(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6074026号
(P6074026)
(45)発行日　平成29年2月1日(2017.2.1)　(24)登録日　平成29年1月13日(2017.1.13)

(51)Int.Cl.　F I
G06F 9/50 (2006.01)　G06F 9/46 465A

請求項の数 17 (全 16 頁)

(21)出願番号　特願2015-501650(P2015-501650)
(86)(22)出願日　平成24年4月16日(2012.4.16)
(65)公表番号　特表2015-514253(P2015-514253A)
(43)公表日　平成27年5月18日(2015.5.18)
(86)国際出願番号　PCT/US2012/033748
(87)国際公開番号　WO2013/158060
(87)国際公開日　平成25年10月24日(2013.10.24)
審査請求日　平成26年9月18日(2014.9.18)

(73)特許権者　593096712
インテル　コーポレイション
アメリカ合衆国　９５０５４　カリフォルニア州　サンタ　クララ　ミッション　カレッジ　ブールバード　２２００
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(72)発明者　フェガデ，ヴィナイ
アメリカ合衆国　９７００６　オレゴン州　ビーヴァートン　ノースウエスト　エイヴォンデール　ドライヴ　１６６７５
最終頁に続く

(54)【発明の名称】スケーラブルでセキュアな実行

(57)【特許請求の範囲】
【請求項１】
第１の電子デバイスのコントローラであって、
第２の電子デバイスにおけるリモートプロセッサとのペアリングを確立し、
前記リモートプロセッサとの第１のセキュアな通信チャネルを作成し、前記第１のセキュアな通信チャネルが、当該コントローラと前記リモートプロセッサとの間で展開される共有の秘密によって少なくとも部分的にセキュアにされており、
前記第１のセキュアな通信チャネルを介して処理タスクの第１の部分を前記リモートプロセッサに伝送し、
第２の通信チャネルを介して前記処理タスクの前記第１の部分からログイン画面用のビットマップを受け取り、前記ビットマップが、前記共有の秘密を使用して暗号化されるとともに、ユーザ入力のための１つ以上の座標を備えており、
前記ビットマップを、当該コントローラに結合されるディスプレイモジュール上に提示し、
前記ビットマップ上の前記１つ以上の座標に対応する位置で、前記ディスプレイモジュールからログイン用のユーザ入力を受け取り、
前記ディスプレイモジュールから受け取った前記ユーザ入力が、ログインが認証されていることを示すとき、当該コントローラとリモートシステムとの間の通信セッションを開始する
ように構成されるロジックを備える、コントローラ。

【請求項２】
前記ロジックは、前記リモートプロセッサと通信する近距離無線通信インタフェースを備える、請求項１に記載のコントローラ。
【請求項３】
当該コントローラに結合されるローカルプロセッサを更に備え、該ローカルプロセッサは、
前記リモートプロセッサから前記処理タスクの前記第１の部分の出力を受け取り、
前記出力を、当該コントローラに結合されたディスプレイに提示する
ように構成されるロジックを備える、請求項１に記載のコントローラ。
【請求項４】
前記ローカルプロセッサは、
入力デバイスから入力を受け取り、
該入力を当該コントローラに渡す
ように構成されるロジックを更に備える、請求項３に記載のコントローラ。
【請求項５】
前記ユーザ入力を検証するように構成されるロジックを更に備える、請求項１に記載のコントローラ。
【請求項６】
電子デバイスであって、
信頼できないコンピューティング環境を実装するプロセッサと、
コントローラであって、
第２の電子デバイスにおけるリモートプロセッサとのペアリングを確立し、
前記リモートプロセッサとの第１のセキュアな通信チャネルを作成し、前記第１のセキュアな通信チャネルが、当該コントローラと前記リモートプロセッサとの間で展開される共有の秘密によって少なくとも部分的にセキュアにされており、
前記第１のセキュアな通信チャネルを介して処理タスクの第１の部分を前記リモートプロセッサに伝送し、
第２の通信チャネルを介して前記処理タスクの前記第１の部分からログイン画面用のビットマップを受け取り、前記ビットマップが、前記共有の秘密を使用して暗号化されるとともに、ユーザ入力のための１つ以上の座標を備えており、
前記ビットマップを、当該コントローラに結合されるディスプレイモジュール上に提示し、
前記ビットマップ上の前記１つ以上の座標に対応する位置で、前記ディスプレイモジュールからログイン用のユーザ入力を受け取り、
前記ディスプレイモジュールから受け取った前記ユーザ入力が、ログインが認証されていることを示すとき、当該コントローラとリモートシステムとの間の通信セッションを開始する
ように構成されるロジックを備える、コントローラと
を備える、電子デバイス。
【請求項７】
前記ロジックは、前記リモートプロセッサと通信する近距離無線通信インタフェースを備える、請求項６に記載の電子デバイス。
【請求項８】
前記コントローラに結合されるローカルプロセッサを更に備え、該ローカルプロセッサは、
前記リモートプロセッサから前記処理タスクの前記第１の部分の出力を受け取り、
前記出力を、前記コントローラに結合されたディスプレイに提示する
ように構成されたロジックを備える、請求項６に記載の電子デバイス。
【請求項９】
前記ローカルプロセッサは、

入力デバイスから入力を受け取り、
該入力を前記コントローラに渡す
ように構成されたロジックを更に備える、請求項８に記載の電子デバイス。
【請求項１０】
前記ユーザ入力を検証するように構成されたロジックを更に備える、請求項６に記載の電子デバイス。
【請求項１１】
第１の電子デバイスのコントローラと、第２の電子デバイスのリモートプロセッサとの間のペアリングを確立するステップと、
前記コントローラと前記リモートプロセッサとの間の第１のセキュアな通信チャネルを作成し、前記第１のセキュアな通信チャネルが、前記コントローラと前記リモートプロセッサとの間で展開される共有の秘密によって少なくとも部分的にセキュアにされているステップと、
前記第１のセキュアな通信チャネルを介して処理タスクの第１の部分を前記コントローラから前記リモートプロセッサへ伝送するステップと、
前記コントローラにおいて、第２の通信チャネルを介して前記処理タスクの前記第１の部分からログイン画面用のビットマップを受け取り、前記ビットマップが、前記共有の秘密を使用して暗号化されるとともに、ユーザ入力のための１つ以上の座標を備えているステップと、
前記ビットマップを、前記コントローラに結合されるディスプレイモジュール上に提示するステップと、
前記ビットマップ上の前記１つ以上の座標に対応する位置で、前記ディスプレイモジュールからログイン用のユーザ入力を受け取るステップと、
前記ディスプレイモジュールから受け取った前記ユーザ入力が、ログインが認証されていることを示すとき、前記コントローラとリモートシステムとの間の通信セッションを開始するステップと
を含む、方法。
【請求項１２】
前記コントローラ内のローカルプロセッサにおいて、前記リモートプロセッサから前記処理タスクの前記第１の部分の出力を受け取るステップと、
前記コントローラに結合されたディスプレイモジュール上に前記出力を提示するステップと
を更に含む、請求項１１に記載の方法。
【請求項１３】
前記ローカルプロセッサにおいて入力デバイスから入力を受け取るステップと、
前記ローカルプロセッサから前記コントローラに前記入力を渡すステップと
を更に含む、請求項１２に記載の方法。
【請求項１４】
前記ユーザ入力を検証するステップを更に含む、請求項１１に記載の方法。
【請求項１５】
非一時的コンピュータ読取可能媒体上に格納される論理命令を備えるコンピュータプログラムであって、コントローラによって実行されると、該コントローラに、
第２の電子デバイスにおけるリモートプロセッサとのペアリングを確立させ、
前記リモートプロセッサとの第１のセキュアな通信チャネルを作成させ、前記第１のセキュアな通信チャネルは、前記コントローラと前記リモートプロセッサとの間で展開される共有の秘密によって少なくとも部分的にセキュアにされており、
前記第１のセキュアな通信チャネルを介して処理タスクの第１の部分を前記リモートプロセッサに伝送させ、
第２の通信チャネルを介して前記処理タスクの前記第１の部分からログイン画面用のビットマップを受け取らせ、前記ビットマップは、前記共有の秘密を使用して暗号化される

