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

特許第5877400号
(P5877400)

(45)発行日　平成28年3月8日(2016.3.8)　(24)登録日　平成28年2月5日(2016.2.5)

(51)Int.Cl.		F I	
G06F 21/44	(2013.01)	G06F	21/44
G06F 21/74	(2013.01)	G06F	21/74
G06Q 20/00	(2012.01)	G06Q	20/00
G06Q 20/40	(2012.01)	G06Q	20/40

請求項の数 29　(全 18 頁)

(21)出願番号	特願2014-509337(P2014-509337)
(86)(22)出願日	平成24年4月30日(2012.4.30)
(65)公表番号	特表2014-519639(P2014-519639A)
(43)公表日	平成26年8月14日(2014.8.14)
(86)国際出願番号	PCT/US2012/035789
(87)国際公開番号	WO2012/151152
(87)国際公開日	平成24年11月8日(2012.11.8)
審査請求日	平成26年10月16日(2014.10.16)
(31)優先権主張番号	61/482,927
(32)優先日	平成23年5月5日(2011.5.5)
(33)優先権主張国	米国(US)
(31)優先権主張番号	13/441,363
(32)優先日	平成24年4月6日(2012.4.6)
(33)優先権主張国	米国(US)

(73)特許権者　506291542
ペイパル　インコーポレイテッド
アメリカ合衆国　カリフォルニア州　９５１３１　サンノゼ　ノース　ファースト　ストリート　２２１１
(74)代理人　100074099
弁理士　大菅　義之
(74)代理人　110000132
大菅内外国特許事務所特許業務法人
(72)発明者　タボー，セバスチアン　ルードヴィク，ジャン
アメリカ合衆国，カリフォルニア州　９４０６１，レッドウッド　シティ，オークリッジ　ドライブ　６０２

最終頁に続く

(54)【発明の名称】取引セキュリティー強化のためのシステムおよび方法

(57)【特許請求の範囲】

【請求項１】

コンピュータ・プログラミング命令を記憶するように構成されたコンピュータ・メモリ記憶コポーネントと、

前記コンピュータ・メモリ記憶コポーネントに動作可能に結合されたコンピュータ・プロセッサ・コポーネントと

を備えるシステムであって、

前記コンピュータ・プロセッサ・コポーネントが、互いから孤立したセキュア・オペレーティング・システムおよび非セキュア・オペレーティング・システムを並行して運用するように構成され、

前記コンピュータ・プロセッサ・コポーネントが、

前記非セキュア・オペレーティング・システムにより運営されるアプリケーションから、前記アプリケーションの証明を含んだ認証要求を受け取るオペレーションと、

前記セキュア・オペレーティング・システムに運営されるセキュア・アプレットとの通信を行うオペレーションであって、前記通信を行うことが、前記アプリケーションの前記証明を前記セキュア・アプレットに転送することを含むオペレーションと、

前記アプリケーションの前記証明に基づいて、前記アプリケーションを認証および審査するオペレーションと

を行うためのコードを実行するように構成される、

システム。

【請求項２】
前記システムが、モバイル電子デバイス上に実装された電子チップを含む、
請求項１に記載のシステム。
【請求項３】
前記アプリケーションが、第三者である開発者からのソフトウェア・プログラムであり、
前記セキュア・アプレットが、支払いプロバイダからのソフトウェア・プログラムの一部分である、
請求項１に記載のシステム。
【請求項４】
前記アプリケーションおよび前記セキュア・アプレットがともに、支払いプロバイダからのソフトウェア・プログラムの一部分である、
請求項１に記載のシステム。
【請求項５】
前記セキュア・オペレーティング・システムと前記非セキュア・オペレーティング・システムとの間のゲートウェイとして構成されたモニタを少なくとも部分的にバイパスすることによって、少なくとも部分的には前記通信が行われる、
請求項１に記載のシステム。
【請求項６】
前記アプリケーションの開発者に認証証書を割り当てることを更に含み、
前記認証証書が、前記認証要求を前記受け取ることの前に割り当てられ、
前記アプリケーションの前記証明が、前記認証証書を含む、
請求項１に記載のシステム。
【請求項７】
前記認証および審査することが、リモート・サーバにアクセスすることなく行われる、
請求項１に記載のシステム。
【請求項８】
コンピュータ・プログラムを記憶した非一時的有形機械可読記憶媒体を備える装置であって、
前記コンピュータ・プログラムが、機械可読命令を含み、
前記機械可読命令が、プロセッサにより電子的に実行されると、
電子チップの非セキュア部分に存在するアプリケーションから、前記アプリケーションの証明を含んだ認証要求を受け取ることと、
前記電子チップのセキュア部分に存在するセキュア・アプレットとの通信を行うことであって、前記セキュア部分が、前記非セキュア部分から分離しており、前記通信を行うことが、前記アプリケーションの前記証明を前記セキュア・アプレットに転送することを含むことと、
前記アプリケーションの前記証明に基づいて、前記アプリケーションを認証および審査することと
を行う装置。
【請求項９】
前記電子チップが、モバイル電子デバイス上のコンピュータ・メモリまたはコンピュータ・プロセッサを含む、
請求項８に記載の装置。
【請求項１０】
前記アプリケーションが、第三者である開発者からのソフトウェア・プログラムであり、
前記セキュア・アプレットが、支払いプロバイダからのソフトウェア・プログラムの一部分である、
請求項８に記載の装置。

【請求項１１】
前記アプリケーションおよび前記セキュア・アプレットがともに、支払いプロバイダからのソフトウェア・プログラムの一部分である、
請求項８に記載の装置。
【請求項１２】
前記通信を行うことのための前記命令が、前記電子チップの前記セキュア部分と前記電子チップの前記非セキュア部分との間のゲートウェイとして構成されたモニタを少なくとも部分的にバイパスすることのための命令を含む、
請求項８に記載の装置。
【請求項１３】
前記コンピュータ・プログラムが、前記アプリケーションの開発者に認証証書を割り当てるための命令を更に含み、
前記認証証書が、前記認証要求を前記受け取ることの前に割り当てられ、
前記アプリケーションの前記証明が、前記認証証書を含む、
請求項８に記載の装置。
【請求項１４】
前記認証および審査を行うための前記命令が、リモート・サーバにアクセスすることなく、前記アプリケーションを認証および審査するための命令を含む、
請求項８に記載の装置。
【請求項１５】
電子チップの非セキュア部分に存在するアプリケーションから、前記アプリケーションの証明を含んだ認証要求を受け取ることと、
前記電子チップのセキュア部分に存在するセキュア・アプレットとの通信を行うことであって、前記セキュア部分が、前記非セキュア部分から分離しており、前記通信を行うことが、前記アプリケーションの前記証明を前記セキュア・アプレットに転送することを含むことと、
前記アプリケーションの前記証明に基づいて、前記アプリケーションを認証および審査することと
を含む方法。
【請求項１６】
前記電子チップが、モバイル電子デバイス上のコンピュータ・メモリを含む、
請求項１５に記載の方法。
【請求項１７】
前記電子チップが、モバイル電子デバイス上のコンピュータ・プロセッサを含む、
請求項１５に記載の方法。
【請求項１８】
前記アプリケーションが、第三者である開発者からのソフトウェア・プログラムであり、
前記セキュア・アプレットが、支払いプロバイダからのソフトウェア・プログラムの一部分である、
請求項１５に記載の方法。
【請求項１９】
前記アプリケーションおよび前記セキュア・アプレットがともに、支払いプロバイダからのソフトウェア・プログラムの一部分である、
請求項１５に記載の方法。
【請求項２０】
前記電子チップの前記セキュア部分と前記電子チップの前記非セキュア部分との間のゲートウェイとして構成されたモニタを部分的にバイパスすることによって、少なくとも部分的には前記通信を行なうことが行われる、
請求項１５に記載の方法。

