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

特許第6440721号
(P6440721)

(45)発行日　平成30年12月19日(2018.12.19)　(24)登録日　平成30年11月30日(2018.11.30)

(51)Int.Cl.		F I		
G06F 21/44	(2013.01)	G06F	21/44	
H04L 9/32	(2006.01)	H04L	9/00	675A
G06F 21/12	(2013.01)	G06F	21/12	310

請求項の数 7　(全 12 頁)

(21)出願番号	特願2016-547148 (P2016-547148)
(86)(22)出願日	平成27年1月16日 (2015.1.16)
(65)公表番号	特表2017-506778 (P2017-506778A)
(43)公表日	平成29年3月9日 (2017.3.9)
(86)国際出願番号	PCT/US2015/011838
(87)国際公開番号	WO2015/116410
(87)国際公開日	平成27年8月6日 (2015.8.6)
審査請求日	平成29年12月26日 (2017.12.26)
(31)優先権主張番号	14/166,743
(32)優先日	平成26年1月28日 (2014.1.28)
(33)優先権主張国	米国(US)

(73)特許権者　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　マリア・エル・ミランダ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

最終頁に続く

(54)【発明の名称】コンピューティングデバイスによるアプリケーションの使用の認証

(57)【特許請求の範囲】

【請求項１】

アプリケーションを使用するのを認証する方法であって、

最初のブートアップ時に前記アプリケーションのための固有ダイジェストを生成するステップと、

前記固有ダイジェストをセキュアメモリに記憶するステップと、

後続のブートアップ時に前記アプリケーションのためのアプリケーションダイジェストを計算するステップと、

前記計算されたアプリケーションダイジェストが前記記憶された固有ダイジェストと一致する場合、前記アプリケーションを使用するのを認証するステップであって、前記固有ダイジェストは、前記最初のブートアップ時に、少なくとも、プロセッサに関連付けられるシリアル番号と前記アプリケーションのハッシュとの連結を含み、前記固有ダイジェストは署名プロセスを用いることなく生成される、ステップと

を含む、方法。

【請求項２】

前記計算されたアプリケーションダイジェストが前記記憶された固有ダイジェストと一致しない場合、前記アプリケーションは使用するのを認証されない、請求項1に記載の方法。

【請求項３】

後続のブートアップ時に前記計算されたアプリケーションダイジェストは、前記プロセ

ッサに関連付けられる前記シリアル番号と前記アプリケーションの前記ハッシュとに基づく、請求項1に記載の方法。
【請求項４】
コードを含む非一時的コンピュータ可読記録媒体であって、前記コードは、プロセッサによって実行されるときに、前記プロセッサに、請求項1～3のいずれか一項に記載の方法を行わせる、非一時的コンピュータ可読記録媒体。
【請求項５】
コンピューティングデバイスであって、
最初のブートアップ時にアプリケーションのための固有ダイジェストを生成するための手段と、
前記固有ダイジェストをセキュアメモリに記憶するための手段と、
後続のブートアップ時に前記アプリケーションのためのアプリケーションダイジェストを計算するための手段と、
前記計算されたアプリケーションダイジェストが前記記憶された固有ダイジェストと一致する場合、前記アプリケーションを使用するのを認証するための手段であって、前記固有ダイジェストは、前記最初のブートアップ時に、少なくとも、プロセッサに関連付けられるシリアル番号と前記アプリケーションのハッシュとの連結を含み、前記固有ダイジェストは署名プロセスを用いることなく生成される、手段と
を含む、コンピューティングデバイス。
【請求項６】
前記計算されたアプリケーションダイジェストが前記記憶された固有ダイジェストと一致しない場合、前記アプリケーションは使用するのを認証されない、請求項5に記載のコンピューティングデバイス。
【請求項７】
後続のブートアップ時に前記計算されたアプリケーションダイジェストは、前記プロセッサに関連付けられる前記シリアル番号と前記アプリケーションの前記ハッシュとに基づく、請求項5に記載のコンピューティングデバイス。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明はコンピューティングデバイスによるアプリケーションの使用を認証する装置および方法に関する。
【背景技術】
【０００２】
通常、コンピューティングデバイスのためのアプリケーションは、コンピューティングデバイスに結び付けられ、使用するために認証される。この実施態様では、ブートアップ時にアプリケーションがロードされるとき、アプリケーションを認証するために署名ダイジェストおよびアプリケーションダイジェストが生成され、そのいずれも多くの場合にチップのシリアル番号を利用する。署名ダイジェストは、ブートROMまたはワンタイムプログラマブルメモリに記憶される公開鍵を用いて解読された署名に基づく。アプリケーションダイジェストは、アプリケーションのハッシュ関数と、シリアル番号とを組み合わせて生成される。署名ダイジェストは、ローカルに計算された計算ハッシュダイジェストと比較され、それらのダイジェストが同じである場合、アプリケーションが認証される。そうでない場合、アプリケーションは認証されない。
【０００３】
残念なことに、チップベンダの固有のシリアル番号に基づく静的署名は、面倒であることがわかっている。
【発明の概要】
【課題を解決するための手段】
【０００４】

