６】

既に述べたように、この実施態様のトラステッド表示は、トラステッドディスプレイプロセッサとユーザスマートカード１２２との間の対話に基づく。特に重要なのは、不揮発性メモリ４２０の「シール」データＳＥＡＬであって、これは、後で詳細に説明するように、トラステッドディスプレイプロセッサ２６０により、ユーザに対してプロセスがユーザのスマートカードと安全に動作していることを示すために、グラフィカルに表現することができるものである。本実施態様では、シールデータＳＥＡＬは、例えばユーザ自身の画像等、独自の識別子としてユーザによって最初に選択され、周知の技術を使用してスマートカード１２２にロードされた、画像ピックスマップの形態である。また、プロセッサ４００は、状態情報（受取った鍵等）を格納しプロセッサ４００に対し作業領域を提供する揮発性メモリ４３０、例えばＲＡＭと、スマートカードリーダと通信するインタフェース４４０、例えば電気接点と、にアクセスすることができる。

【０１０７】

シール画像は、ピックマップとして格納される場合、比較的大容量のメモリを消費する可能性がある。これは、メモリ容量が比較的制限されている場合に画像がスマートカード１２２に格納される必要のある環境において、明らかな欠点であろう。メモリ要件は、多くの異なる技術によって低減することができる。例えば、シール画像は、トラステッドディスプレイプロセッサ２６０によって伸長することができる圧縮画像と、トラステッドディスプレイプロセッサ２６０によって生成される繰返しモザイクのプリミティブな要素を形成するサムネイル画像と、１組の英数字等、トラステッドディスプレイプロセッサ２６０により１つの大きい画像として表示することができるか、または上記のようなサムネイル

画像として使用することができる、本来的に圧縮された画像と、を含むことができる。これらの代替例のいずれにおいても、シールデータ自体を暗号化された形式とすることができ、シールデータは、表示することができる前にトラステッドディスプレイプロセッサ２６０に対しデータを復号化するように要求することができる。代替的には、シールデータを、暗号化されたインデクスとすることができ、それは、ホストコンピュータ１００またはネットワークサーバによって格納される多数の可能な画像のうちの１つを識別する。この場合、インデクスは、トラステッドディスプレイプロセッサ２６０によりセキュアチャネルを介してフェッチされ、正しい画像を検索して表示するために復号化される。更に、シールデータは、適切にプログラムされたトラステッドディスプレイプロセッサ２６０により画像を生成するために解釈することができる命令（例えば、PostScript(R)命令）を含むことができる。

【０１０８】

図１８は、トラステッド署名処理を行うコンテキストにおいて、ホストコンピュータ１００とトラステッドディスプレイプロセッサ２６０とスマートカード１２２機能との間の論理関係を示す。トラステッド署名処理に加わるプロセスを明確に表現するために、ホストコンピュータ１００、トラステッドディスプレイプロセッサ２６０またはスマートカード１２２の機能に論理的に分離するだけでなく、機能を物理アーキテクチャから独立して表現している。更に、「標準表示機能」は、線ｘ－ｙによってトラステッド機能から仕切られており、線の左側の機能は具体的にはトラステッド機能である。図において、機能は長円に表し、機能が作用する「永久」データ（署名プロセスの間のドキュメント画像を含む）は、ボックスに示す。状態データまたは受取った暗号鍵等の動的データは、単に明確にする理由で示していない。長円の間および長円とボックスとの間の矢印は、それぞれの論理通信経路を表す。

【０１０９】

図１８によれば、ホストコンピュータ１００は、ドキュメントの署名を要求するアプリケーションプロセス３５００、例えばワードプロセッサプロセスと、ドキュメントデータ３５０５と、オペレーティングシステムプロセス３５１０と、アプリケーションプロセス３５００から表示コールを受取るＡＰＩプロセス３５１１と、キーボード１１０からアプリケーションプロセス３５００に入力を提供するキーボードプロセス３５１３と、マウス１１５からアプリケーションプロセス３５００に入力を提供するマウスプロセス３５１４と、ＡＰＩプロセス３５１１を介してアプリケーションプロセスから受け取ったコールに基づいてグラフィクスプリミティブを生成するグラフィクスプリミティブプロセス３５１５と、を含む。ＡＰＩプロセス３５１１とキーボードプロセス３５１３とマウスプロセス３５１４とグラフィクスプリミティブプロセス３５１５とは、オペレーティングシステムプロセス３５１０の最上部に構築され、オペレーティングシステムプロセス３５１０を介してアプリケーションプロセスと通信する。

【０１１０】

ホストコンピュータ１００の残りの機能は、トラステッドディスプレイプロセッサ２６０によって提供される機能である。これらの機能は、トラステッドディスプレイプロセッサ２６０のすべての動作を調整し、グラフィクスプリミティブプロセスからのグラフィクスプリミティブとアプリケーションプロセス３５００からの署名要求とを受取る、制御プロセス３５２０と、制御プロセス３５２０からの要求に応答してドキュメント署名手続を表す署名されたサマリを生成するためのサマリプロセス３５２２と、スマートカード１２２からピックスマップのデジタル署名を取得するための署名要求プロセス３５２３と、スマートカード１２２からシールデータ３５４０を取り出すためのシールプロセス３５２４と、サマリプロセス３５２２、署名要求プロセス３５２３およびシールプロセス３５２４によって要求された要求／応答およびデータ署名タスクを行うためにスマートカード１２２と対話するためのスマートカードプロセス３５２５と、署名要求プロセス３５２３によって要求された時に、格納されたピックスマップデータ３５３１を読出し、署名要求プロセス３５２３に渡すためのピックスマップ読出しプロセス３５２６と、制御プロセス３５２

０から受け取ったグラフィクスプリミティブおよびシール画像データに基づいてピックスマップデータ３５３１を生成するためのピックスマップ生成プロセス３５２７と、ピックスマップデータを読出し、それをアナログ信号に変換し、その信号をＶＤＵ１０５に送信するための画面リフレッシュプロセス３５２８と、トラステッドスイッチ１３５がユーザによって起動されたかを監視するためのトラステッドスイッチプロセス３５２９、である。スマートカードプロセス３５２５は、トラステッドディスプレイプロセッサの識別データI_{DP}と秘密鍵S_{DP}データと証明書$Cert_{DP}$データ３５３０とにアクセスすることができる。実際には、スマートカードとトラステッドディスプレイプロセッサとは、標準オペレーティングシステムコールを介して互いに対話（通信）する。

【０１１１】

スマートカード１２２は、シールデータ３５４０と、要求／応答およびデータ署名タスクを行うためにトラステッドディスプレイプロセッサ２６０と対話するためのディスプレイプロセッサプロセス３５４２と、スマートカード識別データI_{SC}、スマートカード秘密鍵データS_{SC}およびスマートカード証明書データ$Cert_{SC}$３５４３、を有する。

【０１１２】

本発明の他の実施態様では、トラステッドスイッチ１３５の機能は、ソフトウェアによって行うことができる。トラステッドスイッチプロセス３５２９が起動されると（ステップ６３０の場合のように）、トラステッドコンポーネント２６０は、専用スイッチの動作を待たずに、その乱数発生機能を使用して、テキスト列の形式のナンスを生成する。そして、このテキスト列は、「アクションを確認するために＜テキスト列＞を入力してください」という形式のメッセージでトラステッドディスプレイに表示される。そして、ユーザは、動作を確認するために、キーボード１１０を使用して所与のテキスト列を入力しなければならない。毎回テキスト列が異なるため、および他のソフトウェアはこのテキスト列にアクセスすることができない（テキスト列は、トラステッドプロセッサ３００とディスプレイとの間でのみ移動する）ため、不当なソフトウェアがこの確認プロセスを破壊することは不可能である。

【０１１３】

各個々のスマートカードには、各スマートカードで異なる、対応するそれぞれの画像データが格納することができる。トラステッドコンポーネントとのユーザ対話のため、例えば、トラステッドコンポーネントによって生成されるダイアログボックスモニタ表示のために、トラステッドコンポーネントは、ユーザのスマートカードから画像データ１００１を取出し、これをモニタ１０５に表示されるダイアログボックスに対する背景として使用する。これにより、ユーザは、モニタ１０５に表示されるダイアログボックスがトラステッドコンポーネントにより生成されるということを確信する。画像データは、人間によって容易に認識可能であることが好ましく、いかなる偽造も、ただちにユーザの目にはっきりと見えるようにするのが良い。例えば、画像データには、ユーザの写真を含めることができる。スマートカード上の画像データは、スマートカードを使用している人に独自のものとすることができる。