【請求項２１】
前記アプリケーションの開発者に認証証書を割り当てることを更に含み、
前記認証証書が、前記認証要求を前記受け取ることの前に割り当てられ、
前記アプリケーションの前記証明が、前記認証証書を含む、
請求項１５に記載の方法。
【請求項２２】
前記認証および審査することが、リモート・サーバにアクセスすることなく行われる、
請求項１５に記載の方法。
【請求項２３】
コンピュータ・プログラミング・コードを記憶するコンピュータ記憶手段と、
前記コンピュータ記憶手段に動作可能に結合されたコンピュータ処理手段と
を備えるシステムであって、
前記コンピュータ処理手段が、互いから孤立したセキュア・オペレーティング・システムおよび非セキュア・オペレーティング・システムを並行して運用し、
前記コンピュータ処理手段が、
前記非セキュア・オペレーティング・システムにより運営されるアプリケーションから、前記アプリケーションの証明を含んだ認証要求を受け取る手段と、
前記セキュア・オペレーティング・システムに運営されるセキュア・アプレットとの通信を行う手段であって、前記通信が、前記アプリケーションの前記証明を前記セキュア・アプレットに転送することを含む手段と、
前記アプリケーションの前記証明に基づいて、前記アプリケーションを認証および審査する手段と
を備えるシステム。
【請求項２４】
前記システムが、モバイル・テレコミュニケーション手段上に実装された集積回路手段を備える、
請求項２３に記載のシステム。
【請求項２５】
前記アプリケーションが、第三者である開発者からのソフトウェア・プログラムであり、
前記セキュア・アプレットが、支払いプロバイダからのソフトウェア・プログラムの一部分である、
請求項２３に記載のシステム。
【請求項２６】
前記アプリケーションおよび前記セキュア・アプレットがともに、支払いプロバイダからのソフトウェア・プログラムの一部分である、
請求項２３に記載のシステム。
【請求項２７】
前記通信を行う手段が、前記セキュア・オペレーティング・システムと前記非セキュア・オペレーティング・システムとの間のゲートウェイとして構成されたモニタを少なくとも部分的にバイパスする手段を備える、
請求項２３に記載のシステム。
【請求項２８】
前記コンピュータ処理手段が、前記アプリケーションの開発者に認証証書を割り当てる手段を更に備え、
前記認証証書が、前記認証要求を前記受け取ることの前に割り当てられ、
前記アプリケーションの前記証明が、前記認証証書を含む、
請求項２３に記載のシステム。
【請求項２９】
前記認証および審査を行う手段が、リモート・サーバにアクセスすることなく、認証お

よび審査を行う手段を備える、
請求項２３に記載のシステム。

【発明の詳細な説明】
【技術分野】
【０００１】
本開示内容は、一般には、オンラインでの支払い管理に関し、より詳細には、支払いセキュリティーに関する。
【背景技術】
【０００２】
物理的な実世界対応物を有することも、有さないこともある、増加の一途をたどるオンライン事業主体により、オンライン取引が、ますます一般的になっている。さらに、これらのオンライン事業主体に提供されるサービスも改善されている。オンライン取引の普及は、一つには、物理的位置での取引ではなく、取引をオンライン化することの容易さおよび便利さに起因する。しかし、支払いのセキュリティーが、オンライン支払いシステムおよび方法での大きな懸念の１つである。必要とされるのは、処理のセキュリティーについてのユーザの懸念に十分に対処することの可能なセキュア支払いプラットフォームおよび技術である。
【発明の概要】
【０００３】
本開示内容のより広い形態のうちの１つの形態は、システムを含む。このシステムは、コンピュータ・プログラミング命令を記憶するように構成されたコンピュータ・メモリ記憶コポーネントと、コンピュータ・メモリ記憶コポーネントに動作可能に結合されたコンピュータ・プロセッサ・コポーネントとを含み、コンピュータ・プロセッサ・コポーネントは、互いから孤立したセキュア・オペレーティング・システムおよび非セキュア・オペレーティング・システムを並行して運用するように構成され、コンピュータ・プロセッサ・コポーネントは、非セキュア・オペレーティング・システムにより運営されるアプリケーションから、アプリケーションの証明を含んだ認証要求を受け取るオペレーションと、セキュア・オペレーティング・システムに運営されるセキュア・アプレットとの通信を行うオペレーションであって、この通信を行うことが、アプリケーションの証明をセキュア・アプレットに転送することを含むオペレーションと、アプリケーションの証明に基づいて、アプリケーションを認証および審査するオペレーションとを、行うためのコードを実行するように構成される。
【０００４】
本開示内容のより広い形態のうちの他の形態は、コンピュータ・プログラムを記憶した非一時的有形機械可読記憶媒体を備える装置を含み、このコンピュータ・プログラムは、プロセッサにより電子的に実行されると以下のことを行う機械可読命令を含むが、それらは、電子チップの非セキュア部分に存在するアプリケーションから、アプリケーションの証明を含んだ認証要求を受け取ることと、電子チップのセキュア部分に存在するセキュア・アプレットとの通信を行うことであって、セキュア部分が、非セキュア部分から分離しており、この通信が、アプリケーションの証明をセキュア・アプレットに転送することを含むことと、アプリケーションの証明に基づいて、アプリケーションを認証および審査すること、を実行する。
【０００５】
本開示内容のより広い形態のうちの他の形態は、認証および審査を行う方法を含む。この方法は、電子チップの非セキュア部分に存在するアプリケーションから、アプリケーションの証明を含んだ認証要求を受け取ることと、電子チップのセキュア部分に存在するセキュア・アプレットとの通信を行うことであって、セキュア部分が、非セキュア部分から分離しており、この通信が、アプリケーションの証明をセキュア・アプレットに転送することを含むことと、アプリケーションの証明に基づいて、アプリケーションを認証および