本発明の態様は、アプリケーションの使用を認証する装置および方法に関連することができる。コンピューティングデバイスが、アプリケーションを利用することができ、セキュアメモリおよびプロセッサを含むことができる。プロセッサは、最初のブートアップ時にアプリケーションのための固有ダイジェストを生成し、固有ダイジェストをセキュアメモリに記憶し、後続のブートアップ時にアプリケーションのためのアプリケーションダイジェストを計算し、計算されたアプリケーションダイジェストが記憶された固有ダイジェストと一致する場合、アプリケーションの使用を認証することができる。

【図面の簡単な説明】

【０００５】

【図１】本発明の態様を実施できるコンピューティングデバイスの図である。

【図２】アプリケーションの使用を認証されるか否かを判断するプロセスの一例を示す流れ図である。

【図３】アプリケーションの使用を認証するか、または認証しないプロセスを実施するために利用することができる構成要素を示すブロック図である。

【図４】計算されたアプリケーションダイジェストを求め、アプリケーションの使用を認証するか、または認証しない際に利用される機能に関連するプロセスの一例を示す図である。

【発明を実施するための形態】

【０００６】

「例示的」または「例」という単語は、本明細書では「例、事例、または例示としての役割を果たすこと」を意味するために使用される。「例示的」または「例」として本明細書に記載される任意の態様または実施形態は、他の態様または実施形態に比べて好ましいか、または有利であると必ずしも解釈されるべきではない。

【０００７】

本明細書において用いられるときに、「コンピューティングシステムまたはデバイス」という用語は、限定はしないが、ラップトップおよびデスクトップコンピュータ、タブレット、スマートフォン、テレビ、家庭電化製品、セルラー電話、パーソナルテレビデバイス、携帯情報端末(PDA)、パームトップコンピュータ、ワイヤレス電子メールレシーバ、マルチメディアインターネット対応セルラー電話、グローバルポジショニングシステム(GPS)レシーバ、ワイヤレスゲームコントローラ、車両(たとえば、自動車)に内蔵されるレシーバ、インタラクティブゲームデバイス、ノートブック、スマートブック、ネットブック、モバイルテレビデバイス、または任意のデータ処理装置を含む、任意の形のプログラマブルコンピュータデバイスを指している。

【０００８】

これ以降詳細に説明される、アプリケーションの使用を認証するために利用することができる一例のコンピューティングデバイス100が、図1に示される。コンピューティングデバイス100は、バス105を介して電気的に結合することができる(または必要に応じて他の方法で通信することができる)ハードウェア要素を備えるように図示されている。ハードウェア要素は、限定はしないが、1つもしくは複数の汎用プロセッサおよび/または1つもしくは複数の専用プロセッサ(デジタル信号処理チップ、グラフィックス加速プロセッサなど)を含む1つもしくは複数のプロセッサ110と、1つもしくは複数の入力デバイス115(たとえば、キーボード、キーパッド、タッチスクリーン、マウスなど)と、少なくとも1つのディスプレイデバイス121を含み、さらに、限定はしないが、スピーカ、プリンタなどを含むことができる1つもしくは複数の出力デバイス120とを含むことができる。さらに、プロセッサ110は、通常モード112およびセキュアモード114において動作することができる。

【０００９】

コンピューティングデバイス100は、限定はしないが、ローカルおよび/またはネットワークアクセス可能記憶装置を含むことができ、かつ/あるいは限定はしないが、ディスクドライブ、ドライブアレイ、光記憶デバイス、プログラム可能、フラッシュ書換え可能な