【０１１４】

本発明の好適な実施態様では、ユーザは、コンピュータプラットフォーム上の選択された論理または物理エンティティ、例えば、ファイル、アプリケーション、ドライバ、ポート、インタフェース、またはそのエンティティ上で発生するイベントを監視するものを指定することができる。２つのタイプの監視を提供することができる。１つは、トラステッドコンポーネントを介してユーザによってセットされる、所定期間に亙る連続した監視であり、もう１つは、エンティティに発生する特定のイベントの監視である。具体的には、ユーザは、価値の高いまたは情報の内容が制限された特定のファイルを指定することができ、許可されているか否かに関わらず、そのファイルを含む任意のインタラクションを、ファイル上に発生しているイベントが削除され消去されまたは破壊されると必ずそのことがただちに明白となるような方法で自動的にログし格納するように、その指定されたファイルの監視を行うことができる。

【０１１５】
図５に、コンピュータエンティティ５００の論理アーキテクチャの概略を示す。論理アーキテクチャは、本明細書で図１ないし図４を参照して説明した物理アーキテクチャに存在するように、コンピュータプラットフォームとトラステッドコンポーネントに同じ基本的部分を有する。すなわち、トラステッドコンポーネントは、それが物理的に関連するコンピュータプラットフォームとは論理的に異なっている。コンピュータエンティティは、コンピュータプラットフォーム（第１のプロセッサおよび第１のデータ記憶手段）に物理的に常駐する論理空間であるユーザ空間５０４と、トラステッドコンポーネント２６０に物理的に常駐する論理空間であるトラステッドコンポーネント空間５１３と、を備える。ユーザ空間５０４には、１つまたは複数のドライバ５０６と、１つまたは複数のアプリケーションプログラム５０７と、ファイル記憶領域５０８と、スマートカードリーダ１２０と、スマートカードインタフェース２５５と、ユーザ空間において動作を実行し、トラステッドコンポーネント２６０に報告するよう動作するソフトウェアエージェント５１１、がある。トラステッドコンポーネント空間は、トラステッドコンポーネントの第２のデータプロセッサおよび第２のメモリ領域によってサポートされる、トラステッドコンポーネントに基づきかつそれに物理的に常駐する論理領域である。確認キー装置１３５は、トラステッドコンポーネント空間５１３に直接入力し、モニタ１０５は、トラステッドコンポーネント空間５１３から画像を直接受取る。コンピュータエンティティの外部には、１つまたは複数のモデムポートを含んでよいドライバ５０６を介してユーザ空間に接続された、外部通信ネットワーク、例えばインターネット５０１と、様々なローカルエリアネットワーク、広域ネットワーク５０２、がある。外部ユーザスマートカード５０３は、ユーザ空間のスマートカードリーダ１２０に入力する。
【０１１６】
トラステッドコンポーネント空間には、トラステッドコンポーネント自体と、トラステッドコンポーネントによって生成されるモニタ１０５上の表示と、確認キーインタフェース３０６を介して確認信号を入力する確認キー１３５が常駐する。
【０１１７】
図６を参照すると、エージェント５１１内には、トラステッドコンポーネント２６０と通信するための通信コンポーネント６０１と、ユーザ空間内の指定された論理または物理エンティティ、例えばコンピュータプラットフォーム上のデータファイル、アプリケーションまたはドライバで発生するイベントを監視することを目的とするファイル監視コンポーネント６００、が提供される。
【０１１８】
図７に、トラステッド空間５１３に常駐するトラステッドコンポーネント２６０上の内部コンポーネントの概略を示す。トラステッドコンポーネントは、ユーザ空間におけるソフトウェアエージェント５１１と通信するための通信コンポーネント７００と、モニタ１００上に表示される複数のインタフェース表示とコンピューティングエンティティのユーザがトラステッドコンポーネント２０２と対話するのを可能にするインタフェースコードとを生成するためのディスプレイジェネレータを含むディスプレイインタフェースコンポーネント７０１と、コンピュータプラットフォーム上の個々のファイル、アプリケーション、ドライバ等を選択し、そのファイル、アプリケーションまたはドライバを監視し、ファイル、アプリケーションまたはドライバで発生するイベントのログを編集（またはコンパイル）するためのイベントロガープログラム７０２と、イベントログがイベントロガー７０２を離れた後に変更された場合にそれがただちに明らかとなるような方法で、イベントロガーコンポーネント７０２によってもたらされるイベントログを暗号的にリンクするために使用される、複数の暗号化機能７０３と、トラステッドコンポーネントによって監視するためにユーザが選択可能な様々なパラメータの動作およびパフォーマンスを予測する予測データを生成するための１組の予測アルゴリズム７０４と、監視されたイベントパラメータがユーザによって設定された所定の範囲外になるか、または予測アルゴリズム７０４によって予測された範囲外になった場合に、アラームを生成するためのアラーム生成コ

ンポーネント７０５、を備える。
【０１１９】
ここで、コンピュータエンティティの動作、特に、トラステッドコンポーネント２６０の動作、及び、コンピュータプラットフォーム上のイベントを監視するための、トラステッドコンポーネント２６０とエージェント５１１との対話機能について説明する。
【０１２０】
図８に、モニタ１０５上のダイアログ表示を生成するため、およびコンピュータエンティティ内のトラステッドコンポーネントが存在し機能していることをモニタのユーザに証明するためにコンピュータエンティティにより実行される、１組のプロセスステップの概略を示す。まず、ステップ８００において、コンピュータエンティティのユーザは、そのスマートカード１２２をスマートカードリーダポート１２０に入れる。スマートカード上の予め記憶されたアルゴリズムは、ナンスＲ１を生成し、そのナンスＲ１を、スマートカードリーダ１２０、スマートカードインタフェース２５５を通しデータバス２２５を介してトラステッドコンポーネント２６０にダウンロードする。ナンスＲ１は、一般に、スマートカード１２２によって生成されるビットのランダムなバーストからなる。スマートカード１２２は、ナンスＲ１を、スマートカードの内部メモリに一時的に格納する。これにより、この記憶されたナンスＲ１をトラステッドコンポーネントから受取られる応答メッセージと比較することができる。ステップ８０２において、トラステッドコンポーネントは、ナンスＲ１を受取り、第２のナンスＲ２を生成し、Ｒ１をＲ２と連結し、暗号化機能７０３を使用して連結Ｒ１‖Ｒ２に署名する。デジタルデータを認証するためにデジタル署名を与えるプロセスは、本技術分野において周知であり、「Handbook of Applied Cryptography」（Menezes Vanoorschot,Vanstone）のセクション１．６および１．８３に記載されている。更に、デジタル署名の使用が、「Applied Cryptography-Second edition」（Schneier）のセクション２．６に紹介されている。そして、トラステッドコンポーネント２６０は、ステップ８０３において、スマートカードに対し署名されたナンスを再び送り返す。スマートカードは、ステップ８０４において、トラステッドコンポーネントから戻された受信メッセージの署名をチェックし、その受信メッセージに含まれるナンスを最初に送信したナンスＲ１と比較する。そのコピーは、その内部メモリに格納されている。ステップ８０５において、トラステッドコンポーネントから戻されたナンスが格納されているナンスと異なる場合、ステップ８０６において、スマートカードは処理を停止する。ナンスが異なるということは、トラステッドコンポーネントが適切に作動していないか、またはスマートカードリーダ１２０とトラステッドコンポーネント２６０との間でナンスデータへのなんらかのタンパリングがあり、その結果ナンスデータが変化した、ということを示す。この時点で、スマートカード１２２は、その生成されたナンスがコンピュータエンティティによって正しく戻されなかったため、コンピュータエンティティを全体として「信用」しない。
【０１２１】
トラステッドコンポーネントから戻されたナンスが、スマートカードによって最初に送信されたナンスとまったく同じであり、ステップ８０５における２つのＲ１ナンスの比較が成功した場合、ステップ８０７において、スマートカードは、その内部メモリから格納された画像データを取り出し、ナンスＲ２を添付し、その連結に署名し、格納された画像データを暗号化し、暗号化した画像データと署名とをスマートカードリーダ１２０を介してトラステッドコンポーネントに送る。トラステッドコンポーネントは、スマートカードリーダインタフェース３０５およびデータバス３０４を介して暗号化された画像と署名データとを受取り、ステップ８０８において、画像データを復号化し、その暗号化機能７０３を用いて署名を検証し、ナンスＲ２を検証する。画像データは、トラステッドコンポーネントのメモリ領域に内部的に格納される。そして、トラステッドコンポーネントは、ステップ８０９において、人間のユーザと対話するために作成し、モニタ１０５上に表示する任意の視覚的表示に対する背景として、その画像データを使用する。
【０１２２】