とともに、ユーザ入力のための１つ以上の座標を備えており、
前記ビットマップを、前記コントローラに結合されるディスプレイモジュール上に提示させ、
前記ビットマップ上の前記１つ以上の座標に対応する位置で、前記ディスプレイモジュールからログイン用のユーザ入力を受け取らせ、
前記ディスプレイモジュールから受け取った前記ユーザ入力が、ログインが認証されていることを示すとき、前記コントローラとリモートシステムとの間の通信セッションを開始させる
ように構成される、コンピュータプログラム。
【請求項１６】
前記論理命令は、前記リモートプロセッサと通信する近距離無線通信インタフェースを備える、請求項１５に記載のコンピュータプログラム。
【請求項１７】
請求項１５又は１６のいずれかに記載のコンピュータプログラムを記憶するコンピュータ読取可能記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本明細書で説明される主題は、一般に、コンピューティングの分野に関し、より具体的には、電子デバイスがリモート電子デバイスの処理能力を用いることを可能にするシステム及び方法に関する。
【背景技術】
【０００２】
典型的な電子商取引において、小売業者（及び内在するエコシステム）は、取引を行っている個人が認証された人であるか分からない。不正な取引がオンラインのエコシステムによって受理されると、一般的に、依拠しているパーティ、この例では小売業者が負担するか、又はだまされた個人が負担する、潜在的な不正コストが存在する。
【０００３】
オンライン空間における別の弱点は、絶えず存在するシステムマルウェアの脅威である。このシステムマルウェアは、多くの場合、権限のない個人が使用するために、支払の認証情報を含む個人情報を盗むのに使用される。この脅威は、自身の情報が危険にさらされるのを恐れるために、オンラインアクティビティを行わない人口の割合に影響を与える。これにより、オンライン取引を通して得られる効率が低減し、興味を持った個人によって購入される商品及びサービス量が制限され、そしてオンライン取引の成長が制限される。
【先行技術文献】
【非特許文献】
【０００４】
【非特許文献１】「Guidelines on GPRS Handset Requirements, Global System for Mobile Communications/GSM Association」、 Ver. 3.0.1、２００２年１０月
【発明の概要】
【発明が解決しようとする課題】
【０００５】
一部のコンピューティングシステムは、メインのプロセッサとは別個に、認証プロセスを管理する信頼できる実行複合体（execution complex）に包まれるセキュアなコントローラを用いることができる。セキュアなコントローラは、限られた計算リソース及びメモリリソースしか有さないことがあり、その結果、計算コストの高いタスクは、セキュアなコントローラにとって実装することが難しい可能性がある。
【課題を解決するための手段】
【０００６】
したがって、計算コストの高いタスクをリモートのプロセッサにオフロードすることを

可能にするセキュアな実行を提供するシステム及び技術により有用性が見いだされる可能性がある。

【０００７】

詳細な説明は、図面を参照しながら記述される。

【図面の簡単な説明】

【０００８】

【図１】一部の実施形態に従って、スケーラブルでセキュアな実行を実装するインフラストラクチャを含むように構成され得る例示的な電子デバイスを示す概略図である。

【図２】一部の実施形態に従って、スケーラブルでセキュアな実行のための例示的なネットワークアーキテクチャを示す高レベルな概略図である。

【図３】一部の実施形態に従って、スケーラブルでセキュアな実行のための例示的なアーキテクチャを示す概略図である。

【図４】一部の実施形態に従って、スケーラブルでセキュアな実行を実装する方法の動作を示すフローチャートである。

【図５】一部の実施形態に従って、スケーラブルでセキュアな実行のための例示的なシステムを示す概略図である。

【発明を実施するための形態】

【０００９】

本明細書で説明されるのは、電子デバイスにおけるスケーラブルでセキュアな実行を実装する例示的なシステム及び方法である。本明細書で説明されるシステム及び方法の一部の実施形態は、ネットワークセキュリティのコンテキスト、特に電子商取引の設定における有用性を見いだす可能性がある。本明細書で説明される一部の実施形態は、セキュアなプロセッサ又は管理容易なエンジンとも呼ばれる、信頼できる実行エンジンにより、処理タスクの１つ又は複数の部分を、別個の処理デバイス上に配置され得るリモートプロセッサにオフロードすることを可能にする。例として、電子商取引アプリケーションのコンテキストでは、第１のコンピューティングデバイス内の信頼できる実行エンジンが、ビットマップ生成のようなグラフィクス中心の動作を、別個のコンピューティングデバイス上に配置されたリモートプロセッサにオフロードすることができる。リモートプロセッサは、ビットマップを、第１のデバイスの信頼できない実行複合体を実行しているアプリケーションに転送することができ、第１のデバイスは、このビットマップをディスプレイ上に提示し、ディスプレイから入力を収集することができる。ビットマップ生成をリモートプロセッサにオフロードすることは、第１のデバイスにおいてマルウェアが、ユーザ入力又はビットマップ領域からの出力を妨害又は監視するのを妨げる。