どとすることができる、ランダムアクセスメモリ(「RAM」)および/もしくはリードオンリーメモリ(「ROM」)などの固体記憶デバイス、ならびに/または同様のものを含むことができる、1つまたは複数の非一時的記憶デバイス125をさらに含む(かつ/または1つまたは複数の非一時的記憶デバイス125と通信する)ことができる。そのような記憶デバイスは、限定はしないが、種々のファイルシステム、データベース構造などを含む、任意の適切なデータストアを実現するように構成することができる。

【００１０】

また、コンピューティングデバイス100は、限定はしないが、モデム、ネットワークカード(ワイヤレスまたは有線)、赤外線通信デバイス、ワイヤレス通信デバイス、および/またはチップセット(BlueTooth(登録商標)デバイス、802.11デバイス、Wi-Fiデバイス、WiMAXデバイス、セルラー通信デバイスなど)などを含むことができる通信サブシステム130をも含むことができる。通信サブシステム130は、ネットワーク、他のコンピュータシステム、および/または本明細書において説明される任意の他のデバイスとデータを交換できるようにする場合がある。多くの実施形態では、コンピューティングデバイス100は、先に説明されたように、RAMまたはROMデバイスを含むことができる作業メモリ135をさらに備える。また、コンピューティングデバイス100は、後にさらに詳細に説明されるように、アプリケーションの使用を認証するのを助けるセキュアメモリ137を含むことができる。

【００１１】

コンピューティングデバイス100はまた、オペレーティングシステム140、アプリケーション145、デバイスドライバ、実行可能ライブラリおよび/または他のコードを含む、作業メモリ135内に現在配置されているように示される、ソフトウェア要素も含むことができる。一実施形態では、本明細書において説明されるような本発明の実施形態を実施するために、方法を実施し、および/またはシステムを構成するように、アプリケーションを設計することができる。単なる例として、以下に論じられる方法に関連して説明される1つまたは複数の手順は、コンピュータデバイス(および/またはコンピュータデバイス内のプロセッサ)によって実行可能なコードおよび/または命令として実現することができ、本発明の実施形態によれば、一態様において、その後、そのようなコードおよび/または命令は、説明される方法に従って1つまたは複数の動作を実行するように汎用コンピュータ(たとえば、コンピューティングデバイス)を構成し、および/または適応させるために使用することができる。

【００１２】

これらの命令および/またはコードのセットは、上記の記憶デバイス125などの非一時的コンピュータ可読記憶媒体に記憶される場合がある。場合によっては、記憶媒体は、コンピューティングデバイス100などのコンピュータシステム内に組み込まれる場合がある。他の実施形態では、記憶媒体は、そこに記憶された命令/コードを用いて汎用コンピュータをプログラムし、構成し、および/または適応させるために使用できるように、コンピュータシステムから分離することができ(たとえば、コンパクトディスクなどのリムーバブルメディア)、かつ/またはインストールパッケージにおいて提供することができる。これらの命令は、コンピュータ制御のコンピューティングデバイス100によって実行可能である実行可能コードの形をとることができ、ならびに/あるいは(たとえば、種々の一般的に入手可能なコンパイラ、インストールプログラム、圧縮/解凍ユーティリティなどのいずれかを用いて)コンピューティングデバイス100上でのコンパイルおよび/またはインストール時に、実行可能コードの形態をとるソースコードおよび/またはインストール可能コードの形をとることができる。

【００１３】

特定の要件に従ってかなりの変更を加えることができることは、当業者には明らかであろう。たとえば、カスタマイズされたハードウェアを使用することもでき、および/または、特定の要素は、ハードウェア、ソフトウェア(アプレットなどのポータブルソフトウェアを含む)、または両方において実現することができる。さらに、ネットワーク入力/出

力デバイスなどの他のコンピューティングデバイスへの接続が用いられる場合もある。

【００１４】

先に説明されたように、現存の従来の方法による(たとえば、チップベンダからの)プロセッサの固有シリアル番号に基づく各ブートアップ時のアプリケーションの静的署名は、面倒であることがわかっている。説明されるように、本発明の実施形態は、ブートアップのためにプロセッサのシリアル番号に基づく署名を必要とはしない。本発明の態様は、署名を必要とすることなく、アプリケーションをコンピューティングデバイスに動的に結び付ける装置および方法を提供する。