図９乃至し図１１に、コンピュータプラットフォーム上で監視されるアイテムを選択し、監視セッションを起動するためのコンピュータエンティティによって実行される１組のプロセスステップを示す。ステップ９００において、ユーザは、モニタ１０５上の通常のオペレーティングシステムビューにおいて表示されるアイコンの上でポインティングデバイス１１５をクリックすることにより、セキュリティ監視機能を選択する。アイコンは、トラステッドコンポーネント２６０のディスプレイインタフェース７０１のディスプレイジェネレータコンポーネントによって生成される。アイコンをクリックすることにより、トラステッドコンポーネントは、例えば本明細書では図１０に示すように、モニタ１０５上にダイアログボックス表示を生成する。モニタ１０５上のダイアログボックス表示は、トラステッドコンポーネント２６０のセキュアなメモリ領域においてディスプレイインタフェースコンポーネント７０１によって直接生成される。ユーザのスマートカード５０３からダウンロードされる画像１００１の表示は、ユーザに対し、ダイアログボックスがトラステッドコンポーネントによって生成されていることの視覚的確認を与える。トラステッドコンポーネントは、スマートカードに格納された画像データにアクセスすることができる、コンピュータエンティティの唯一の要素であるためである。セキュリティ監視ダイアログボックスには、コンピュータエンティティの動作（本明細書では説明しない）のファイル監視モードにおいて起動される「ファイル」用のアイコン１００２と、イベント監視動動作用の「イベント」アイコン１００３がある。ユーザは、ステップ９０２において、イベントアイコン１００３上でポインティングデバイス１１５を動作させて「イベント」アイコン１００３をクリックすることにより、イベント監視メニュー１１００を選択する。「イベント」アイコンの起動時、トラステッドコンポーネントは、第２のダイアログボックスを生成する。この第２のダイアログボックスは、上述したようなイベントモニタメニュー１１００に対する背景として表示される予めロードされたユーザの画像も有する、イベント監視メニュー１１００を含む。イベントモニタメニューは、データエントリ領域１１０１～１１０３を有するダイアログボックスを含み、その領域の各々は、ユーザファイル、ドライバまたはアプリケーション等のコンピュータプラットフォーム上のアイテムを選択するためのドロップダウンメニューを有する。一般に、イベントが発生するとイベントデータをもたらすコンピュータプラットフォームのいかなる物理または論理コンポーネントも、トラステッドコンポーネントによって選択することができる。説明を簡単にするために、以下では、主にデータファイル、アプリケーションプログラムおよびドライバを選択した場合に関連して説明するが、本明細書で説明する方法および原理は、コンピュータプラットフォームのコンポーネントおよび機能の一般的なセットにも適用可能である、ということが理解されよう。選択ボックス１１０１～１１０３の各々においてドロップダウンメニューを起動することにより、コンピュータプラットフォームに存在するデータファイル、ドライバまたはアプリケーションの対応するそれぞれのリストの一覧が示される。ユーザは、ステップ９０４、９０５、９０６において、従来からの方法でドロップダウンメニューから選択されたアイコン上でポインティングデバイスを起動することにより、これらのファイルおよび／またはアプリケーションおよび／またはドライバのいずれかを選択することができる。更に、イベントモニタメニューは、イベント選択メニュー１１０４を含む。イベント選択メニューは、選択ボックス１１０１、１１０２、１１０３においてそれぞれ選択されるファイル、アプリケーションまたはドライバに対し、トラステッドコンポーネント内でイベントロガー７０２によって監視することができる複数のイベントタイプのリストを示す。監視することができるイベントのタイプは、以下のイベントをそのセット内に含む。すなわち、選択されたファイルがアプリケーションまたはユーザによってコピーされるというイベントであるファイルコピー、指定されたファイルがアプリケーションまたはユーザによって保存されるというイベントであるファイル保存、ファイルがアプリケーションまたはユーザによってリネームされたというイベントであるファイルリネーム、ファイルがアプリケーションまたはユーザによってオープンされているというイベントであるファイルオープン、ファイル内のデータがオーバライトされたというイベントであるファイルオーバライト、ファイル内のデータがいずれかのユーザ、アプリケ

ーションまたは他のエンティティによって読出されたというイベントであるファイル読出し、ファイル内のデータが、ユーザ、アプリケーションまたは他のエンティティによって変更されているというイベントであるファイル変更、ファイルがコンピュータエンティティの印刷ポートに送信されたというイベントであるファイル印刷、特定のドライバがいずれかのアプリケーションまたはファイルによって使用されたというドライバ使用、ドライバが再構成されたというイベントであるドライバ再構成、ドライバ使用イベントのサブセットであり、モデム使用されたか否かに適用するモデム使用、ディスクドライブが何らかの書込みまたは読出しで使用されたというイベントであるディスクドライブ使用、アプリケーションがオープンされたというイベントであるアプリケーションオープン、およびアプリケーションがクローズされたというイベントであるアプリケーションクローズ、である。ユーザは、ダイアログボックス１１００において監視されるアプリケーション、ドライバまたはファイル、及びイベントを選択すると、監視セッションを起動するために、視覚的に変化する確認キーアイコン１１０５によって確認される確認キー１３５を起動する。監視セッションはユーザのスマートカード表示からのユーザの画像１００１を有するダイアログボックス１１００の使用により、および独立して確認キー１３５を押下することによってのみ、起動することができる。モニタ１００上の画像１００１の表示により、ユーザは、トラステッドコンポーネントがダイアログボックスを生成していることを確信することができる。コンピュータプラットフォームとは独立してトラステッドコンポーネント２０２に直接入力される、確認キー１３５がユーザによって押下されることにより、トラステッドコンポーネントに対し、何か他のエンティティ、例えばウイルス等ではなくて、ユーザが監視セッションを起動している、という直接の確認が与えられる。

【０１２３】

また、ユーザは、データ入力ウインドウ１１０６において、開始時刻および日付と停止時刻および日付とを入力することにより、監視期間を指定することもできる。代替的には、指定されたエンティティにおける１つのイベントが監視される場合、ユーザは、最初のイベントのみを選択するボックス１１０７においてポインティングデバイス１１５を用いて確認することにより、そのイベントのみの監視を指定することができる。

【０１２４】

ここで、２つの動作モードについて説明する。第１の動作モードでは、ユーザが指定した期間に、指定されたエンティティの連続したイベント監視が発生する。第２の動作モードでは、ユーザが指定したイベントが発生するまで、またはそのユーザが指定したイベントを監視するユーザが指定した期間が経過するまで、指定されたエンティティの連続した監視が発生する。

【０１２５】

図１２に、ユーザが指定した監視期間に亙る指定された論理または物理エンティティの連続した監視に対する手続きを示す。

【０１２６】

図１２には、本明細書において図８乃至図１１を参照して上述したようなイベント監視セッションを開始するユーザ入力に応答して、トラステッドコンポーネント２６０により動作されるプロセスステップの概略が示されている。ステップ１２００において、ディスプレイインタフェース７０１は、データバス２２５を介しておよびトラステッドコンポーネントの通信インタフェース７００を介して、ポインティングデバイス１１５、キーボード１１０を使用して入力される、ダイアログボックスを介するユーザからのコマンドを受取る。イベントロガー７０２は、ユーザ空間のエージェント５１１に対し、イベント監視を開始するよう命令する。イベントロガー７０２を構成する命令は、トラステッドコンポーネント２６０内に常駐するメモリ領域内に格納されている。更に、イベントロガー７０２は、トラステッドコンポーネントのメモリ領域内で実行される。対照的に、エージェント５１１を構成する命令は、ホストプロセッサで、すなわちトラステッドコンポーネントのＣＰＵ独自のプログラム領域４０３において実行されるのに適した形態で、トラステッドコンポーネント２６０内部に格納されるが、エージェント５１１は、信頼されないユーザ

空間内、すなわちトラステッドコンポーネント２６０外部で実行される。エージェント５１１は、イベントロガー７０２から監視されるファイル、アプリケーションおよび／またはドライバの詳細を受取る。ステップ１２００において、エージェント５１１は、指定された論理エンティティ（例えば、ファイル、アプリケーションまたはドライバ）から一連のイベントデータを受取る。かかる監視は、連続したプロセスであり、エージェント５１１は、かかるイベントデータがオペレーティングシステムによって（例えば、ファイルに関するイベントをログするための機能を含むMicrosoft Windows4.0(R)オペレーティングシステムにおいて）自動的に格納されるデータファイルを定期的に読出すことにより、ステップ１２００を実行することもできる。しかしながら、セキュリティを最大化するために、エージェント５１１は、応答を引出すためにファイル、アプリケーションまたはドライバに直接問合せることにより、イベントデータ自体を定期的に収集することが好ましい。ステップ１２０１において、エンティティのイベントに関する収集されたデータは、トラステッドコンポーネント２６０に直接報告され、トラステッドコンポーネント２６０は、その後それらをステップ１２０２においてトラステッドメモリ領域に格納する。ステップ１２０３において、イベントロガーは、イベント監視セッションの開始からユーザが指定した所定の監視期間が経過したかチェックする。イベント監視セッション期間がまだ経過していない場合、イベントロガー７０２は、エージェント５１１によってサポートされる指定されたファイル、アプリケーションまたはドライバに対する更なるイベントを待ち続け、ステップ１２０３においてユーザが指定した所定の期間が経過するまで上述したようにステップ１２００～１２０２を実行する。ステップ１２０４において、トラステッドコンポーネントは、トラステッドメモリに格納されたイベントデータの内容を取出し、そのイベントログに対し暗号化機能７０３を適用することによりセキュアなイベントログファイルを提供する。本明細書において上述したようにイベントログファイルをセキュアにするプロセスにより、セキュアにされたファイルは、少なくとも以下の特性を有するものとなる。