【００１０】

本明細書は、スケーラブルでセキュアな実行を実装することが可能なハードウェア及びソフトウェア環境並びにスケーラブルでセキュアな実行を実装する例示的な動作の説明を提供する。以下の説明では、様々な実施形態の完全な理解を提供するために多くの具体的な詳細を説明する。しかしながら、様々な実施形態は、これらの具体的な詳細を用いずに実施され得ることが、当業者には理解されよう。他の例では、周知の方法、手順、構成要素及び回路は、特定の実施形態を曖昧にしないために、詳細に図示されないが説明されないことがある。

【００１１】

図１は、一部の実施形態に従って、スケーラブルでセキュアな実行を実装するように適合される例示的な電子デバイス１１０の概略図である。図１に図示されるように、電子デバイス１１０は、モバイルフォン、タブレットコンピュータ、ポータブルコンピュータ又はパーソナルデジタルアシスタント（ＰＤＡ）のような、従来のモバイルデバイスとして具現化され得る。

【００１２】

一部の実施形態において、電子デバイスは、信頼できる実行複合体を含むことができる。この信頼できる実行複合体は、信頼できる実行エンジンとも呼ばれることがあり、また

セキュアな要素又は管理容易なエンジンと呼ばれることもある。信頼できる実行複合体は、信頼できない実行複合体とも呼ばれるプライマリ実行複合体とは別個の１つ又は複数のコントローラを備えることができる。この分離は、信頼できる実行複合体が、信頼できない実行複合体とは物理的に別個であるという意味において、物理的なものであってよい。あるいは、信頼できる実行複合体は、信頼できる実行複合体が、信頼できない実行複合体をホストしているものと同じチップ又はチップセットでホストされ得るが、信頼できる実行複合体がセキュアであるようにシリコンレベルでは分離されるという意味において、論理的なものであってもよい。

【００１３】

様々な実施形態において、電子デバイス１１０は、ディスプレイ、１つ又は複数のスピーカ、キーボード１つ又は複数の他のＩ／Ｏデバイス、マウス等を含む、１つ又は複数の付属の入力／出力デバイスを含むか、この入力／出力デバイスに結合され得る。例示的なＩ／Ｏデバイスには、タッチスクリーン、音声作動入力デバイス、トラックボール、地理位置情報デバイス、加速度計／ジャイロスコープ、バイオメトリック特徴入力デバイス及び電子デバイス１１０がユーザからの入力を受け取るのを可能にする任意の他のデバイスが含まれ得る。

【００１４】

電子デバイス１１０は、システムハードウェア１２０及びメモリ１４０を含む。メモリ１４０は、ランダムアクセスメモリ及び／又は読取専用メモリとして実装されてよい。ファイルストアがコンピューティングデバイス１１０に通信可能に結合されてもよい。ファイルストアは、例えばｅＭＭＣ、ＳＳＤ、１つ又は複数のハードドライブあるいは他のタイプのストレージデバイスのようなコンピューティングデバイス１１０に内蔵のものとすることができる。ファイルストアは、例えば１つ又は複数の外部ハードドライブ、ネットワーク接続ストレージあるいは別個のストレージネットワークのような、コンピュータ１１０に対して外付けのものであってもよい。

【００１５】

システムハードウェア１２０は、１つ又は複数のプロセッサ１２２、グラフィクスプロセッサ１２４、ネットワークインタフェース１２６並びにバス構造１２８を含むことができる。一実施形態において、プロセッサ１２２は、米国のカルフォルニア州サンタクララにある、本件出願人のインテル社から入手可能なＩｎｔｅｌ（登録商標）Ａｔｏｍ（登録商標）プロセッサ、Ｉｎｔｅｌ　Ａｔｏｍベースのシステムオンチップ（ＳＯＣ）又はＩｎｔｅｌ　Ｃｏｒｅ２　Ｄｕｏ（登録商標）プロセッサベースのプロセッサとしてもよい。本明細書で使用されるとき、「プロセッサ」という用語は、任意のタイプの計算要素を意味し、これらに限られないが、マイクロプロセッサ、マイクロコントローラ、複数命令セットコンピューティング（ＣＩＳＣ）マイクロプロセッサ、縮小命令セットコンピューティング（ＲＩＳＣ）マイクロプロセッサ、超長命令後（ＶＬＩＷ）マイクロプロセッサ又は任意の他のタイプのプロセッサ若しくは処理回路等である。

【００１６】

グラフィクスプロセッサ１２４は、グラフィック及び／又はビデオ動作を管理する補助プロセッサとして機能し得る。グラフィクスプロセッサ１２４は、電子デバイス１１０のマザーボード上に一体化されてもよく、あるいはマザーボード上の拡張スロットを介して結合されてもよい。

【００１７】

一実施形態において、ネットワークインタフェース１２６は、イーサーネット（登録商標）インタフェース（例えばＩＥＥＥ　８０２．３－２００２を参照されたい）のような有線インタフェースとすることができ、あるいはＩＥＥＥ　８０２．１１ａ，ｂ又はｇ準拠インタフェース（例えば２００３年の８０２．１１GのＩＥＥＥ規格に関するIEEE for IT-Telecommunications and information exchange between systems LAN/MAN--Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension

in the 2.4 GHz Band, 802.11G-2003等を参照されたい）のような無線インタフェースとすることもできる。無線インタフェースの別の例は、ＧＰＲＳ（general packet radio service）インタフェースである（例えば非特許文献１（「Guidelines on GPRS Handset Requirements, Global System for Mobile Communications/GSM Association」、 Ver. 3.0.1、２００２年１０月）を参照されたい）。

【００１８】

バス構造１２８は、システムハードウェア１２０の様々なコンポーネントを接続する。一実施形態において、バス構造１２８は、様々な利用可能なバスアーキテクチャのいずれかを使用する、メモリバス、周辺バス若しくは外部バス及び／又はローカルバスを含む、幾つかのタイプのバス構造のうちの１つ又は複数とすることができる。そのよう様々な利用可能なバスアーキテクチャには、これらに限られないが、１１ビットバス、業界標準アーキテクチャ（ＩＳＡ）、マイクロチャネルアーキテクチャ（ＭＳＡ）、拡張ＩＳＡ（ＥＩＳＡ）、ＩＤＥ（Intelligent Drive Electronics）、ＶＥＳＡローカルバス（ＶＬＢ）、ＰＣＩ、ＵＳＢ、ＡＧＰ（Advanced Graphics Port）、ＰＣＭＣＩＡ（Personal Computer Memory Card International Association bus）、ＳＣＳＩ（Small Computer Systems Interface）、ＨＳＩ（High Speed Synchronous Serial Interface）、ＳＬＩＭｂｕｓ（登録商標）（Serial Low-power Inter-chip Media Bus）等が含まれる。