審査することとを含む。
【図面の簡単な説明】
【０００６】
【図１】本開示内容の様々な態様による電子チップの略ブロック図である。
【図２】本開示内容の様々な態様による、認証および審査を行うための高レベル・アーキテクチャの図である。
【図３】本開示内容の様々な態様による、認証および審査を行う方法の図である。
【図４】本開示内容の様々な態様による、図３の方法の様々なステップを実装するためのコンピュータの図である。
【発明を実施するための形態】
【０００７】
以下の開示内容では、本開示内容の様々な特徴を実装するための互いに異なる多くの実施形態または例が提供されることを理解されたい。本開示内容を簡略化するために、構成部品および構成の具体的な例を以下で説明する。これらは当然単なる例であり、限定を行うことを意図しない。簡略化および明確化のために、様々な特徴を異なるスケールで任意に描くこともある。
【０００８】
モバイル・コンピューティング技術およびモバイル通信技術が発展し続けるにつれて、モバイル・デバイスを伴う取引が、ますます一般的になっている。モバイル・デバイスを通して取引を行うことの普及は、一つには、有形の資金証書（例、現金または小切手）を伴う物理的位置での従来式取引の代わりとなる、モバイル・デバイスを通した取引（例、オンライン購入）の容易さおよび便利さに起因する。しかし、モバイル取引が普及するにつれ、こうした取引を標的とした攻撃も増大している。これらの攻撃は、ユーザの個人情報または金融情報を盗もうと企てることを含むことも、悪徳業者が正当な販売業者のふりをしようとすることを含むこともある。
【０００９】
本明細書では、上で議論した攻撃が実質的に阻止されるように、または減少するように、モバイル取引のセキュリティーを高める方法およびシステムを開示する。
【００１０】
図１を参照すると、電子チップ１００の略ブロック図が示されている。電子チップ１００は、携帯電話ハンドセット、コンピュータ・タブレット、ラップトップなどのモバイル・デバイスに実装することができる。いくつかの実施形態では、電子チップ１００は、たとえばＡｄｖａｎｃｅｄ　ＲＩＳＣ　Ｍａｃｈｉｎｅ（ＡＲＭ（登録商標））プロセッサなどのコンピュータ・プロセッサを含む。このコンピュータ・プロセス・ユニットは、コンピュータ命令を記憶することの可能なメモリ・ストレージを含むことがある。他の実施形態では、電子チップ１００は、たとえば、リード・オンリー・メモリ（ＲＯＭ）、ＦＬＡＳＨ、ランダム・アクセス・メモリ（ＲＡＭ）、ハードディスク、光ディスク、磁気ディスク、または他の適当な種類の揮発性メモリ・デバイスおよび不揮発性メモリ・デバイスなどのコンピュータ・メモリ記憶デバイスを含む。
【００１１】
電子チップ１００は、ＴｒｕｓｔＺｏｎｅ（登録商標）対応チップである。ＴｒｕｓｔＺｏｎｅ（登録商標）は、ＡＲＭ　Ｈｏｌｄｉｎｇｓ（登録商標）社によって開発された技術であり、アプリケーションを安全に実行することのできる信頼された環境を支援するプラットフォームを提供する。より詳細には、電子チップ１００は、「通常世界」１１０Ａおよび「セキュア世界」１１０Ｂを含み、これらは、セキュア情報がセキュア世界１１０Ｂから通常世界１１０Ａに漏れることを阻止するために互いから分離している。これらの２つの世界１１０Ａおよび１１０Ｂは、同一の電子チップ１００上で互いに並行に動作する。セキュア世界１１０Ｂは、ハンドセットのメイン・オペレーティング・システムの立上げ時間前に、プレロードされ、妥当性が確認される。いくつかの実施形態では、通常世界１１０Ａが、ハンドセットのメイン・オペレーティング・システムを運用し、セキュ

ア世界１１０Ｂが、異なる（よりセキュアな）オペレーティング・システムを運用する。こうして、通常世界１１０Ａに存在するコンポーネントまたはアプリケーションの整合性を検証するために、セキュア世界１１０Ｂを使用することができる。いくつかの実施形態では、１組の制御パラメータを最新の既知のコンフィギュレーションまたは権限付与コンフィギュレーションに適用することにより、こうした整合性検証を実現することができる。

【００１２】

通常世界１１０Ａおよびセキュア世界１１０Ｂは、それぞれ、１つまたは複数のソフトウェア・アプリケーションを含むことがある。いくつかの実施形態では、セキュア世界１１０Ｂに存在するソフトウェア・アプリケーションを、アプレットと称することもある。たとえば、アプリケーション１２０が通常世界に存在し、１つまたは複数のセキュア・アプレット１３０がセキュア世界に存在する。いくつかの実施形態では、アプリケーション１２０は、カリフォルニア州、サンノゼのＰＡＹＰＡＬ，ＩＮＣ（登録商標）などの支払いプロバイダ事業主体、または、ユーザの口座に送金を行うことおよびユーザの口座から送金を行うことの可能な他の適当な金融機関によって開発されたコンピュータ・ソフトウェア・プログラムの一部分を含む。このアプリケーションは、インターネットを通して、たとえばＧＯＯＧＬＥ　ＰＬＡＹ（登録商標）またはＡＰＰＬＥ　ＡＰＰ　ＳＴＯＲＥ（登録商標）などを通して提供され、ユーザによりダウンロードされてもよい。アプリケーション１２０は、低レベルのセキュリティーを必要とする標準的タスクを行う助けとなる機能およびインタフェースを含むこともある。たとえば、アプリケーション１２０は、支払いプロバイダ事業主体のユーザが自身の口座を用いて、自身の購入履歴を検索することなど、標準的な管理タスクを行うことを可能にするプログラミング命令を含むこともある。他のいくつかの実施形態では、アプリケーション１２０は、有形商品またはデジタル商品の販売を提供する商業者など、第三者である開発者によって開発されたコンピュータ・ソフトウェア・プログラムの一部分であることもある。その場合、第三者である開発者からのアプリケーション１２０を、ＧＯＯＧＬＥ　ＰＬＡＹ（登録商標）またはＡＰＰＬＥ　ＡＰＰ　ＳＴＯＲＥ（登録商標）を通してダウンロードすることもできる。

【００１３】

セキュア世界１１０Ｂに存在するセキュア・アプレット１３０は、セキュア・タスクを行うように構成されたプログラム・モジュールである。いくつかの実施形態では、セキュア・アプレット１３０は、支払いプロバイダ事業主体によって開発されたコンピュータ・ソフトウェア・プログラムの他の部分である。言い換えると、その筋書きでは、セキュア世界１１０Ｂに存在するセキュア・アプレット１３０および通常世界１１０Ａに存在するアプリケーション１２０は、単一のダウンロード可能なアプリケーションのうちの２つの部分である。

【００１４】

アプリケーション１２０が、より低いレベルのセキュリティーを有する通常世界１１０Ａに存在するので、高いレベルのセキュリティーを必要とするタスクが行われる必要がある場合は、アプリケーション１２０は、セキュア・アプレット１３０からの認証サービスまたは審査サービスを要求することもある。これらのセキュア・タスクには、証明入力サービス、セキュア・アイデンティフィケーション入力サービス、セキュア・ユーザ・インタフェース・サービス、キー・アクセス（key access）・サービス、または暗号化／復号化サービスが含まれることがあるが、これらに限定されない。通常世界１１０Ａとセキュア世界１１０Ｂとは分離されているので、通常世界１１０Ａとセキュア世界１１０Ｂとの通信を行うために、モニタ１４０として知られるソフトウェア・モジュールを使用することもある。いくつかの実施形態では、モニタ１４０が、通常世界１１０Ａとセキュア世界１１０Ｂとの唯一の通信手段である。たとえば、モニタ１４０は、アプリケーション１２０をセキュア世界１１０Ｂ内のいかなるエンティティにもアクセスさせることなく、アプリケーション１２０とのインタフェースをとることができる。次いで、モニタ１４０が、アプリケーション１２０からの要求を、セキュア・アプレット１３０など、セキュア世界

１１０Ｂ内の対象エンティティに中継することができる。次いで、モニタ１４０が、時には検証キーまたはトークンなどの要求資源とともに、アプリケーション１２０にフィードバックを与える。