【００１５】

詳細には、本発明の態様は、アプリケーションの使用を認証する装置および方法に関連することができる。さらに詳細に説明されるような、一実施形態では、コンピューティングデバイス100は、アプリケーション145の使用を認証するために、セキュアメモリ137およびプロセッサ110を含むことができる。プロセッサ110は、最初のブートアップ時にアプリケーション145のための固有ダイジェストを生成し、固有ダイジェストをセキュアメモリ137に記憶し、後続のブートアップ時にアプリケーション145のためのアプリケーションダイジェストを計算し、計算されたアプリケーションダイジェストが記憶された固有ダイジェストと一致する場合、アプリケーションの使用を認証することを含む、動作を実行するためにセキュアモード114において動作することができる。このようにして、アプリケーション145は、最初のブートアップ時にコンピューティングデバイス100に結び付けることができる。説明されるように、アプリケーション145は、アプリケーションのハッシュ関数およびプロセッサ110のシリアル番号に基づいてアプリケーションのための固有ダイジェストを計算し、その固有ダイジェストをセキュアメモリ137のようなセキュア記憶域に保存することによって、最初のブートアップ時にコンピューティングデバイス100に動的に結び付けることができる。

【００１６】

さらに図2を参照すると、本発明の実施形態を実施する方法プロセス200が以下に説明される。ブロック202において、アプリケーションの最初のブートアップ時にセキュアモード114において動作するプロセッサ110によって、アプリケーション145のための固有ダイジェストが生成される。次に、ブロック204において、セキュアモード114において動作するプロセッサ110によって指示されるのに応じて、固有ダイジェストがセキュアメモリ137に記憶される。ブロック206において、後続のブートアップ時に、セキュアモード114において動作するプロセッサ110が、アプリケーション145のためのアプリケーションダイジェストを計算する。ブロック208において、セキュアモード114において動作するプロセッサ110が、計算されたダイジェストがセキュアメモリ137に記憶された記憶固有ダイジェストと一致すると判断する場合、アプリケーション145の使用が認証される(ブロック210)。しかしながら、計算されたダイジェストがセキュアメモリ137に記憶された固有ダイジェストと一致しない場合、アプリケーション145の使用は認証されない(ブロック212)。

【００１７】

さらに図3を参照すると、アプリケーションを認証するか、または認証しないためのプロセスを実施するために利用することができる構成要素を示すブロック図が以下に説明される。この例では、プロセッサ110は、セキュアブートローダ312およびセキュアオーセンティケータ320のセキュア動作を含むセキュア動作を実行する信頼ゾーン310を生成するために、セキュアモード114において動作する。たとえば、最初のブートアップ時に、セキュアブートローダ312が、コンピューティングデバイスにロードされているアプリケーション145のための固有ダイジェストを生成する。たとえばこれは、そのコンピューティングデバイス上で使用するためのライセンスされたアプリケーションをロードするためにコンピューティングデバイス製造業者によって行われる場合がある。セキュアブートローダ312は、最初のブートアップのための固有ダイジェスト325がアプリケーションのための固有ダイジェストエントリ330としてセキュアメモリ137に記憶されるように指示することができる。(たとえば、コンピューティングデバイスの購入者による、)アプリケーション14

5の後続のブートアップ時に、オーセンティケータ320が、アプリケーション145のためのアプリケーションダイジェストを計算し、そのダイジェストを、アプリケーションのためにセキュアメモリ137にあらかじめ記憶されている固有ダイジェスト327と比較することができる。オーセンティケータ320が、計算されたアプリケーションダイジェストが、アプリケーションのためにセキュアメモリ137に記憶された記憶固有ダイジェスト327と一致すると判断する場合、アプリケーション145は、コンピューティングデバイスによって使用するのを認証される(340)。一方、オーセンティケータ320が、計算されたアプリケーションダイジェストが、アプリケーションのためにセキュアメモリ137に記憶された記憶固有ダイジェスト327と一致しないと判断する場合、アプリケーション145は、コンピューティングデバイスによって使用するのを認証されない(342)。セキュアモード114において動作するプロセッサ110が、先に説明されたセキュアブートローダ312およびオーセンティケータ320の動作を実施できることを理解されたい。