【００１９】

電子デバイス１１０は、ＲＦ信号を送受信するＲＦトランシーバ１３０と、近距離通信（ＮＦＣ：Near Field Communication）無線機１３４と、ＲＦトランシーバ１３０によって受信した信号を処理する信号処理モジュール１３２を含んでもよい。ＲＦトランシーバは、例えばＢｌｕｅｔｏｏｔｈ（登録商標）又はＩＥＥＥ８０２．１１Ｘ、ＩＥＥＥ８０２．１１ａ，ｂ又はｇ準拠インタフェース（例えば２００３年の８０２．１１ＧのＩＥＥＥ規格に関するIEEE for IT-Telecommunications and information exchange between systems LAN/MAN--Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band, 802.11G-2003等を参照されたい）のようなプロトコルによるローカル無線接続を実装することができる。無線インタフェースの別の例は、ＷＣＤＭＡ（登録商標）、ＬＴＥ、ＧＰＲＳ（general packet radio service）インタフェース（例えば非特許文献１（「Guidelines on GPRS Handset Requirements, Global System for Mobile Communications/GSM Association」、 Ver. 3.0.1、２００２年１０月）を参照されたい）である。

【００２０】

電子デバイス１１０は更に、例えばキーパッド１３６及びディスプレイ１３８のような１つ又は複数の入力／出力インタフェースを含んでもよい。一部の実施形態において、電子デバイス１１０は、キーパットを有さずに、入力用にタッチパネルを使用してもよい。

【００２１】

メモリ１４０は、コンピューティングデバイス１１０の動作を管理するためのオペレーティングシステム１４２を含むことができる。一実施形態において、オペレーティングシステム１４２は、システムハードウェア１２０へのインタフェースを提供するハードウェアインタフェース１５４を含む。加えて、オペレーティングシステム１４２は、コンピューティングデバイス１１０の動作において使用されるファイルを管理するファイルシステム１５０と、コンピューティングデバイス１１０上で実行される処理を管理する処理制御サブシステム１５２を含むことができる。

【００２２】

オペレーティングシステム１４２は、リモートソースからのデータパケット及び／又はデータストリームを送受信するようにシステムハードウェア１２０と協働して動作し得る、１つ又は複数の通信インタフェースを含む（又は管理する）ことができる。オペレーティングシステム１４２は、該オペレーティングシステム１４２とメモリ１４０内に存在す

る１つ又は複数のアプリケーションモジュールとの間のインタフェースを提供する、システムコールインタフェースモジュール１４４を更に含んでよい。オペレーティングシステム１４２は、ＵＮＩＸ（登録商標）オペレーティングシステム又はそのいずれかの派生形（例えばＬｉｎｕｘ（登録商標）、Ａｎｄｒｏｉｄ（登録商標）等）として、あるいはＷｉｎｄｏｗｓ（登録商標）ブランドのオペレーティングシステム又は他のオペレーティングシステムとして具現化され得る。

【００２３】

電子デバイス１１０は、信頼できる実行エンジン１７０を備えることができる。一部の実施形態において、信頼できる実行エンジン１７０を、電子デバイス１１０のマザーボード上に配置される独立の集積回路として実装することができ、他の実施形態では、信頼できる実行エンジン１７０を、同じＳＯＣダイ（die）上の専用のプロセッサブロックとして実装してもよく、また他の実施形態では、信頼できる実行エンジン１７０を、プロセッサ１２２の一部分において実装してもよく、ここでプロセッサ１２２の該部分は、ＨＷ実施機構を使用するプロセッサの残りの部分とは別個である。

【００２４】

図１に示される実施形態において、信頼できる実行エンジン１７０は、プロセッサ１７２と、メモリモジュール１７４と、１つ又は複数の認証モジュール１７６と、Ｉ／Ｏモジュール１７８と、近距離通信（ＮＦＣ）モジュール１８０と、見た通りのものを反映する（ＷＹＳＩＷＹＳ：what you see is what you sign）モジュール１８２と、強化型プライバシ識別情報（ＥＰＩＤ：enhanced privacy identification）モジュール１８４と、１つ又は複数のアプリケーションプロキシ１８６とを備える。一部の実施形態において、メモリモジュール１７４は、持続型フラッシュメモリモジュールを備えることがあり、様々な機能モジュールが、例えばファームウェア又はソフトウェア等の持続型メモリモジュール内にエンコードされる論理命令として実装され得る。Ｉ／Ｏモジュール１７８は、シリアルＩ／Ｏモジュールを備えてもよく、パラレルＩ／Ｏモジュールを備えてもよい。信頼できる実行エンジン１７０は、メインプロセッサ１２２及びオペレーティングシステム１４２とは離れているので、信頼できる実行エンジン１７０をセキュアにすることが可能である、すなわち信頼できる実行エンジン１７０は、典型的にホストプロセッサ１２２からＳＷ攻撃を実装するハッカーに対してアクセス不可能にされ得る。

【００２５】

一部の実施形態において、信頼できる実行エンジンは、ホスト電子デバイス内において、信頼できる実行複合体を定義してよく、そのようなホスト電子デバイス内において、処理タスクの一部分を、異なる電子デバイス上のリモートプロセッサにオフロードすることを可能にするよう、スケーラブルでセキュアな実行プロシージャを実装してもよい。処理をリモートプロセッサへオフロードすることは、マルウェアの能力を妨げるか、あるいは信頼できない実行複合体上で動作しているソフトウェアを監視して、入力、出力及び動作からの処理結果を改ざん又は読み取るのを妨げる。

【００２６】

図２は、スケーラブルでセキュアな実行プロシージャを実装することができるネットワーク環境の高レベルな概略図である。図２を参照すると、電子デバイス１１０及びリモートデバイス１１２は、ネットワーク２４０を介して１つ又は複数のリモートサーバ２３０へ結合され得る。電子デバイス１１０は、適切な近距離通信リンクによりリモートデバイス１１２との無線通信を可能にする、近距離通信（ＮＦＣ）インタフェースを備えることができる。一部の実施形態において、電子デバイス１１０及びリモートデバイス１１２はそれぞれ、モバイル電話、タブレット、ＰＤＡ又は電子デバイス１１０に関連して上述したような他のモバイルコンピューティングデバイスとして具現化されてよい。ネットワーク２４０は、例えばインターネットのような公衆通信ネットワークとして実装されてもよく、プライベート通信ネットワークとして、あるいはその組み合わせとして実装されてもよい。

【００２７】

リモートサーバ２３０は、コンピュータシステムとして具現化され得る。一部の実施形態において、サーバ２３０は、電子商取引サーバとして具現化されて、ベンダ又はセキュアプラットフォームを操作する第三者によって管理されることがある。他のリモートサーバ２３０は、例えば取引清算（transaction clearing）サービス又はクレジットカードサービス等の第三者支払いシステムによって操作されることもある。