・認証－許可されたユーザまたはプログラムが、イベントログファイルの起源を正確に突きとめることができなければならない。

・完全性－イベントログファイルが無許可の個人またはプログラムによって変更されていないことを確認できなければならない。

【０１２７】

任意選択事項であるが、セキュアにされたファイルは、機密性という特性－無許可のユーザまたはプログラムが、そのイベントログファイルに含まれる情報にアクセスすることができてはならない－と、否認拒絶性という特性－データの適正な認証は、後に不正に否認されることが不可能である－とを有するべきである。

【０１２８】

ステップ１２０５において、トラステッドコンポーネントは、セキュアなイベントログファイルをメモリ装置に書込む。メモリ装置は、トラステッド空間にあってもユーザ空間にあってもよい。例えば、セキュアなイベントログファイルを、ハードディスクドライブ２４０のユーザがアクセス可能な部分に格納することができる。

【０１２９】

指定されたファイル、アプリケーションまたはドライバで発生した複数のイベントを記述するデータを含むセキュアなイベントログファイルを提供することにより、ファイルを読出すユーザは、ファイルのデータがトラステッドコンポーネントによって書かれており、破損していない、ということを確信することができる。データに対する破損は、即時に明らかとなる。本明細書における最良の形態では、イベントログファイルをセキュアにすることは、本技術分野において既知である、データの任意のチャンクを連鎖させる連鎖アルゴリズムを適用することによって行われる。かかる連鎖プロセスでは、前の暗号化プロセスの出力を使用して、次の暗号化プロセスが初期化される。各暗号化データブロックのデータ量は、単一のプレーンテキストブロックではなく、任意の長さのデータである。当該技術分野において既知のかかる連鎖アルゴリズムの詳細は、Menezes Vanoorschot, Vanst

oneによる「Handbook of Applied Cryptography」の２２９頁に記載されている。連鎖プロセス中に使用される鍵は、トラステッドコンポーネント２６０内に格納される鍵であり、好ましくはトラステッドコンポーネントの秘密署名鍵である。そして、セキュアにされたイベントログの妥当性は、トラステッドコンポーネントの公開署名鍵を処理する任意のエンティティによって容易に確認することができる。かかる方法は、情報セキュリティの当業者には周知である。

【０１３０】

イベントデータは、好ましくは、追加のデバイスドライバを使用することによって収集される。ＮＴは、追加のデバイスドライバを現存のデバイスドライバの間に挿入することができるように設計されている。従って、ファイル、アプリケーションおよび他のデバイスドライバへのアクセスをトラップし、対話（相互作用）の詳細をイベントデータとして提供するドライバを設計し挿入することが可能である。設計に関する情報およびデバイスドライバの使用は、例えば、「The Windows NT Device Driver Book」（著者A.Baker、Prentice Hall出版）に見ることができる。また、「BlueWater Systems」等の営利会社が、デバイスドライバツールキットを販売している。

【０１３１】

図１３には、上述したように、ダイアログボックスを介するユーザによるデータ入力によって指定される特別なイベントの１つを監視するための、トラステッドコンポーネントおよびエージェント５１１によって適用される、１組のプロセスステップが示されている。監視される特別なイベントの詳細は、ステップ１３００においてユーザによって指定される。ステップ１３０１において、特定のエンティティ、例えば監視されるファイルアプリケーションまたはドライバの詳細が入力される。ステップ１３０２において、監視されるイベントタイプおよびエンティティの詳細が、トラステッドコンポーネントからエージェント５１１に送信される。そして、エージェントは、ステップ１３０３において、その特定の指定されたエンティティ上のイベントを連続的に監視する。ステップ１３０４においてエージェントにより、いずれかのイベントが発生したかが定期的にチェックされ、いずれのイベントも発生していない場合、エージェントは指定されたエンティティをステップ１３０３において監視し続ける。イベントが発生した場合、ステップ１３０５において、詳細がトラステッドコンポーネントに返される。そして、トラステッドコンポーネントは、ステップ１３０６において、イベントデータに暗号化機能を適用することによりセキュアなイベントデータをもたらし、ステップ１３０７において、図１２を参照して上述したように、トラステッド空間かまたはユーザ空間のメモリ領域にセキュアなイベントデータを書込む。

【０１３２】

セキュアなイベントデータは、例えば監査に使用することができるログである。調査者は、セキュアなイベントデータからなるログを調査することができる。その調査者は、標準の暗号化技術を使用してイベントデータの完全性、およびそれが完全な状態であることを確認することができる。そして、調査者は、プラットフォームの履歴を構成することができる。これは、プラットフォームに対する攻撃、またはプラットフォームの疑わしい不正な使用を調査するために有用である。イベントデータは、ユーザによるかまたは一方的にプラットフォームの所有者により挙動を変更することができない公平なエンティティ（トラステッドコンポーネント２６０）によって収集されている。このため、イベントログは、プラットフォーム内のアクティビティの信用できる記録としての役割を果たす。イベントログを、報告書として発行したり、自動的に、例えば、本発明の範囲外であるコンピュータプログラムによって解釈することができる。

【０１３３】

イベントログに格納することができるイベントデータのタイプには、以下のものが含まれる。以下のリストは、非網羅的なものではなく、本発明の他の実施態様では、当業者によって認識されるような一般的な変更を行うことができる。すなわち、イベント発生の時刻、イベント発生の日付、パスワードが使用されたか否か、ファイルがコピーされた場合、

いずれの宛先にファイルがコピーされたか、ファイルが操作された場合、メガバイト単位でのファイルのサイズ、ファイルがオープンしていた時間、アプリケーションがオンラインであった時間、ドライバがオンライであった時間、ファイルがコピーされた先の、またはドライバがアクセスした、またはアプリケーションがアドレス指定した、インターネットアドレス、ファイルがコピーされた先の、アプリケーションがアドレス指定した、またはドライバが通信した、ネットワークアドレスである。

【０１３４】

イベントログに格納されたイベントデータを、プラットフォームまたはトラステッドコンポーネントのデータファイルに物理的に格納することができる。イベントログデータは、第１のセキュアなイベントデータが第２のイベントデータをセキュアにするために使用され、第２のセキュアなイベントデータが第３のイベントデータをセキュアにするために使用され、等のように、連鎖機能を使用してセキュアにされる。そのためデータの連鎖に対するいかなる変化も明らかである。

【０１３５】

また、トラステッドコンポーネントは、セキュアなイベントログデータを提供するだけでなく、イベントの報告書を編集することができる。報告書を、モニタ１０５に表示することができる。報告書の内容を構成することができる項目には、上記イベントログにおいて指定されるようなイベントと共に以下のものが含まれる。すなわち、イベントの時刻、イベントの日付、パスワードが使用されたか否か、ファイルのコピー先、ファイルのサイズ（メガバイト単位）、ファイルまたはアプリケーションがオープンしていた時間、ドライバがオンラインであった時間、ドライバが使用されていた時間、使用されていたポート、通信していたインターネットアドレス、通信していたネットワークアドレスである。

【０１３６】

エージェント５１１は、トラステッドコンポーネント２６０に代ってイベント監視動作を実行するが、トラステッドコンポーネント２６０はトラステッド空間５１３にあるのに対し、エージェント５１１は、コンピュータプラットフォームのユーザ空間で動作しなければならない。エージェント５１１は、トラステッド空間５１３より本質的にセキュアでない環境にあるため、ウイルス等によるコンピュータプラットフォームへの悪質な攻撃による危険に晒されることになる可能性がある。トラステッドコンポーネントは、２つのメカニズムのいずれかにより、かかる悪質な攻撃の可能性に対処する。第１に、代替的な実施態様では、エージェント５１１は、トラステッドコンポーネント２６０内にのみ常駐することができる。エージェント５１１が実行するすべての動作は、イベントデータを収集するために、トラステッドコンポーネントの通信インタフェース７００を介して動作するコード監視コンポーネント６００により、トラステッドユーザ空間５１３内から実行される。しかしながら、この手法の欠点は、エージェント５１１が存在しないため、それがトラステッドコンポーネント２６０と残りのユーザ空間５０４との間のバッファとして作用することができない、ということである。