【００１５】

しかし、図示の実施形態では、モニタ１４０が、大きく（または少なくとも部分的に）バイパスされている。代わりに、通常世界１１０Ａとセキュア世界１１０Ｂとの間の通信を行うために、通常世界１１０Ａに存在する「フック（hook）」１５０Ａおよびセキュア世界１１０Ｂに存在する「フック」１５０Ｂを使用することもできる。フック１５０Ａおよび１５０Ｂは、ソフトウェア・モジュール、または、モニタ１４０上で動作する論理機能とすることができる。モニタ１４０は、２つの世界１１０Ａ-１１０Ｂ間のゲートウェイのように機能し、オペレーティング・システム・レベルでスイッチングを行い、フック１５０Ａ-１５０Ｂは、２つの世界１１０Ａ-１１０Ｂ間のゲートウェイを事実上「開いたまま」にする「ドアストップ」として機能し、アプリケーション・レベルでスイッチングを行う。いくつかの実施形態では、フック１５０Ａ-１５０Ｂは、単一のアプリケーションのためにゲートウェイを「開いたまま」にする。言い換えると、１つのアプリケーションにより使用される際、フック１５０Ａ-１５０Ｂにサインまたは承認されていない他のアプリケーションが、その当初のアプリケーションをプライオリティ・リストから落とすことはできない。各フックは、自体のスペース内、または、それぞれの世界内のアプリケーションもしくはアプレット内に存在してもよい。

【００１６】

セキュア世界１１０Ｂに存在するフック１５０Ｂは、モニタ・ツールキット１６０の資源により実装される。モニタ・ツールキット１６０は、モニタ機能一式を含む。１度目のプロビジョニングおよび起動については、フック１５０Ａおよびフック１５０Ｂはモニタ１４０をなお通過することがあるが、このことは、経路１７０で示している。その後、フック１５０Ａとフック１５０Ｂとの間で直接通信を確立することができるが、このことは、経路１８０で示している。したがって、アプリケーション１２０など、通常世界１１０Ａに存在するエンティティは、モニタ１４０をバイパスしながら、フック１５０Ａ-１５０Ｂを通して、セキュア・アプレットなど、セキュア世界１１０Ｂに存在する信頼されたエンティティと通信することもできる。

【００１７】

モバイル・デバイス取引内のセキュリティーを高めるために、図１で説明するシステムを使用することが可能である。たとえば、認証を要求しているアプリケーションが、遠く離れたセキュア・エンティティによる検証を求めることができない場合（このことは、ネットワーク接続のロスまたは他の理由に起因することある）、セキュア世界のセキュア・アプレット１３０を使用して、このアプリケーションを認証または審査することもできる。このことが可能であるのは、セキュア世界１１０がモバイル・デバイス自体に対してローカルなものであるとしても、セキュア・アプレット１３０（および他のエンティティ）がセキュア世界１１０Ｂに存在するので既にセキュアなものとして妥当性が認められているからである。この意味で、電子チップ１００のセキュア世界１１０Ｂは、高まったセキュリティーを伴うタスクを行うようになされている。

【００１８】

たとえば、支払いプロバイダ事業主体は、セキュリティーの妥当性確認が支払いプロバイダ事業主体によりセキュア世界からも同様に行われる様々なプロットフォーム用のアプリケーションを、この支払いプロバイダ事業主体のパートナーが開発することを可能にする開発者キットを、パートナーに提供することができる。開発者のアプリケーションが正当なものであることを確認する方法を開発者に提供することは、取引の整合性についてエンドユーザを安心させるだけでなく、詐欺的取引が行われるのを開発者が目にするリスクを制限する。これは、支払いプロバイダ・エンティティのモバイル・ライブラリから、第三者である開発者からのアプリケーションにサインをするようになされた機能のサブセットを作成することにより行うことができる。こうした第三者は、支払いプロバイダからの

アプリケーション・プログラミング・インタフェース（ＡＰＩ）を適切に活用し、自体の対スプーフィング／対フィッシング・ユーザ体験を提供することができる。

【００１９】

少なくとも２つのユースケースが適用される。「Ｉｎ　Ａｐｐ　Ｐａｙｍｅｎｔ」ユースケースでは、支払いプロバイダが、自体のライブラリを商業者などの第三者である開発者に提供することができる。この第三者である開発者に開発されたアプリケーション（例、アプリケーション１２０）は、支払いプロバイダからのライブラリを含むこともできるが、こうすることで、自体のライブラリに、支払いプロバイダのセキュア世界モジュール（例、セキュア世界１１０Ｂに存在するセキュア・アプレット１３０）にのみ理解されるコード列が埋め込まれる。なりすましたアプリケーションが、第三者である開発者からの正当なアプリケーションを模倣しようとすると、それは、支払いモジュールの開始時に失敗する。

【００２０】

「Ｉｎ　Ｆｌｏｗ　Ｐａｙｍｅｎｔ」ユーザ・ケースでは、第三者支払いプロバイダからのアプリケーションと同様に第三者である開発者からのアプリケーションも、スタンド・アロン・モードである。支払い時に、１つのアプリケーションから他方のアプリケーションへの移譲がある。その第三者アプリケーションによる支払いプロバイダ・アプリケーションの呼出しの妥当性を確認する妥当性確認メカニズムを、セキュア世界１１０Ｂに格納することができる。

【００２１】

上記のユースケースを説明するための例として、「Ｂｉｇ　Ｍａｒｔ」という商業者が、ユーザのモバイル・デバイスにダウンロード可能なショッピング・アプリケーションを開発すると仮定する。「Ｂｉｇ　Ｍａｒｔ」は、支払いプロバイダ事業主体のパートナーのうちの１つであってもよい。したがって、支払いプロバイダ事業主体は、自体のライブラリを「Ｂｉｇ　Ｍａｒｔ」に提供してもよい。このライブラリは、対応キーに整合することの可能なキーなど、埋め込んだセキュリティー・メカニズムを有する。実際に、支払いプロバイダは、自体の複数のパートナー開発者に、異なる一連のキーを割り当てることができる。支払いプロバイダは、どのキーがどの開発者に割り当てられているかの記録をとり、その情報を自体のダウンロード可能なアプリケーション内に維持することができる。

【００２２】

支払いプロバイダのユーザは、支払いプロバイダからのアプリケーションならびに「Ｂｉｇ　Ｍａｒｔ」からのアプリケーションを自身のモバイル・デバイスにダウンロードする。ユーザは、「Ｂｉｇ　Ｍａｒｔ」からのアプリケーションを使用することにより、オンライン購入を行うことができる。この時、「Ｂｉｇ　Ｍａｒｔ」アプリケーションは、ユーザの名前、住所、クレジットカード情報などの機密情報をユーザに尋ねることがある。従来式の支払いシナリオでは、ユーザは、「Ｂｉｇ　Ｍａｒｔ」からのアプリケーションが正当なものであること、または信用してよいことを知ることができない。ここでは、「Ｂｉｇ　Ｍａｒｔ」アプリケーションは、ユーザのモバイル・デバイスのセキュア世界に存在するセキュア・アプレットにより、認証または審査することができる。いくつかの実施形態では、認証（authentication）とは、特定のアプリケーションの正当性および／またはセキュリティーの妥当性をそれ自体のために確認するプロセスのことである場合があり、審査（vetting）とは、特定のアプリケーションの正当性および／またはセキュリティーの妥当性を他に対して確認するプロセスのことである場合がある。言い換えると、特定のアプリケーションを審査することは、他者がこのことを信用可能であることを意味する。例に戻ると、「Ｂｉｇ　Ｍａｒｔ」アプリケーションの認証および／または審査は、セキュア世界に存在する支払いプロバイダのセキュア・アプレットで行うことができる。具体的には、「Ｂｉｇ　Ｍａｒｔ」アプリケーションは、フックを通してセキュア・アプレットに自体の認証証明または審査証明を提示する。認証証明または審査証明は、支払いプロバイダ事業主体により「Ｂｉｇ　Ｍａｒｔ」アプリケーションに与えられたキーを