【００２８】

図３は、一部の実施形態に従ってスケーラブルでセキュアな実行を実装するシステムのより詳細な概略図である。図３を参照すると、電子デバイス１１０は、ネットワーク３４０を介して取引システム３５０に結合され得る。加えて、電子デバイス１１０は検証システム３６０にも結合され得る。検証システム３６０は、取引システム３５０と分離されてもよく、一体化されてもよい。同様に、一部の実施形態において、リモートデバイス１１２も、ネットワーク３４０を介して取引システム３５０及び検証システム３６０に結合され得る。

【００２９】

一部の実施形態において、ブラウザ又は他のアプリケーション３２０は、電子デバイス１１０の信頼できない実行複合体内において実行することができる。ブラウザ３２０は、認証プラグイン３２２を含むことがあり、該認証プラグイン３２２は、電子デバイス１１０の信頼できる実行複合体において実行する認証モジュール１７６と協働する。リモートデバイス１１２は、入力／出力モジュール３３６と、プロセッサ３３４と、メモリ３３０内に存在する認証モジュール３２２とを含む。

【００３０】

図３において取引システム３５０として識別される、取引を管理するリモートエンティティは、電子商取引のウェブサイト等として具現化され、通信ネットワーク３４０を介してホストデバイスに結合され得る。使用において、電子デバイス１１０の持ち主又はオペレータは、ブラウザ又は他のアプリケーションソフトウェアを使用して、ネットワーク経由で取引システム３５０にアクセスし、システム３５０上で電子商取引を開始することができる。

【００３１】

単独又は認証プラグイン３２２との組み合わせによる認証モジュール１７６と、入力／出力モジュール１７８と、セキュリティスプライトジェネレータ１７９と、リモートデバイス１１２上のプロセッサ３３４と、認証モジュール３３２は、プロセッサ１７２によって実装される処理タスクの一部がリモートデバイス１１２のリモートプロセッサ３３４にオフロードされる、スケーラブルでセキュアな実行動作を実装することができる。

【００３２】

スケーラブルでセキュアな実行を実装するシステムの様々な構造を説明したので、システムの動作的態様を、図４を参照して説明することにする。一部の実施形態において、図４のフローチャートに示される動作は、信頼できる実行エンジン１７０のプロセッサ１７２により、単独で、あるいは電子デバイスの信頼できない実行複合体において動作するプロセッサ１２２及びリモートデバイス１１２のプロセッサ３３４との組み合わせで実装され得る。

【００３３】

図４を参照すると、一部の実施形態において、図４に示される動作、動作４０５及び動作４１０において、セキュアコントローラとも呼ばれる信頼できる実行エンジンと、リモートプロセッサ、例えばリモートデバイス１１２上のプロセッサ３３４との間にセキュアなペアリングが確立される。一部の実施形態において、このペアリングは、ユーザが登録シーケンスを開始することによって、例えば電子デバイス１１０上でリモートデバイス１１２をタップすることにより、あるいは他の方法で登録プロセスを起動することにより開始され得る。登録要求に応答して、信頼できる実行エンジン１７０のプロセッサ１７２が、認証モジュール１７６を起動し、リモートデバイス１１２のプロセッサ３３４が認証モジュール３３２を起動する。それぞれの認証モジュール１７６、３３２は、例えばディフ

ィー・ヘルマン鍵共有プロトコル等のような適切な暗号化アルゴリズムを使用して共有の秘密を展開してもよい。

【００３４】

動作４１５及び動作４２０において、信頼できる実行エンジン１７０及びリモートプロセッサ３３４は、それぞれの入力／出力モジュール１７８、３３６により、セキュアな通信接続を確立する。通信接続は、無線接続を介して、あるいは例えば赤外線接続又は無線ネットワーク接続等の任意の他の適切な通信媒体を介して実装され得る。

【００３５】

動作４２５において、ブラウザ３２０又は他の適切なアプリケーションが、電子デバイス１１０のローカルプロセッサ１２２上で起動される。動作４３０及び動作４３５において、発見プロセスが電子デバイス１１０とリモートデバイス１１２との間で実装される。例として、一部の実施形態において、デバイス１１０、１１２は、Ｂｌｕｅｔｏｏｔｈ又は他の無線ネットワーク機能を備えることがあり、無線ネットワークを介して互いを発見することができる。

【００３６】

動作４４０において、ブラウザ上のアプリケーションがリモートサーバに接続する。例として、図３に示される実施形態では、ブラウザを使用して、電子商取引ウェブサイト等であり得る取引システム３５０に接続することができる。一部の実施形態において、電子デバイス１１０は、リモートサーバからログイン要求を受信し、これに応答して、信頼できない実行複合体において動作する認証プラグイン３２２が、信頼できる実行複合体内の認証モジュール１７６を起動する。

【００３７】

一部の実施形態において、信頼できる実行複合体は、ログイン画面用のビットマップ画像を生成し、これを電子デバイスのディスプレイ１３８上に提示する。例として、一部の実施形態において、ＷＹＳＩＷＹＳモジュール１８２は、電子デバイスのディスプレイ上にセキュアなウィンドウを開き、ウィンドウ上のダイアログボックス３８０内に認証要求を提示する。電子デバイス１１０のユーザは、ログイン要求を認証する入力を、セキュアなウィンドウ内に入力することによって認証要求に応答する。ＷＹＳＩＷＹＳモジュール１８２は、その入力に関連するピンを生成してもよい。

【００３８】

しかしながら、一部の実施形態において、信頼できる実行複合体は、ビットマップを生成する処理をリモートデバイス１１２にオフロードする。そのような実施形態において、プロセッサ１７２上で実行する認証モジュール１７６は、確認コードを生成して、該確認コード及び確認ページをリモートデバイス１１２上のプロセッサ３３４へ転送する。

【００３９】

動作４５０において、リモートデバイス１１２上のプロセッサ３３４は確認コードを受信し、動作４５５において、プロセッサ３３４はビットマップを構成し、共有の秘密を使用してビットマップを暗号化する。加えて、リモートデバイス１１２上のプロセッサ３３４は、ユーザ名とパスワードの組み合わせのようなユーザ入力要素用の座標を生成する。

【００４０】

ビットマップは電子デバイス１１０に渡される。一部の実施形態において、セキュアスプライトジェネレータ１７９が、ビットマップをディスプレイ１３８上にレンダリングすることができる。他の実施形態において、信頼できない実行複合体におけるグラフィクスプロセッサ１２４が、ビットマップをディスプレイ１３８上にレンダリングしてもよい。簡単に図３を参照すると、レンダリングされたビットマップは、ディスプレイ上にダイアログボックス３８０を提示することがある。ダイアログボックス３８０は、ユーザ名用の入力ウィンドウ３８２、パスワード用の入力ウィンドウ３８４及びユーザがダイアログボックス３８０に入力をするためのキーボード３８６のような入力機構を備えることができる。