【０１３７】

一方、エージェント５１１を構成するコードを、トラステッドコンポーネント２６０のトラステッドメモリ領域のトラステッド空間に格納し、定期的にユーザ空間５０４に「送出する(launched)」ことができる。すなわち、監視セッションが開始すると、エージェントを、トラステッドコンポーネントからコンピュータプラットフォームのユーザ空間またはカーネル空間にダウンロードすることができ、それはそこに常駐して、その連続的な監視機能を実行する。本発明者が考える最良の態様であるこの第２の方法では、エージェント５１１が危険に晒されることのリスクを低減するために、トラステッドコンポーネントは、周期的間隔で、トラステッド空間のセキュアなメモリ領域からユーザ空間にエージェント全体を再送出することができ、および／またはユーザ空間のエージェント５１１を定期的に監視することにより、それがトラステッドコンポーネントによる定期的な問合せに対して正しく応答していることを確実にすることができる。

【０１３８】

エージェント５１１をトラステッド空間のその永久的な常駐からユーザ空間に送出する場合、これは、トラステッドコンポーネントからコンピュータプラットフォームへ、エージェントを構成するコードをコピーすることにより成し遂げられる。監視セッションがユーザによって指定される有限の監視期間を有する場合、エージェント５１１がユーザ空間に存在する期間を、監視セッションの期間と一致するように構成することができる。すなわち、エージェントは、監視セッションの継続時間中にのみ存在し、監視セッションが終了すると、エージェントをユーザ／カーネル空間から削除することができる。イベントおよび／またはエンティティの新たなセットに対する新たな監視セッションを開始するために、新たなエージェントをその監視セッションの継続時間にユーザ空間に送出することができる。

【０１３９】

ユーザの指定に従って何日かまたは何ヶ月かの延長期間に亙って延長することが可能な監視セッション中、トラステッドコンポーネントは定期的にエージェント自体を監視する。

【０１４０】

図１４には、コンピュータプラットフォーム上のトラステッドコンポーネント２６０およびエージェント５１１によって実行される、トラステッド空間からユーザ空間にダウンロードされるエージェント５１１を送出するプロセスステップの概略が示されており、そこではトラステッドコンポーネントは、コンピュータプラットフォーム上にセットアップされ、実行しているエージェント５１１を監視する。

【０１４１】

ステップ１４００において、トラステッドコンポーネントのセキュアなメモリ領域に格納されたエージェント５１１を構成するネイティブコードが、ステップ１４０１においてトラステッドコンポーネントから直接エージェントコードを読出すコンピュータプラットフォームによって、コンピュータプラットフォームにダウンロードされる。ステップ１４０２において、コンピュータプラットフォーム上のデータプロセッサは、コンピュータプラットフォーム上のユーザ空間に常駐するネイティブエージェントコードの実行を開始する。エージェントは、ステップ１４０３において、上述したように連続的に動作し続ける。その間、トラステッドコンポーネント２６０は、ステップ１４０４において、適当な選択された期間後、ナンスチャレンジメッセージを生成し、ステップ１４０５においてこのナンスを、それを受取るエージェントに送る。ナンスは、トラステッドコンポーネントによって生成されるランダムビットシーケンスから構成することができる。ナンスの目的は、トラステッドコンポーネントが、エージェントがまだそこにありまだ動作していることをチェックできるようにすることである。ナンスがエージェントによって返されない場合、トラステッドコンポーネントは、エージェントが動作するのを中止し、および／または危険に晒されたことを知る。ステップ１４０７において、エージェントはナンスに署名し、ステップ１４０８において、エージェントは署名したナンスをトラステッドコンポーネントに返す。トラステッドコンポーネントは、ステップ１４０９において署名されたナンスを受取り、その後予め選択された期間後新たなナンスを送るステップ１４０４を繰返す。所定の待機期間後（ステップ１４０６）、ステップ１４０４においてナンスがエージェントに送られた時に、トラステッドコンポーネントがエージェントから返されるナンスを受取っていない場合、ステップ１４１０において、トラステッドコンポーネントは、エージェント５１１が正しく動作していないこと、及び、ファイル監視動作が危険に晒された可能性があることを示すアラーム信号を生成する。それは、モニタに表示されることとなる。

【０１４２】

第２の実施態様では、トラステッドコンポーネント２６０は、コンピュータプラットフォームに常駐するオペレーティングシステムによって提供されるユーティリティおよび機能を使用するプログラムにより、データおよびプラットフォームリソースの使用に関する情報を収集するように動作することができる。この情報は、アクセス権、ファイル使用、アプリケーション使用、メモリ（ＲＡＭ）利用、メモリ（ハードディスク）利用およびメイ

ンプロセッサ命令サイクル割付けの統計量を含むことができる。

【０１４３】

従前の特許出願「Trusted Computing Platform」には、トラステッドコンポーネントが他のエンティティと協動し、トラステッドコンポーネントによって測定された完全性メトリクスの値をそれらに報告する方法が記載されている。そして、それら他のエンティティは、測定されたメトリクスを、トラステッドサードパーティによって発行されるデジタル証明書に含まれる適正な値と比較する。その従前の特許出願は、静的メトリクスの例、すなわちプラットフォームのＢＩＯＳメモリのダイジェストを与える。また、この出願の方法によって作成された測定値を、完全性メトリクスとして報告することもできる、それらは常に変化している可能性があるため、動的完全性メトリクスと呼ばれる。すなわち、測定された値は、その時点で数秒前に測定された値と異なる可能性がある。エンティティは、測定された動的メトリクスの現在の値を繰返し要求しなければならない。例えば、ある完全性メトリクスは、本明細書で説明する最良の態様に従って、発生したイベントがデータへのアクセスを統制するポリシーと矛盾するか否かを示すブール値を含む。例えば、Javaアプレット等のモバイルソフトウェアが、書込み許可を有していなかったにも関わらずユーザ空間のファイルに対して書込みを行った場合、かかるブール値は真（TRUE）となる。

【０１４４】

他の完全性メトリクスは、異常な挙動が検出されたことを示すブール値を含む。かかる異常な挙動は、必ずしも、コンピュータプラットフォームが危険になったことを示すとは限らないが、コンピュータプラットフォームの使用における警告を示唆することができる。コンピュータプラットフォームと通信する慎重なエンティティは、第２の完全性メトリクスが、異常な挙動が検出されたことを示す場合、そのプラットフォームで非常に敏感なデータを処理しないよう選択することができる。プラットフォームが繰返し動作を行うように使用されない限り、異常な挙動を正確に定義することは困難である。本明細書における最良の態様では、異常なデータを、トラステッドコンポーネントにより、所定の期間に亙って編集された挙動のそれまでの平均測定値の所定数の標準偏差外にあるコンピュータプラットフォームのリソースの挙動であるものとして、定義し、監視することができる。例えば、データファイルが、それまでに所定期間に亙り特定の範囲、例えば１４０～１８０メガバイト内のサイズを有していた場合、ファイルサイズが急激に、例えば５００メガバイトまで増大し、予め設定することができる所定数の標準偏差を超えると、第２の完全性メトリクスブール値は、状態を真の状態に変化させて、異常な挙動を示すことができる。

【０１４５】

更なる例として、アプリケーション、例えばワードプロセッシングアプリケーションが所定範囲、例えば１日あたり１～１０回の範囲の頻度でデータファイルを保存するという履歴を有していた場合において、アプリケーションの挙動が、例えば１日あたり１００回保存するというふうに大きく変化した場合には、そのパラメータを監視するブールメトリクスは、真の状態をトリガすることができる。

【０１４６】

当然ながら、上述したように、トラステッドコンポーネントは、完全性チャレンジ（完全性要求）によってポーリングされるのを待つ代りに、緊急のイベントを報告する際に能動的な役割を果たす場合がある。イベントを、トラステッドコンポーネント２６０内部で、トラステッドコンポーネント内部に格納されるポリシールールと一致させることができる。イベントが、ポリシーが非常に重要であるとみなすルールを破った場合、トラステッドコンポーネント２６０は、関連するエンティティに対しアラーム指示メッセージを直ちに送り、および／または図１０および図１１に示すダイアログボックスのスタイルを使用して、モニタ１０５上でユーザに対し緊急メッセージを表示することができる。