含むことがある。セキュア・アプレットは、そのキーを検索し、セキュア世界に記憶された対応するキーとペアにするように試みる。キーのペアリングが成功すれば、これは「Ｂｉｇ　Ｍａｒｔ」アプリケーションが正当で、信用できるものであることを意味し、こうして、「Ｂｉｇ　Ｍａｒｔ」アプリケーションは、認証および審査される。キーのペアリングが成功しなければ、これは「Ｂｉｇ　Ｍａｒｔ」アプリケーションが偽物のアプリケーションであるかもしれないことを示し、それは認証または審査されない。

【００２３】

いくつかの実施形態では、「Ｂｉｇ　Ｍａｒｔ」アプリケーションの認証または審査は、モバイル・デバイス上の可視表現および／または音声表現でユーザに通信されることがある。たとえば、モバイル・デバイスの表示画面は、「Ｂｉｇ　Ｍａｒｔ」アプリケーションが認証および審査され、ユーザが先に進み、盗みまたはデータ損失の心配なく機密情報を「Ｂｉｇ　Ｍａｒｔ」アプリケーションに提供してよいことをユーザに知らせるための特定のパターンを表示することができる。

【００２４】

図２は、本開示内容の様々な態様を示す簡略高レベル・アーキテクチャ２００である。アーキテクチャ２００は、支払いプロバイダ２１０を含む。支払いプロバイダは、カリフォルニア州、サンノゼのＰＡＹＰＡＬ，ＩＮＣ（登録商標）などの事業主体、または、ユーザの口座に送金を行うことおよびユーザの口座から送金を行うことの可能な他の適当な金融機関であってもよい。支払いプロバイダ２１０は、「クラウド」内に離れて位置するサーバを有し、相互認証イネーブルメント（mutual authentication enablement）・サービス、ポスト／プレ・プロビジョニング（post/pre-provisioning）・サービス、リモート・イネーブルメント（remote enablement）・サービス、無線（ＯＴＡ）サービスなどのサービスを行うように構成される。

【００２５】

また、アーキテクチャ２００は、互いに並行して動作するが、互いから分離した通常世界２２０Ａおよびセキュア世界２２０Ｂを含む。トラストレット（セキュア・アプレット）２３０が、セキュア世界２２０Ｂ内に存在する。トラストレット２３０は、支払いプロバイダ２１０に信用されたアプリケーションであってもよい（たとえば、トラストレット２３０は、支払いプロバイダ２１０に開発されたアプリケーションであってもよい）。トラストレット２３０は、支払いプロバイダ２１０と直接通信することができる。アプリ２４０（１つまたは複数のアプリケーションを含むことができる）が、セキュア世界２２０Ａ内に存在する。アプリ２４０は、セキュアなオペレーションが行われることが必要な外部エンティティ２５０と通信を行うので、セキュア世界２２０Ｂへの切替えを必要とする。これらのセキュア・オペレーションには、証明入力サービス、セキュアＩＤサービス、セキュア・ユーザ・インタフェース・サービス、キー・アクセス・サービス、または暗号化／復号化サービスが含まれることがある。

【００２６】

通常オペレーティング・システム２６０が、通常世界２２０Ａを運営し、セキュア・オペレーティング・システム２７０が、セキュア世界を運営する。セキュア・モニタ２８０が、通常世界２２０Ａとセキュア世界２２０Ｂとの間のデフォルト・ゲートウェイとして働く。ただし、オペレーティング・システム２６０は、「フック」２９０を自体の中で制御および維持することが可能なように実装され、オペレーティング・システム２７０は、「フック」２９５を制御および維持することが可能なように実装され、この場合、セキュア世界２２０Ｂとの通信を確立するために、フック２９０-２９５を使用することができる。さらに、通常オペレーティング・システム２６０およびセキュア・オペレーティング・システム２７０は、セキュア世界２２０Ｂに存在する信用されたアプリケーション（例、トラストレット２３０）からのアプリケーションに応答し、通常世界２２０Ａに存在するアプリケーション（例、アプリ２４０）についての信用／審査を証明するために、同一のフック２９０-２９５を使用することが可能なように実装される。このようにして、通常世界２２０Ａと支払いプロバイダ２１０との間にオープンな流れが存在する。すなわち

、モニタ２８０により通信がブロックされず、アプレットおよびアプリケーションを、「クラウド」（言い換えると、支払いプロバイダ２１０のリモート・サーバ）から管理することができる。

【００２７】

通常オペレーティング・システム２６０およびセキュア・オペレーティング・システム２７０についての命令を実行するために、ＴｒｕｓｔＺｏｎｅ（登録商標）-ｅｎａｂｌｅｄ　ＡＲＭ（登録商標）コア・プロセッサ３００を使用する。ＴｒｕｓｔＺｏｎｅ（登録商標）-ｅｎａｂｌｅｄ　ＡＲＭ（登録商標）コア・プロセッサ３００は、セキュア・ヴォールト３１０を含む。プライベート鍵３２０と公開鍵３３０との両方を、セキュア・ヴォールト３１０中に保管することができる。プライベート鍵３４０を、支払いプロバイダ２１０のサーバ内に離して保管することもできる。これらのプライベート鍵および公開鍵は、たとえばアプリ２４０について、認証タスクおよび／または審査タスクを行うために使用することができる。

【００２８】

上で説明した高レベル・アーキテクチャ２００は、本開示内容の概念の多くの実装形態の例のうちの１つに過ぎないことが理解される。他の実施形態が、本開示内容の趣旨および範囲から逸脱することなく、様々な実装形態の詳細を有することもある。

【００２９】

図３は、本開示内容の様々な態様による、認証タスクおよび審査タスクを行う方法４００のフローチャートである。方法４００はステップ４１０を含むが、このステップでは、電子チップの非セキュア部分に存在するアプリケーションからの認証要求が受け取られる。いくつかの実施形態では、電子チップには、モバイル電子デバイス上のコンピュータ・メモリが含まれる。他の実施形態では、電子チップには、モバイル電子デバイス上のコンピュータ・プロセッサが含まれる。認証要求は、アプリケーションの証明を含む。いくつかの実施形態では、こうした証明は、アプリケーションの開発者に割り当てられた認証証書を含む。たとえば、認証証書はキーを含むことがある。

【００３０】

方法４００はステップ４２０を含むが、このステップでは、電子チップのセキュア部分に存在するセキュア・アプレットとの通信が行われる。セキュア部分は、非セキュア部分から分離している。この通信には、アプリケーションの証明をセキュア・アプレットに転送することが含まれる。いくつかの実施形態では、アプリケーションは、第三者である開発者からのソフトウェア・プログラムであり、セキュア・アプレットは、支払いプロバイダからのソフトウェア・プログラムの一部分である。他の実施形態では、アプリケーションおよびセキュア・アプレットはともに、支払いプロバイダからのソフトウェア・プログラムの一部分である。電子チップのセキュア部分と電子チップの非セキュア部分との間のゲートウェイとして構成されたモニタを少なくとも部分的にバイパスすることによっても、少なくとも部分的には通信が行われる。

【００３１】

方法４００はステップ４３０を含むが、このステップでは、アプリケーションが、アプリケーションの証明に基づいて認証および審査される。特定の実施形態では、認証および審査を、リモート・サーバにアクセスすることなく行う。

【００３２】

上で議論したステップ４１０～４３０の前、最中、または後に追加の方法ステップを実行することもできることが分かる。ただし、簡潔にするために、こうした追加のステップについては、本明細書では具体的に説明または議論を行わない。