【００４１】

ユーザは、ユーザ名／パスワードの組み合わせを、それぞれのウィンドウ３８２、３８４にキーボード３８６を使用して入力することができる。動作４７５において、入力がセキュアコントローラにおいて受信される。一部の実施形態において、信頼できる実行エンジンは、ダイアログボックス３８０への入力が、信頼できない実行複合体に対して見えないように、ビットマップ領域をシステムハードウェアからブロックする。一部の実施形態において、入力は、入力／出力インタフェース１７８によって直接検出され得る。他の実施形態において、入力は、入力によって検出されて、信頼できない実行複合体において動作している認証プラグイン３２２によってキャプチャされることがある。そのような実施形態では、入力座標がリモートデバイス１１２のプロセッサ３３４上で生成されたので、マルウェアによるスニッフィングは阻害されることに留意されたい。したがって、マルウェアは、入力座標又は座標に関連する入力を知らないことになる。

【００４２】

動作４８０において、ユーザ入力が検証される。例として、一部の実施形態では、認証モジュール１７６は、ＥＰＩＤモジュール１８４を起動する。ＥＰＩＤモジュール１８４は、識別パケットを生成してラップし、そのパケットがＮＦＣ通信リンクでセキュアに取得されたものであって、ＷＹＳピンがＷＹＳＩＷＹＳモジュール１８２を使用してセキュアに取得されたものであること証明する署名を適用する。電子デバイス１１０は、ラップされた識別パケットをリモートの検証サーバ３６０に転送し、該リモート検証サーバが、ユーザ入力を検証して、認証応答を電子デバイス１１０に返す。一部の実施形態において、検証応答は、信頼できる実行エンジン１７０内のＩ／Ｏインタフェース１７８を介して受信され、したがって電子デバイス１１０の信頼できない動作環境からはアクセス可能ではない。

【００４３】

動作４８５において、認証モジュール１７６は、リモート検証サーバ３６０からの応答をレビューする。動作４８５におけるリモート認証サーバ４６０からの応答が、ログインが認証されていないことを示す場合、制御は動作４９０に移り、ログインプロシージャが終了し、アクセスは拒否される。一方、動作４８５におけるリモート検証サーバ４６０からの応答が、ログインが認証されていることを示す場合、制御は動作４９５に移り、電子デバイス１１０と取引システム３５０との間のセキュアな通信セッションが開始され得る。

【００４４】

上述のように、一部の実施形態において、電子デバイス１１０はコンピュータシステムとして具現化されることがある。図５は、一部の実施形態に係るコンピュータシステム５００の概略図を示す。コンピュータシステム５００は、コンピューティングデバイス５０２と、（例えばコンピューティングデバイス５０２に電力を供給する）電源アダプタ５０４とを含む。コンピューティングデバイス５０２は、ラップトップ（又はノートブック）コンピュータ、パーソナルデジタルアシスタント、デスクトップコンピューティングデバイス（例えばワークステーション又はデスクトップコンピュータ）、ラック装着型のコンピューティングデバイス等のような任意の適切なコンピューティングデバイスとすることができる。

【００４５】

電力は、以下のソースのうちの１つ又は複数から（例えばコンピューティングデバイスの電源５０６を通して）コンピューティングデバイス５０２の様々なコンポーネントへ供給され得る。そのようなソースは、１つ又は複数のバッテリパック、ＡＣアウトレット（例えば電源アダプタ５０４のような変換及び／又はアダプタを通して）、自動車用の電源、飛行機用の電源等である。一部の実施形態において、電源アダプタ５０４は、電力供給ソースの出力（例えば約１１０ＶＡＣから２４０ＶＡＣまでのＡＣアウトレット電圧）を、約５ＶＤＣから１２．６ＶＤＣまでの間に及ぶ直流（ＤＣ）電圧に変換することができる。

【００４６】

コンピューティングデバイス５０２は、１つ又は複数の中央処理ユニット（ＣＰＵ）５０８も含み得る。一部の実施形態において、ＣＰＵ５０８は、本件出願人であるカルフォルニア州サンタクララにあるインテル社から入手可能な、Ｐｅｎｔｉｕｍ（登録商標）ＩＩプロセッサファミリ、Ｐｅｎｔｉｕｍ ＩＩＩ、Ｐｅｎｔｉｕｍ ＩＶを含むＰｅｎｔｉｕｍファミリのプロセッサ又はＣＯＲＥ２ Ｄｕｏプロセッサのうちの１つ又は複数のプロセッサとすることができる。あるいは、インテルのＩｔａｎｉｕｍ（登録商標）ＸＥＯＮ、Ｃｅｌｅｒｏｎ（登録商標）のような他のＣＰＵを使用してもよい。あるいは、他の製造業者による１つ又は複数のプロセッサを用いてもよい。さらに、プロセッサは、単一コア設計であってもマルチコア設計であってもよい。

【００４７】

チップセット５１２を、ＣＰＵ５０８に結合するか一体化してもよい。チップセット５１２は、メモリコントロールハブ（ＭＣＨ）５１４を含むことがある。ＭＣＨ５１４は、メインシステムメモリ５１８に結合されるメモリコントローラ５１６を含むことがある。メインシステムメモリ５１８は、データ及びＣＰＵ５０８若しくはシステム５００内に含まれる任意の他のデバイスによって実行される命令シーケンスを格納する。一部の実施形態において、メインメモリ５１８は、ランダムアクセス（ＲＡＭ）を含むが、メインメモリは、動的ＲＡＭ（ＤＲＡＭ）、同期ＤＲＡＭ（ＳＤＲＡＭ）等のような他のメモリタイプを使用して実装されることもある。複数のＣＰＵ及び／又は複数のシステムメモリのような追加のデバイスをバス５１０に結合してもよい。

【００４８】

ＭＣＨ５１４は、グラフィック・アクセラレータ５２２に結合されるグラフィクスインタフェース５２０も含むことがある。一部の実施形態において、グラフィクスインタフェース５２０は、アクセラレイテッド・グラフィクス・ポート（ＡＧＰ）を介してグラフィクス・アクセラレータ５２２に結合される。一部の実施形態において、（フラットパネルディスプレイのような）ディスプレイ５４０は、例えばビデオメモリやシステムメモリのようなストレージデバイスに格納された画像のデジタル表現を、ディスプレイによって解釈されて表示されるディスプレイ信号に変換する信号変換器を介して、グラフィクスインタフェース５２０に結合されてもよい。ディスプレイデバイスによって生成されるディスプレイ５４０の信号は、様々な制御デバイス中を通った後に、ディスプレイによって解釈され、その後表示され得る。