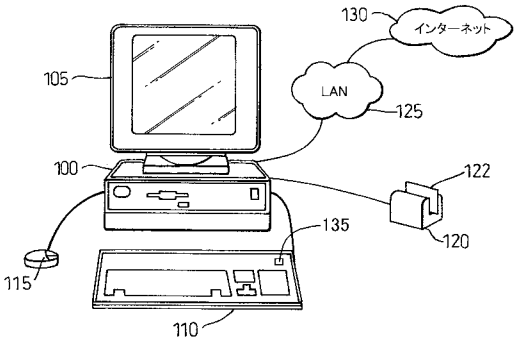
【図面の簡単な説明】

【図１】　本発明の好適な実施態様に従って動作するのに適したコンピュータシステムを示す図である。

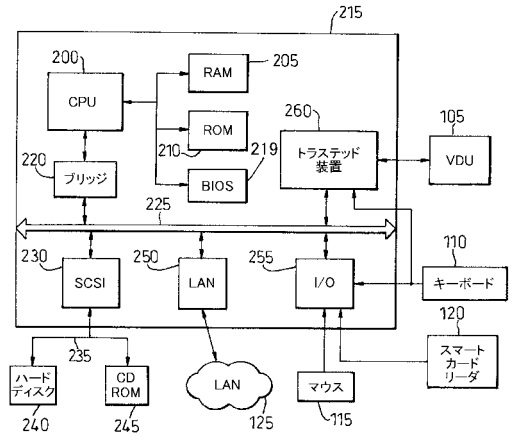
【図２】　本発明の好適な実施態様に従って動作するのに適したコンピュータプラットフ

ォームのハードウェアアーキテクチャを示す図である。
【図３】　本発明の好適な実施態様に従って動作するのに適したトラステッド装置のハードウェアアーキテクチャを示す図である。
【図４】　本発明の好適な実施態様に従って動作するのに適したスマートカード処理エンジンのハードウェアアーキテクチャを示す図である。
【図５】　コンピュータプラットフォームに常駐する監視されたユーザ空間と、トラステッドコンポーネントに常駐するトラステッド空間に分割されたコンピュータエンティティの論理アーキテクチャを概略的に示す。
【図６】　コンピュータプラットフォームで発生するイベントを監視し、トラステッドコンポーネントに報告する、監視エージェントのコンポーネントを概略的に示す。
【図７】　トラステッドコンポーネント自体の論理コンポーネントを概略的に示す。
【図８】　モニタ装置上の表示を介してユーザとトラステッドコンポーネントとの間のセキュアな通信を確立するために実行されるプロセスステップを概略的に示す。
【図９】　ディスプレイモニタを使用してセキュリティ監視機能を選択するためのプロセスステップを概略的に示す。
【図１０】　トラステッドコンポーネントによって生成される第１のダイアログボックス表示を概略的に示す。
【図１１】　ユーザによるデータの入力のために使用される第２のダイアログボックス表示を概略的に示す。
【図１２】　コンピュータプラットフォーム上のファイル、アプリケーションまたはドライバなどの、論理および／または物理エンティティを監視するために、監視エージェントとトラステッドコンポーネントとによって実行される処理を概略的に示す。
【図１３】　コンピュータプラットフォームにおいて指定されたイベントを連続的に監視するために、エージェントとトラステッドコンポーネントとにより処理されるプロセスステップを概略的に示す。
【図１４】　コンピュータプラットフォーム上にエージェントを実装し、コンピュータプラットフォーム上のエージェントの存在および完全性を監視するために、監視エージェントとトラステッドコンポーネントとの相互作用（対話）によって実行されるプロセスステップを概略的に示す。
【図１５】　コンピューティング装置の完全性メトリクスを取得することに関連するステップを示すフローチャートである。
【図１６】　トラステッドコンピューティングプラットフォームと、完全性を検査するトラステッドプラットフォームを含むリモートプラットフォームとの間の通信を確立することに関連するステップを示すフローチャートである。
【図１７】　スマートカードとホストプラットフォームとを相互に認証するプロセスを示すフローチャートである。
【図１８】　トラステッドディスプレイプロセッサとして動作するように構成されたトラステッド装置と、本発明の好適な実施態様に従って動作するのに適したスマートカードを含むコンピュータプラットフォームの機能アーキテクチャを示す図である。