【００３３】

図４は、たとえば、方法４００の様々な方法ステップといった、本明細書で説明する様々な方法およびデバイスを実装するのに適したコンピュータ・システム６００のブロック図である。様々な実装形態で、これらのステップを実行することの可能なデバイスが、ネットワーク通信デバイス（例、モバイル携帯電話、ラップトップ、パーソナル・コンピュ

ータ、タブレットなど）、ネットワーク・コンピューティング・デバイス（例、ネットワーク・サーバ、ＴｒｕｓｔＺｏｎｅ（登録商標）対応コンピュータ・プロセッサ、電子通信インタフェースなど）、または他の適当なデバイスを含むこともある。したがって、方法４００を実装可能なデバイスを、以下のようにして、コンピュータ・システム６００として実装することができることを理解されたい。

【００３４】

本開示内容の様々な実施形態によれば、ネットワーク・サーバやモバイル通信デバイスなどのコンピュータ・システム６００が、バス・コンポーネント６０２または情報通信用の他の通信メカニズムを含むが、これらは、ＴｒｕｓｔＺｏｎｅ（登録商標）対応処理コンポーネント６０４（例、プロセッサ、マイクロ・コントローラ、デジタル信号プロセッサ（ＤＳＰ）など）、システム・メモリ・コンポーネント６０６（例、ＲＡＭ）、静的記憶コンポーネント６０８（例、ＲＯＭ）、ディスク・ドライブ・コンポーネント６１０（例、磁気的または光学的）、ネットワーク・インタフェース・コンポーネント６１２（例、モデムまたはイーサーネット・カード）、表示コンポーネント６１４（例、陰極線管（ＣＲＴ）ディスプレイまたは液晶ディスプレイ（ＬＣＤ））、入力コンポーネント６１６（例、キーボード）、カーソル制御コンポーネント６１８（例、マウスまたはトラックボール）、画像キャプチャ・コンポーネント６２０（例、アナログ・カメラまたはデジタル・カメラ）などのサブシステムおよびコンポーネントを相互接続する。一実装形態では、ディスク・ドライブ・コンポーネント６１０が、１つ以上のディスク・ドライブ・コンポーネントを有するデータベースを含むことがある。

【００３５】

本開示内容の実施形態によれば、コンピュータ・システム６００は、ＴｒｕｓｔＺｏｎｅ（登録商標）対応プロセッサ６０４がシステム・メモリ・コンポーネント６０６に含まれる１つ以上の命令からなる１つ以上のシーケンスを実行することにより、特定のオペレーションを実行する。こうした命令は、静的記憶コンポーネント６０８やディスク・ドライブ・コンポーネント６１０などの他のコンピュータ可読媒体から、システム・メモリ・コンポーネント６０６に読み込むことができる。他の実施形態では、本開示内容を実現するために、ソフトウェア命令の代わりに（またはこれと組み合わせて）ハードワイヤード回路を使用することもできる。

【００３６】

ロジックをコンピュータ可読媒体内で符号化することもできるが、この媒体は、実行用に命令をＴｒｕｓｔＺｏｎｅ（登録商標）対応プロセッサ６０４に提供することに関与する任意の媒体を指すこともある。こうした媒体は、不揮発性媒体および揮発性媒体を含めた多くの形態をとることができるが、不揮発性媒体および揮発性媒体に限定されない。一実施形態では、コンピュータ可読媒体は非一時的媒体である。様々な実装形態で、不揮発性媒体は、ディスク・ドライブ・コンポーネント６１０などの光ディスクまたは磁気ディスクを含み、揮発性媒体は、システム・メモリ・コンポーネント６０６などの動的メモリを含む。一態様では、電波通信および赤外データ通信中に生成されるものを含めた音波または光波の形態のものなどの伝送媒体を介して、実行命令に関連するデータおよび情報をコンピュータ・システム６００に送信することができる。様々な実装形態で、伝送媒体には、バス６０２を備えたワイヤを含めて、同軸ケーブル、銅線、およびファイバ・オプティックスが含まれることがある。

【００３７】

コンピュータ可読媒体のいくつかの一般的な形態には、たとえば、フロッピー・ディスク、フレキシブル・ディスク、ハード・ディスク、磁気テープ、他の任意の磁気媒体、ＣＤ-ＲＯＭ、他の任意の光媒体、パンチ・カード、紙テープ、穴のパターンを伴う他の任意の物理的媒体、ＲＡＭ、ＰＲＯＭ、ＥＰＲＯＭ、ＦＬＡＳＨ-ＥＰＲＯＭ、他の任意のメモリ・チップもしくはメモリ・カートリッジ、搬送波、または、コンピュータが読取りを行うようになされた他の任意の媒体が含まれる。

【００３８】

本開示内容の様々な実施形態では、本開示内容を実現するための命令シーセンスの実行が、コンピュータ・システム６００により行われることがある。本開示内容の他の様々な実施形態では、通信リンク６３０（例、ＬＡＮ、ＷＬＡＮ、ＰＴＳＮや、テレコミュニケーション・ネットワーク、モバイル・ネットワークおよび携帯電話ネットワークを含めた他の様々な有線または無線ネットワークなどの通信ネットワーク）により結合された複数のコンピュータ・システム６００が、互いに協働して本開示内容を実現するために命令シーケンスを実行することもある。

【００３９】

コンピュータ・システム６００は、１つまたは複数のプログラム（すなわち、アプリケーション・コード）を含めて、メッセージ、データ、情報および命令を通信リンク６３０および通信インタフェース６１２を通して送信および受信することができる。受信されたプログラム・コードは、ディスク・ドライブ・コンポーネント６１０もしくは他の何らかの不揮発性記憶コンポーネント内に実行のために受け入れられた時、および／または、そこに格納された時に、ＴｒｕｓｔＺｏｎｅ（登録商標）対応プロセッサ６０４により実行されることがある。

【００４０】

適用可能であれば、本開示内容により提供する様々な実施形態を、ハードウェア、ソフトウェア、またはハードウェアとソフトウェアとの組合せを使用して実現することもできる。また、適用可能であれば、本開示内容の趣旨から逸脱することなく、本明細書に記載の様々なハードウェア・コンポーネントおよび／またはソフトウェア・コンポーネントを組み合わせて、ソフトウェア、ハードウェア、および／またはその両方を備える複合コンポーネントにすることもできる。適用可能であれば、本開示内容の範囲から逸脱することなく、本明細書に記載の様々なハードウェア・コンポーネントおよび／またはソフトウェア・コンポーネントを、ソフトウェア、ハードウェア、またはその両方を備える複数のサブ・コンポーネントに分離することもできる。さらに、適用可能であれば、ソフトウェア・コンポーネントを、ハードウェア・コンポーネントとして実現することができ、その逆もまた同じであることが企図される。

【００４１】

コンピュータ・プログラム・コードやコンピュータ・プログラム・データなど、本開示内容によるソフトウェアは、１つ以上のコンピュータ可読媒体上に記憶することができる。１つ以上の汎用または特定目的コンピュータおよび／またはコンピュータ・システムをネットワーク化したものおよび／またはそうしていないものを使用することにより、本明細書中で特定したソフトウェアを実装することができることも企図される。適用可能であれば、本明細書で説明した特徴を実現するために、本明細書に記載する様々なステップの順序を変更すること、複合ステップに組み合わせること、および／または、複数のサブステップに分離することができる。