【００４９】

ハブインタフェース５２４は、ＭＣＨ５１４をプラットフォームコントロールハブ（ＰＣＨ）５２６へ結合する。ＰＣＨ５２６は、コンピューティングシステム５００に結合された入力／出力（Ｉ／Ｏ）デバイスへのインタフェースを提供する。ＰＣＨ５２６は、ＰＣＩバスに結合され得る。したがって、ＰＣＨ５２６は、ＰＣＩバス５３０へのインタフェースを提供するＰＣＩブリッジ５２８を含む。ＰＣＩブリッジ５２８は、ＣＰＵ５０８と周辺デバイスとの間のデータ経路を提供する。加えて、カルフォルニア州サンタクララにあるインテル社から入手可能なＰＣＩエクスプレスアーキテクチャのような、他のタイプのＩ／Ｏ相互接続技術を使用してもよい。

【００５０】

ＰＣＩバス５３０は、オーディオデバイス５３２並びに１つ又は複数のディスクドライブ５３４に結合され得る。加えて、ＣＰＵ５０８とＭＣＨ５１４を組み合わせて単一のチップを形成してもよい。さらに、他の実施形態において、グラフィクス・アクセラレータ５２２はＭＣＨ５１４に含まれてもよい。

【００５１】

加えて、ＰＣＨ５２６に結合される他の周辺装置は、様々な実施形態において、ＩＤＥ（integrated drive electronic）又はＳＣＳＩ（small computer system interface）ハードドライブ、ＵＳＢポート、キーボード、マウス、パラレルポート、シリアルポート、フロッピー（登録商標）ディスクドライブ、デジタル出力サポート（例えばデジタルビデオインタフェース（ＤＶＩ）等を含むことがある。したがって、コンピューティン

グデバイス５０２は、揮発性及び／又は非揮発性メモリを含むことができる。

【００５２】

以上のように、本明細書では、電子デバイスにおいてスケーラブルでセキュアな実行を実装するアーキテクチャ及び関連する方法が説明されている。一部の実施形態では、このアーキテクチャは、リモート電子デバイスプラットフォームにおいて具現化されるハードウェアの能力を使用して、別個のデバイスにおけるセキュアなコントローラのための計算コストが高い処理タスクを実行する。実行複合体が、信頼できる実行エンジンにおいて実装されるので、動作は電子デバイス上のマルウェアからアクセス可能ではない。一部の実施形態では、信頼できる実行エンジンは、リモート又は取り付け可能なデバイス、例えばドングルにおいて実装されてもよい。

【００５３】

本明細書で記載されるとき、「論理命令」という用語は、１つ又は複数の論理動作を実行するために１つ又は複数のマシンによって理解され得る表現に関連する。例えば論理命令は、１つ又は複数のデータオブジェクトに対して１つ又は複数の動作を実行するため、プロセッサコンパイラによって解釈可能な命令を備えることがある。しかしながら、これはマシン読取可能命令の例示に過ぎず、実施形態はこの点に限定されない。

【００５４】

本明細書で記載されるとき、「コンピュータ読取可能媒体」という用語は、１つ又は複数のマシンによって知覚可能な表現を保持することができる媒体に関連する。例えばコンピュータ読取可能媒体は、コンピュータ読取可能命令又はデータを格納するための１つ又は複数のストレージデバイスを備えてもよい。ストレージデバイスは、例えば光、磁気又は半導体記憶媒体のような記憶媒体としてもよい。しかしながら、これはコンピュータ読取可能媒体の例示にすぎず、実施形態はこの点に限定されない。

【００５５】

本明細書で記載されるとき、「ロジック」という用語は、１つ又は複数の論理的動作を実行するための構造に関連する。例えばロジックは、１つ又は複数の入力信号に基づいて１つ又は複数の出力信号を提供する回路を備えることがある。そのような回路は、デジタル入力を受信してデジタル出力を提供する有限の状態マシン、あるいは１つ又は複数のアナログ入力信号に応答して１つ又は複数のアナログ出力信号を提供する回路であってもよい。そのような回路は、特定用途向け集積回路（ＡＳＩＣ）又はフィールドプログラマブルゲートアレイ（ＦＰＧＡ）において提供されることがある。またロジックは、マシン実行可能命令を実行する処理回路との組み合わせによるメモリ内に格納される、マシン読取可能命令を備えてもよい。しかしながら、これらは、ロジックを提供し得る構造の例示にすぎず、実施形態はこの点に限定されない。

【００５６】

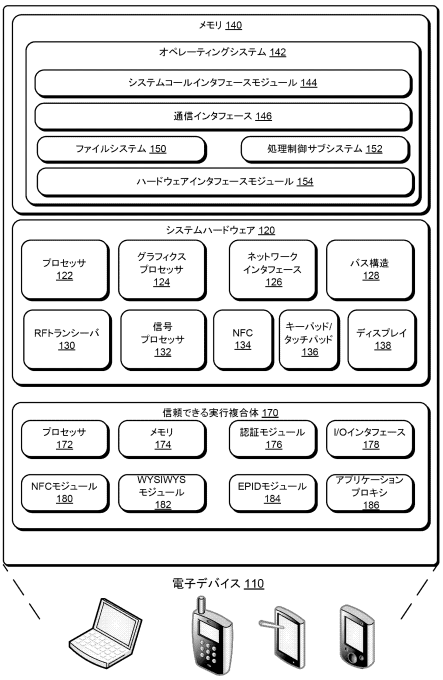
本明細書で説明される方法の一部は、コンピュータ読取可能媒体において論理命令として具現化されてもよい。プロセッサにおいて実行されると、論理命令により、プロセッサは、説明される方法を実装する専用のマシンとしてプログラムされることになる。プログラムは論理命令によって本明細書で説明される方法を実行するように構成されると、説明される方法を実行するための構造を構成する。あるいは、本明細書で説明される方法は、例えばフィールドプログラマブルゲートアレイ（ＦＰＧＡ）、特定用途向け集積回路（ＡＳＩＣ）等におけるロジックに要約されてもよい。

【００５７】

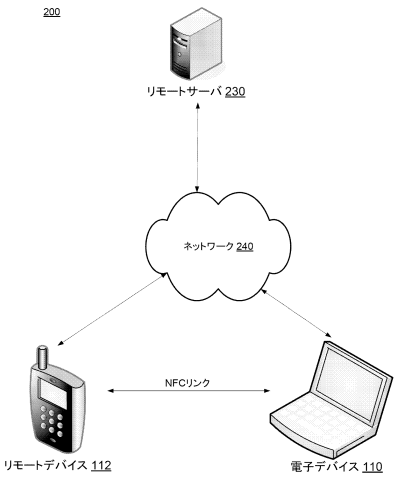
詳細な説明及び特許請求の範囲において、結合及び接続という用語並びにその派生語が使用されていることがある。特定の実施形態において、接続されるという用語は、２つ又はそれ以上の要素が、直接物理的に又は電気的に互いに接触することを示すのに使用されることがある。結合されるという用語は、２つ又はそれ以上の要素が直接物理的に又は電気的に接触することを意味することがある。しかしながら、結合されるという用語は、２つ又はそれ以上の要素が互いに直接接触していないが、依然として互いに協働するか対話し得る状態を意味することもある。