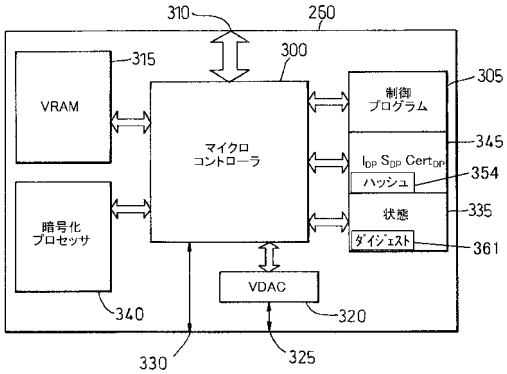
【図１】



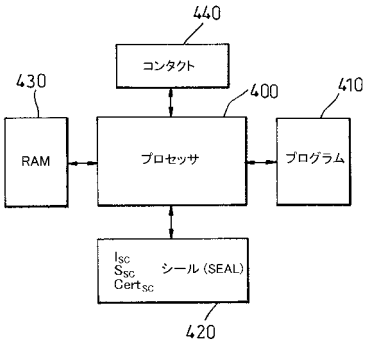
【図２】



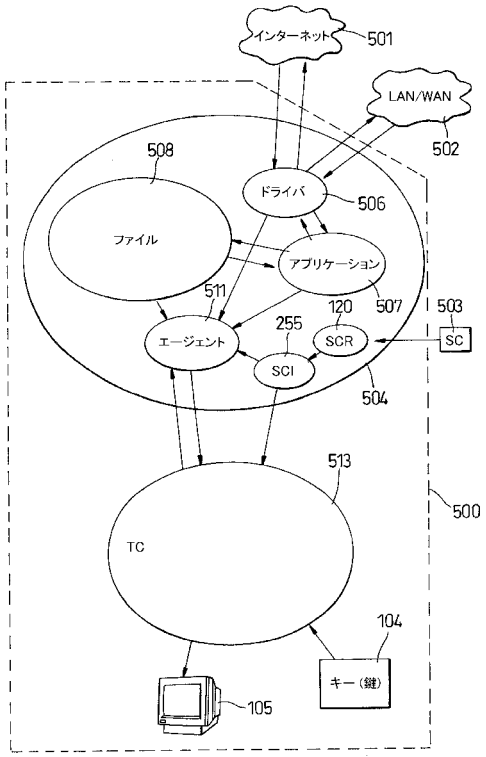
【図３】



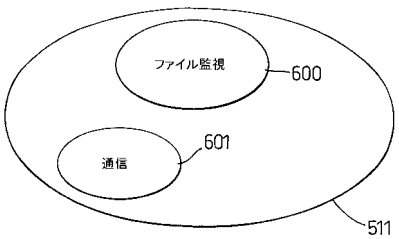
【図４】



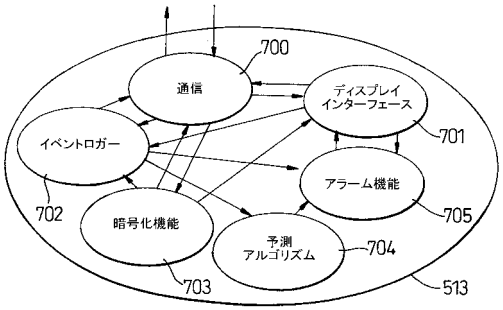
【図５】



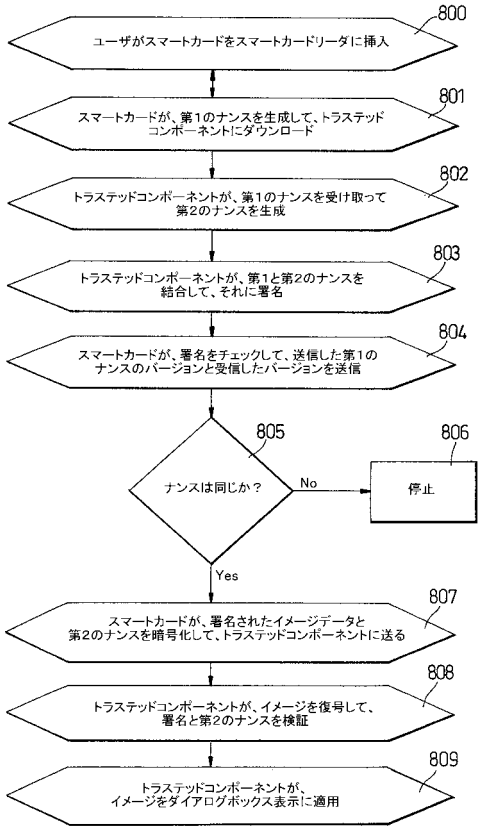
【図６】



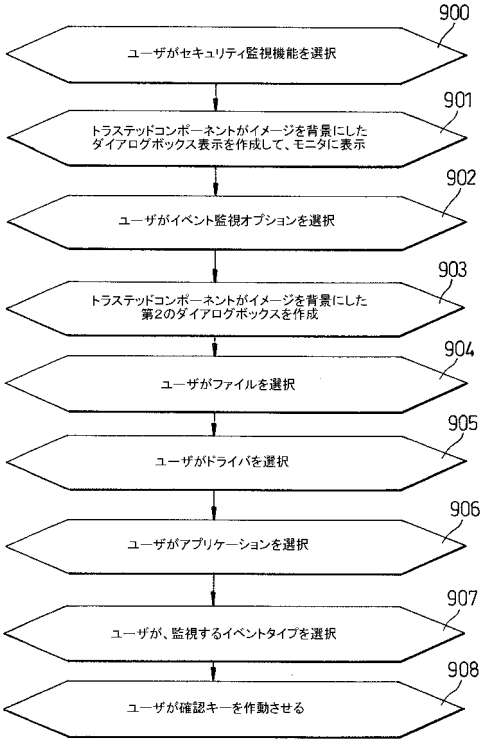
【図７】



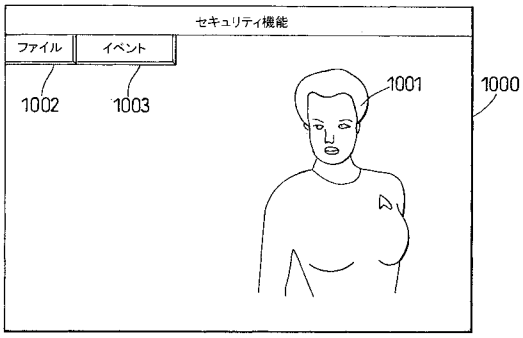
【図８】


800
ユーザがスマートカードをスマートカードリーダに挿入
801
スマートカードが、第1のナンスを生成して、トラステッドコンポーネントにダウンロード
802
トラステッドコンポーネントが、第1のナンスを受け取って第2のナンスを生成
803
トラステッドコンポーネントが、第1と第2のナンスを結合して、それに署名
804
スマートカードが、署名をチェックして、送信した第1のナンスのバージョンと受信したバージョンを送信
805
ナンスは同じか？
No
806
停止
Yes
807
スマートカードが、署名されたイメージデータと第2のナンスを暗号化して、トラステッドコンポーネントに送る
808
トラステッドコンポーネントが、イメージを復号して、署名と第2のナンスを検証
809
トラステッドコンポーネントが、イメージをダイアログボックス表示に適用

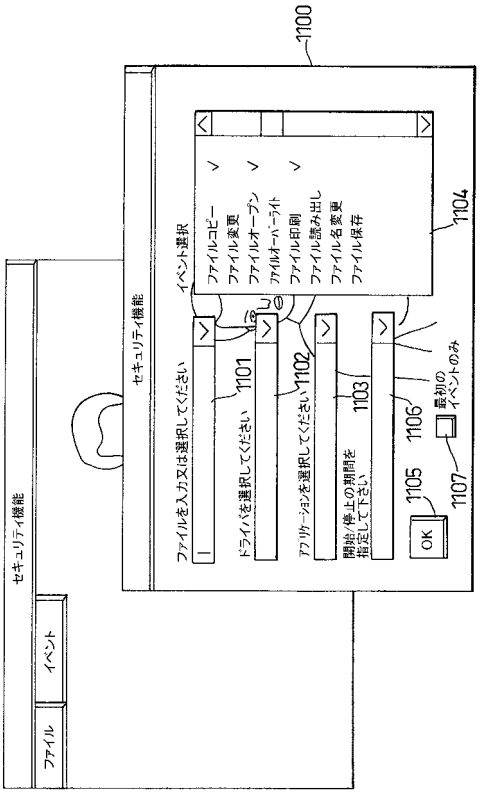
【図９】


900
ユーザがセキュリティ監視機能を選択
901
トラステッドコンポーネントがイメージを背景にしたダイアログボックス表示を作成して、モニタに表示
902
ユーザがイベント監視オプションを選択
903
トラステッドコンポーネントがイメージを背景にした第2のダイアログボックスを作成
904
ユーザがファイルを選択
905
ユーザがドライバを選択
906
ユーザがアプリケーションを選択
907
ユーザが、監視するイベントタイプを選択
908
ユーザが確認キーを作動させる

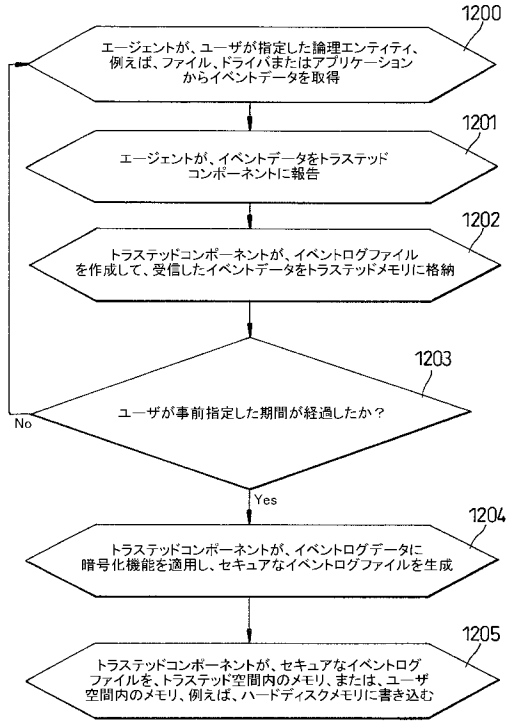
【図１０】


セキュリティ機能
ファイル
イベント
1002
1003
1001
1000

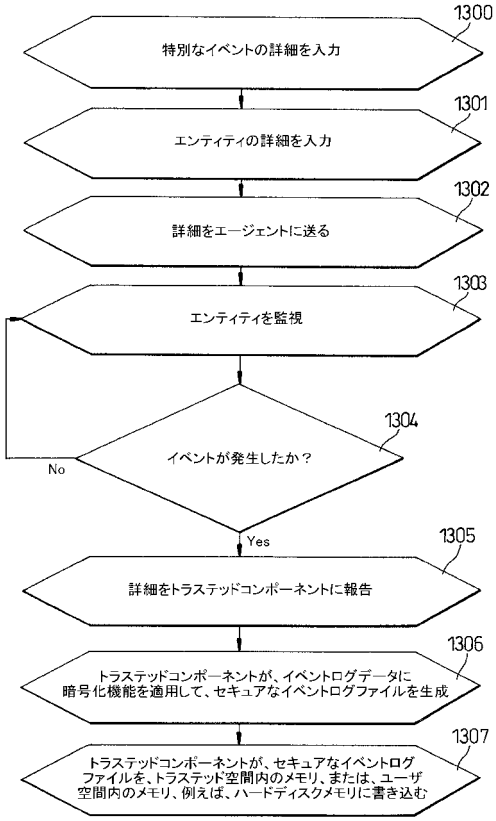
【図１１】


1100
セキュリティ機能
イベント選択
ファイルコピー
ファイル変更
ファイルオープン
ファイルオーバーライト
ファイル印刷
ファイル読み出し
ファイル名変更
ファイル保存
1104
ファイルを入力又は選択してください
1101
ドライバを選択してください
1102
アプリケーションを選択してください
1103
開始/停止の期間を指定して下さい
1106
最初のイベントのみ
1105
OK
1107
セキュリティ機能
イベント
ファイル