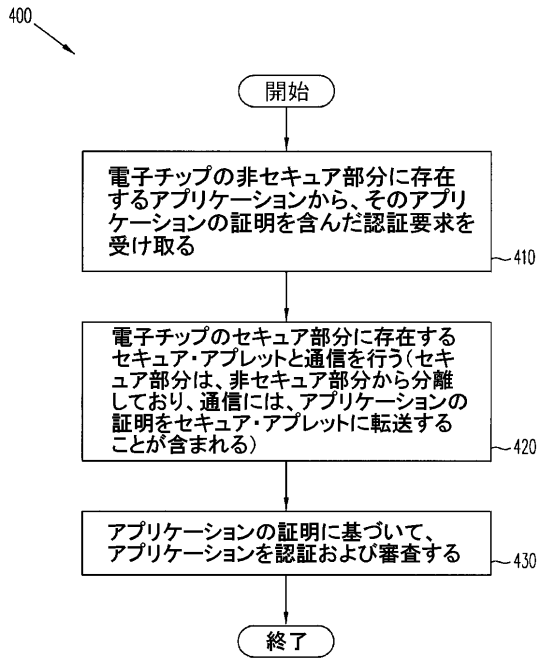
【００４２】

図面のうちの１つまたは複数に示す同様の要素を識別するために、同様の参照符号を付していることを理解されたい。ラベル分けしたこれらの図面は、本開示内容の実施形態を説明することを目的としており、それらを限定することを目的としていない。

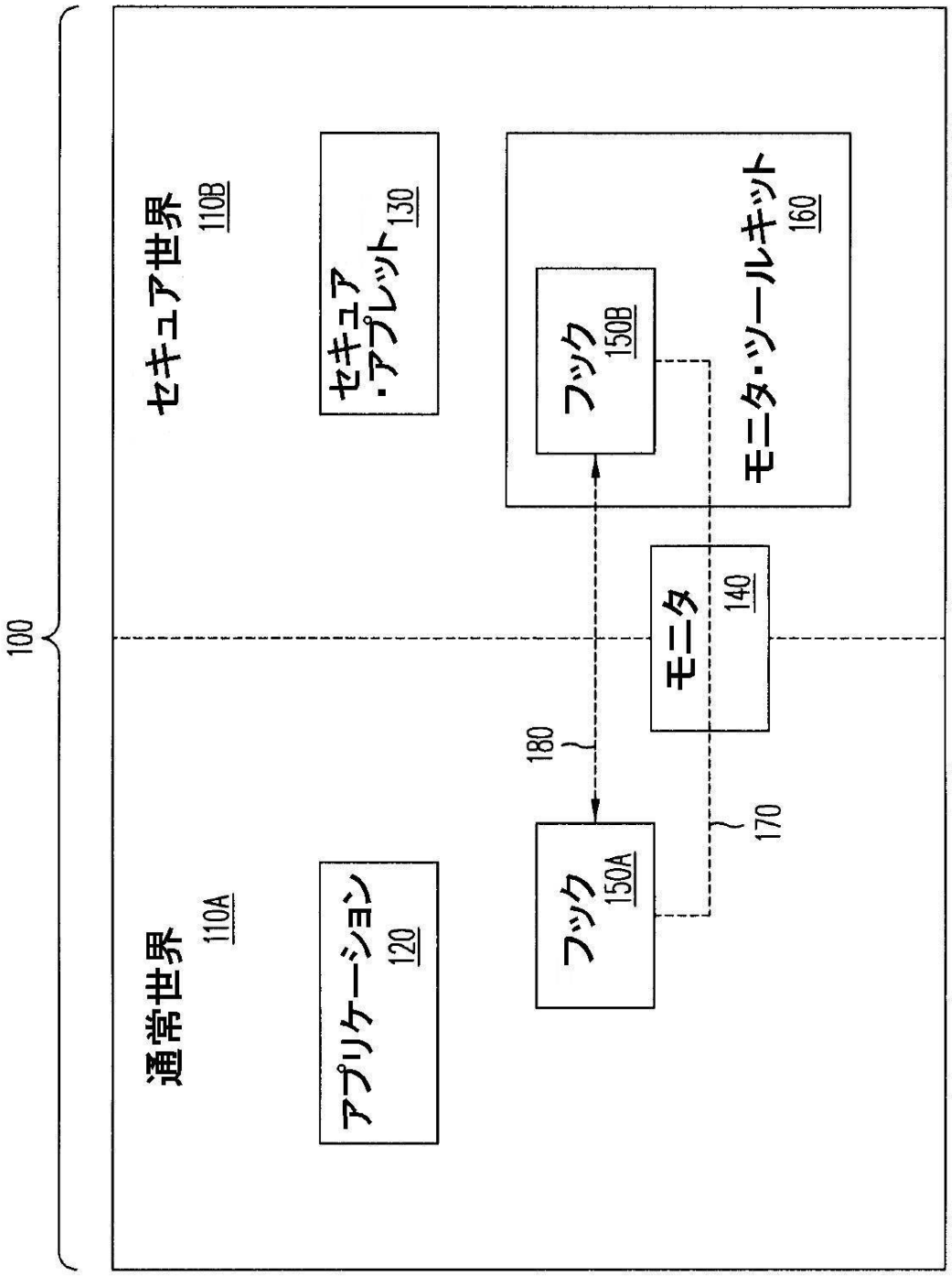
【００４３】

先に述べた開示内容は、開示した厳密な形態または特定の使用分野に、本開示内容を限定することを意図しない。よって、本開示内容に対する様々な代替実施形態および／または修正形態が、それらが本明細書中で明示されたか暗示されたかに関わらず、本開示内容に鑑みて使用可能であることが企図される。このようにして記載した本開示内容の実施形態をもって、当業者は、本開示内容の範囲から逸脱することなく、形式および詳細について変更を加えることができることを理解するであろう。したがって、本開示内容は、特許請求の範囲によってのみ限定される。