【００５８】
本明細書において、「一実施形態」又は「一部の実施形態」への言及は、実施形態に関連して説明される特定の特徴、構造又は特性が、少なくとも１つの実装において含まれることを意味する。本明細書の様々な箇所における「一実施形態において（一実施形態では）」というフレーズの使用は、同じ実施形態を示していることもあり、必ずしも全て同じ実施形態を示していないこともある。
【００５９】
実施形態を、構造的特徴及び／又は方法的動作に特有の言語で説明してきたが、特許請求に係る主題は、説明される具体的な特徴又は動作に限定されないことは理解されよう。むしろ、具体的な特徴及び動作は、特許請求に係る主題を実装する例示的形式として開示される。

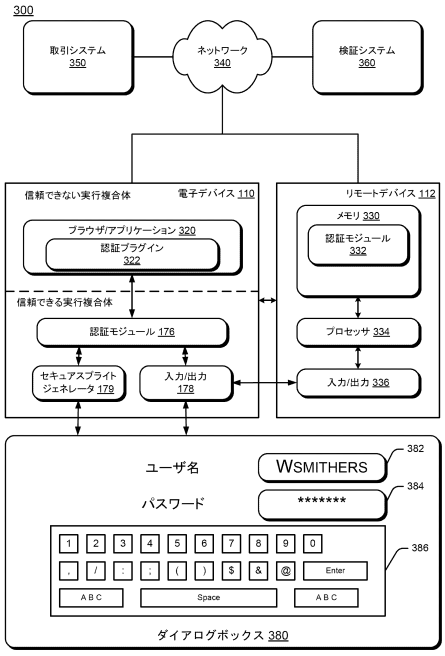
【図１】



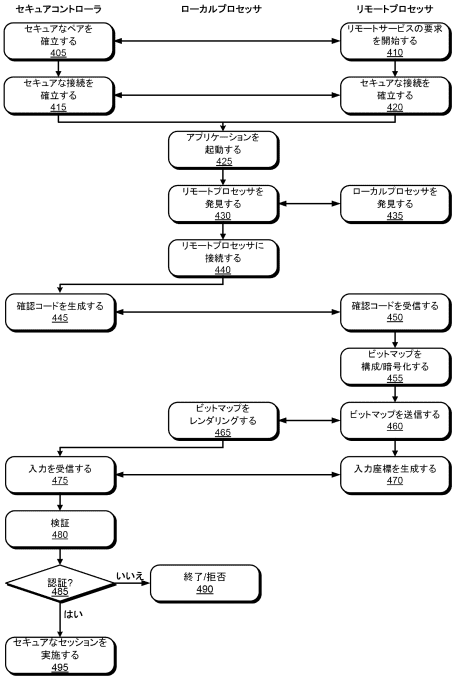
【図２】



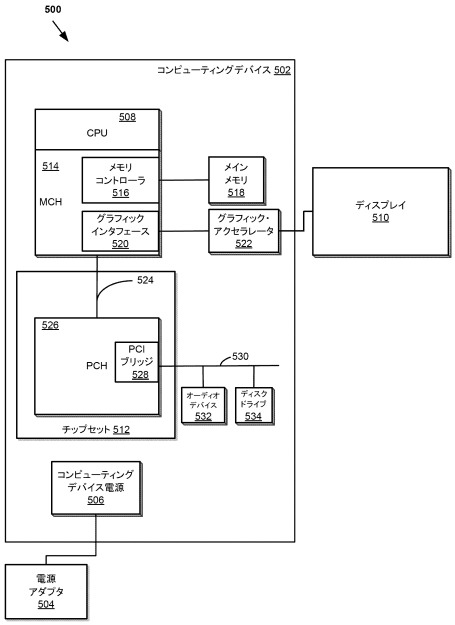
【図３】


300
取引システム
350
ネットワーク
340
検証システム
360
信頼できない実行複合体
電子デバイス 110
ブラウザ/アプリケーション 320
認証プラグイン
322
信頼できる実行複合体
認証モジュール 176
セキュアスプライト
ジェネレータ 179
入力/出力
178
リモートデバイス 112
メモリ 330
認証モジュール
332
プロセッサ 334
入力/出力 336
ユーザ名
WSMITHERS
382
パスワード
****
384
1 2 3 4 5 6 7 8 9 0
. / : ; ( ) $ & @ Enter
A B C
Space
A B C
386
ダイアログボックス 380

【図４】


セキュアコントローラ
ローカルプロセッサ
リモートプロセッサ
セキュアなペアを
確立する
405
リモートサービスの要求
を開始する
410
セキュアな接続を
確立する
415
セキュアな接続を
確立する
420
アプリケーションを
起動する
425
リモートプロセッサを
発見する
430
ローカルプロセッサを
発見する
435
リモートプロセッサに
接続する
440
確認コードを生成する
445
確認コードを受信する
450
ビットマップを
構成/暗号化する
455
ビットマップを
レンダリングする
465
ビットマップを送信する
460
入力を受信する
475
入力座標を生成する
470
検証
480
認証?
485
いいえ
終了/拒否
490
はい
セキュアなセッションを
実施する
495

【図５】


500
コンピューティングデバイス 502
508
CPU
514
MCH
メモリ
コントローラ
516
メイン
メモリ
518
グラフィック
インタフェース
520
グラフィック・
アクセラレータ
522
ディスプレイ
510
524
526
PCH
PCI
ブリッジ
528
530
オーディオ
デバイス
532
ディスク
ドライブ
534
チップセット 512
コンピューティング
デバイス電源
506
電源
アダプタ
504

フロントページの続き

(72)発明者　バクシ，サンジェイ
アメリカ合衆国　９７２３１　オレゴン州　ポートランド　ノースウエスト　レッド　シダー　コート　１５２２２

審査官　大塚　俊範

(56)参考文献　特開２０１１－２５３５２５（ＪＰ，Ａ）
特開２０１０－０９２４８５（ＪＰ，Ａ）
特表２０１２－５０３２２９（ＪＰ，Ａ）
特開２０１０－１７６４５２（ＪＰ，Ａ）
国際公開第２０１１／０６６１５２（WO，Ａ１）
特表２００６－５０２４５７（ＪＰ，Ａ）
特表２０１１－５１１３５５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　　９／５０