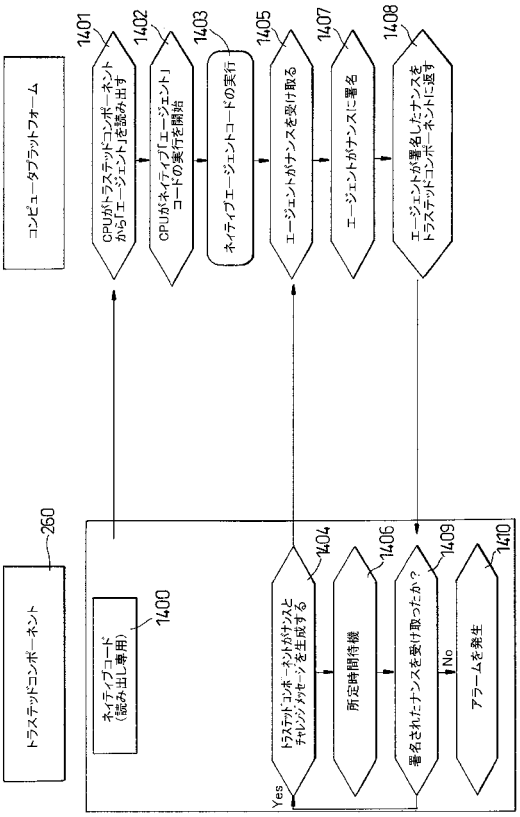
【図１２】



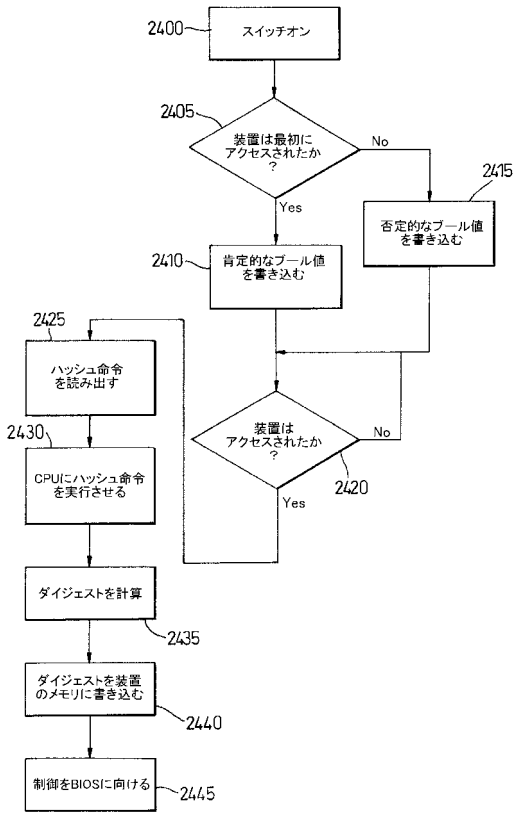
【図１３】



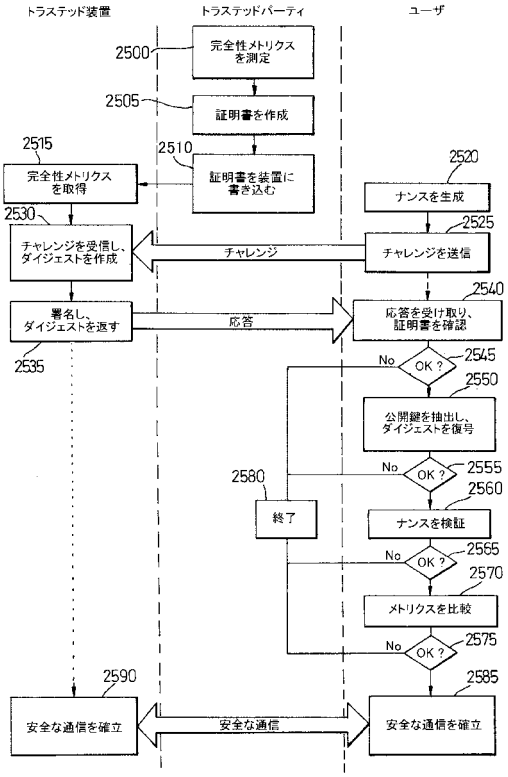
【図１４】



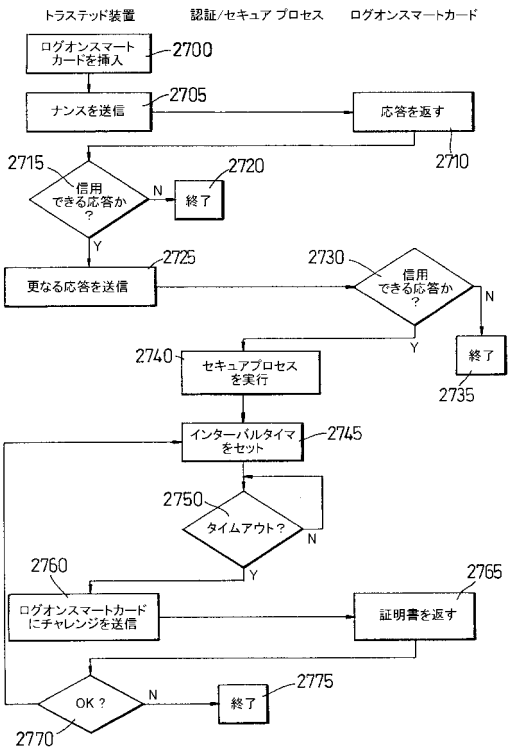
【図１５】



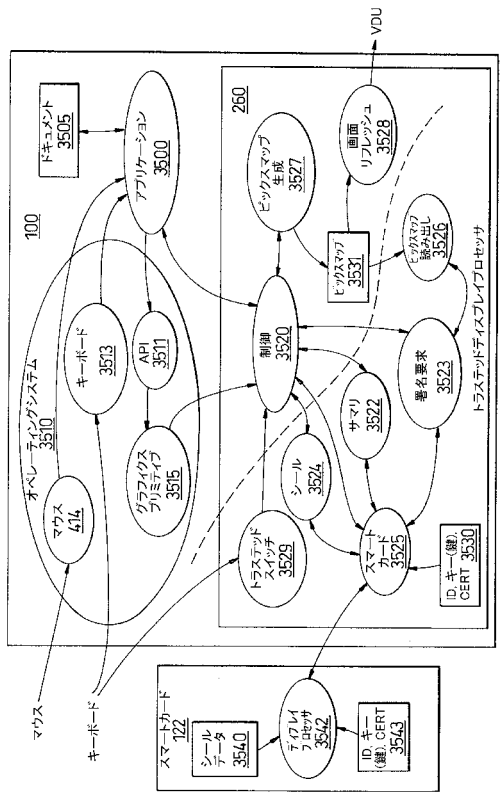
【図１６】


トラステッド装置
トラステッドパーティ
ユーザ
2500
完全性メトリクスを測定
2505
証明書を作成
2510
証明書を装置に書き込む
2515
完全性メトリクスを取得
2520
ナンスを生成
2525
チャレンジを送信
チャレンジ
2530
チャレンジを受信し、ダイジェストを作成
2535
署名し、ダイジェストを返す
応答
2540
応答を受け取り、証明書を確認
No
OK？
2545
2550
公開鍵を抽出し、ダイジェストを復号
2555
2560
ナンスを検証
2565
2570
メトリクスを比較
2575
2580
終了
2585
2590
安全な通信を確立
安全な通信
安全な通信を確立

【図１７】


トラステッド装置
認証/セキュア プロセス
ログオンスマートカード
ログオンスマートカードを挿入
2700
ナンスを送信
2705
応答を返す
2710
2715
信用できる応答か？
N
終了
2720
Y
更なる応答を送信
2725
2730
信用できる応答か？
N
終了
2735
Y
2740
セキュアプロセスを実行
インターバルタイマをセット
2745
2750
タイムアウト？
N
Y
2760
ログオンスマートカードにチャレンジを送信
2765
証明書を返す
OK？
N
終了
2775
2770

【図１８】


VDU
260
100
ドキュメント 3505
アプリケーション 3500
画面リフレッシュ 3528
ビックスマップ生成 3527
ビックスマップ 3531
ビックスマップ読み出し 3526
制御 3520
署名要求 3523
サマリ 3522
シール 3524
スマートカード 3525
ID、キー(鍵)CERT 3530
トラステッドスイッチ 3529
トラステッドディスプレイプロセッサ
オペレーティングシステム 3510
キーボード 3513
API 3511
グラフィクスプリミティブ 3515
マウス 414
マウス
キーボード
スマートカード 122
シールデータ 3540
ディスプレイプロセッサ 3542
ID、キー(鍵)CERT 3543

フロントページの続き

(72)発明者　プラウドラー，グレーム，ジョン
イギリス国ブリストル・ビーエス３４・８エックスキュー，ストーク・ガイフォード，タッチストーン・アベニュー・５
(72)発明者　バラチェフ，ボリス
イギリス国ブリストル・ビーエス８・４エルティー，ホットウェルズ，グランビィ・ヒル，ラットランド・ハウス・７
(72)発明者　ピアソン，シアニ，リン
イギリス国ブリストル・ビーエス９・３ピーゼット，ウェストバーリー－オン－トリム，サンディリーズ・３５
(72)発明者　チャン，デイビッド
アメリカ合衆国カリフォルニア州９５０３０，モンテセレノ，メイズ・アベニュー・１６１１２

審査官　林　毅

(56)参考文献　特開平０９－２１４４９３（ＪＰ，Ａ）
特開平１０－２９３７０４（ＪＰ，Ａ）
特開平１０－２９３７０５（ＪＰ，Ａ）
特表平１０－５１０６４７（ＪＰ，Ａ）
特開平１１－００３２４８（ＪＰ，Ａ）
特開平１０－０８３３８２（ＪＰ，Ａ）
国際公開第９８／０４２１０３（WO，Ａ１）
国際公開第９８／０４５７７８（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　11/34
G06F　 9/445
G06F　11/30
G06F　21/00
G06F　21/22