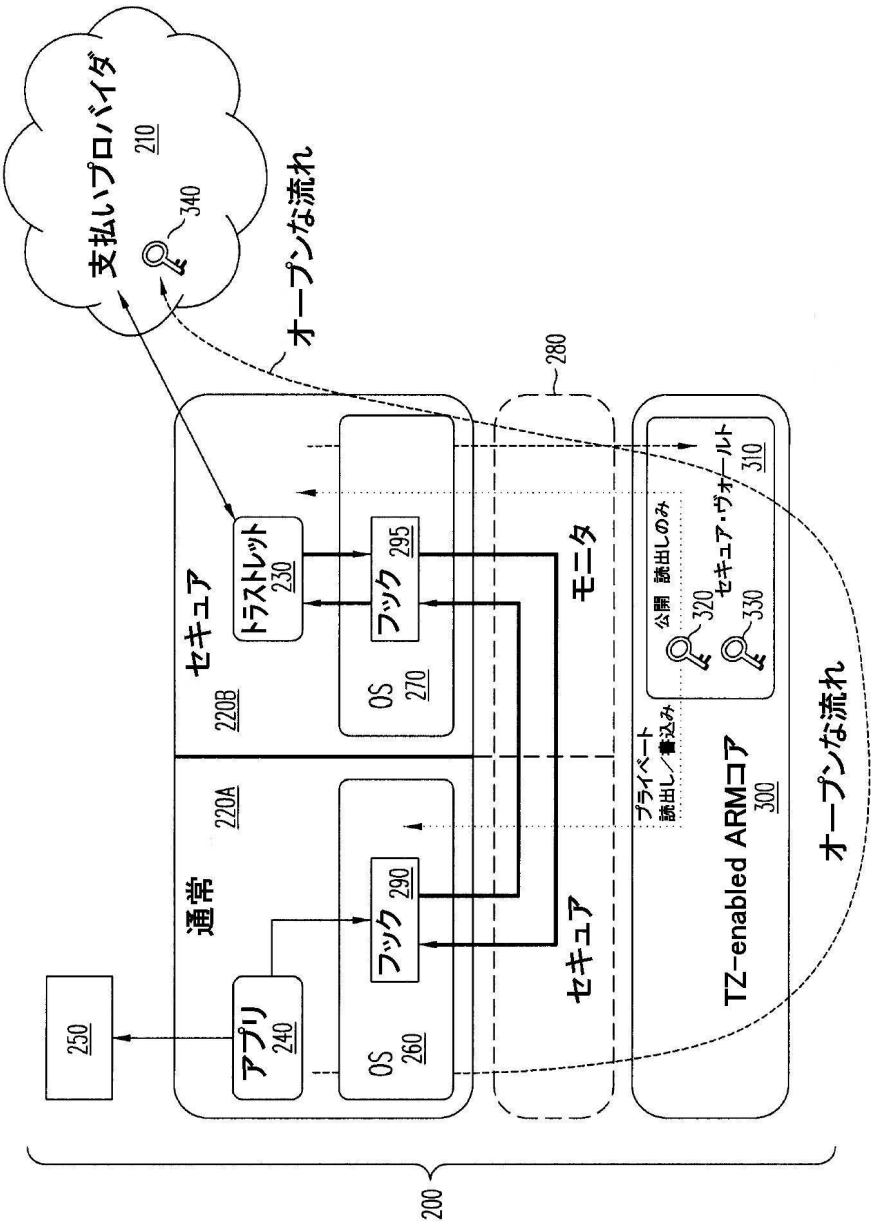
【図３】


400
開始
電子チップの非セキュア部分に存在するアプリケーションから、そのアプリケーションの証明を含んだ認証要求を受け取る
410
電子チップのセキュア部分に存在するセキュア・アプレットと通信を行う（セキュア部分は、非セキュア部分から分離しており、通信には、アプリケーションの証明をセキュア・アプレットに転送することが含まれる）
420
アプリケーションの証明に基づいて、アプリケーションを認証および審査する
430
終了

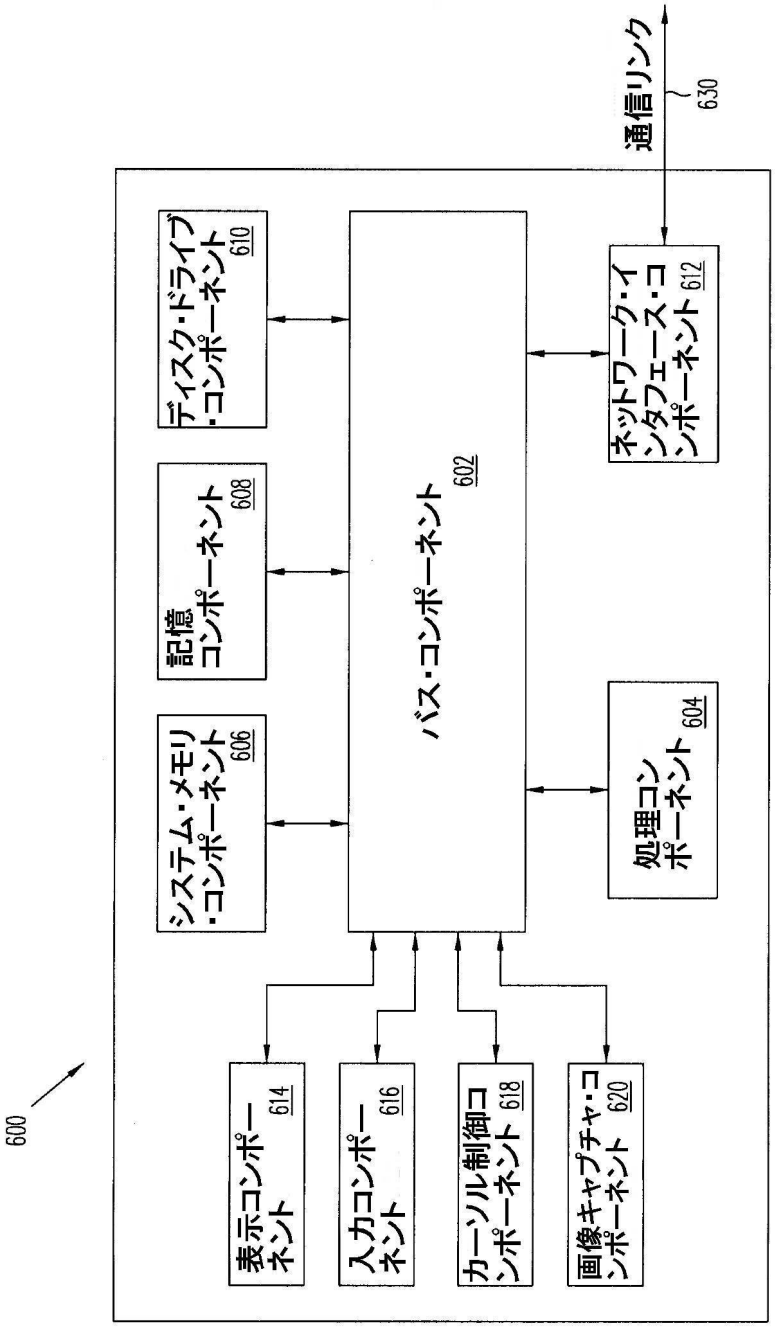
【図１】


100
セキュア世界
110B
通常世界
110A
セキュア・アプレット
130
アプリケーション
120
モニタ・ツールキット
160
フック
150B
フック
150A
モニタ
140
180
170

【図２】


支払いプロバイダ
210
340
オープンな流れ
280
セキュア
220B
トラストレット
230
フック
295
OS
270
モニタ
通常
220A
フック
290
OS
260
アプリ
240
250
セキュア
プライベート
読出し／書込み
公開 読出しのみ
320
セキュア・ヴォールト
330
TZ-enabled ARMコア
300
310
オープンな流れ
200

【図４】


600
通信リンク
630
ディスク・ドライブ・コンポーネント 610
記憶コンポーネント 608
システム・メモリ・コンポーネント 606
バス・コンポーネント 602
ネットワーク・インタフェース・コンポーネント 612
処理コンポーネント 604
表示コンポーネント 614
入力コンポーネント 616
カーソル制御コンポーネント 618
画像キャプチャ・コンポーネント 620

フロントページの続き

(72)発明者　ナハリ，ハーディ
アメリカ合衆国，カリフォルニア州　９４０４０，マウンテン　ビュー，ランニングウッド　サークル　８１５

審査官　平井　誠

(56)参考文献　特開２００４－１７１５６３（ＪＰ，Ａ）
米国特許出願公開第２００９／０３２８２０７（ＵＳ，Ａ１）
米国特許出願公開第２００９／０２６５７５６（ＵＳ，Ａ１）
米国特許出願公開第２００８／０２１６０９６（ＵＳ，Ａ１）
米国特許出願公開第２００９／０１５０６７８（ＵＳ，Ａ１）
米国特許出願公開第２００９／０１６５０８１（ＵＳ，Ａ１）
特開２００９－２３０５４９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１