【００１８】

機能、動作および構成要素に関する種々の例示的な実施形態が以下に説明される。たとえば、最初のブートアップのための固有ダイジェスト325は、アプリケーション145の少なくともハッシュ関数に基づいて生成することができる。さらに、最初のブートアップのための固有ダイジェスト325は、プロセッサに関連付けられるシリアル番号325と、アプリケーションのハッシュ関数との連結にさらに基づくことができる。最初のブートアップのためのこの固有ダイジェストは、アプリケーションのための固有ダイジェストエントリ330として、セキュアメモリ137に記憶することができる。その後、後続のブートアップ時に、プロセッサに関連付けられるシリアル番号325およびアプリケーション145のハッシュ関数の連結に基づいて、計算されたアプリケーションダイジェストが求められる。先に説明されたように、オーセンティケータ320が、計算されたアプリケーションダイジェストが、アプリケーションのためにセキュアメモリ137に記憶された記憶固有ダイジェスト327と一致すると判断する場合、アプリケーション145は、コンピューティングデバイスによって使用するのを認証される(340)。一方、オーセンティケータ320が、計算されたアプリケーションダイジェストが、アプリケーションのためにセキュアメモリ137に記憶された記憶固有ダイジェスト327と一致しないと判断する場合、アプリケーション145は、コンピューティングデバイスによって使用するのを認証されない(342)。

【００１９】

一実施形態では、ハッシュ関数はセキュアハッシュアルゴリズムとすることができる。さらに、セキュアメモリ137は、リプレイ保護メモリブロックのような、保護メモリブロックを含むことができる。しかしながら、任意のタイプのセキュアまたは保護タイプのメモリまたは記憶装置を利用できることを理解されたい。

【００２０】

図4をさらに参照すると、計算されたアプリケーションダイジェストを求めること、およびアプリケーションを認証すること、もしくは認証しないことに関連するプロセス400の一例が以下に説明される。一実施形態では、プロセス400において見ることができるように、計算されたアプリケーションダイジェスト415の第1の反復を生成するために、セキュアハッシュアルゴリズム410によって、後続のブートアップ時に、アプリケーション402およびヘッダ404の組合せが処理される。次に、計算されたアプリケーションダイジェストを生成するために、計算されたアプリケーションダイジェスト415の第1の反復が、プロセッサに関連付けられるシリアル番号325と連結される(ブロック420)。決定ブロック430において、オーセンティケータが、計算されたアプリケーションダイジェストが、そのアプリケーションのためにセキュアメモリ137に記憶された記憶固有ダイジェスト330と一致するか否かを判断し、一致する場合、アプリケーションは、コンピューティングデバイスによって使用するのを認証される(450)。一方、決定ブロック430において、オーセンティケータが、計算されたアプリケーションダイジェストが、アプリケーションのためにセキュアメモリ137に記憶された記憶固有ダイジェスト327と一致しないと判断する場合、アプリケーション145は、コンピューティングデバイスによって使用するのを認証されない(45

5)。

【００２１】

したがって、先に説明されたように、最初のブートアップ時に、セキュアブートローダ312は最初にアプリケーション145を認証し、アプリケーションのための固有ダイジェスト330をセキュアメモリ137に記憶する。(プロセッサのシリアル番号で署名することなどの)署名プロセスは不要である。さらに、後続のブートアップ時のいずれにおいても、認証のための署名プロセスは不要である。先に説明されたように、後続のブートアップにおいて、セキュアブートローダ312が、アプリケーション145を認証することができる。ハッシュアルゴリズムを用いてアプリケーションのダイジェストが計算されるとともに、最初のブートアップ時にセキュアメモリ137に保存され、記憶された固有ダイジェスト330と比較することができる。したがって、各アプリケーションの署名は不要である。これは、アプリケーションの認証における時間効率を著しく改善する。

【００２２】

これまでに説明された本発明の態様は、先に説明されたように、デバイス(たとえば、コンピューティングデバイス100)のプロセッサ(たとえば、プロセッサ110)による命令の実行に関連して実施される場合があることを理解されたい。具体的には、限定はしないがプロセッサを含む、デバイスの回路が、本発明の実施形態による方法またはプロセス(たとえば、図2～図4のプロセスおよび機能)を実行するために、プログラム、ルーチンの制御下、または命令の実行下で動作することができる。たとえば、そのようなプログラムは、(たとえば、メモリおよび/または他のロケーションに記憶される)ファームウェアまたはソフトウェアにおいて実現される場合があり、デバイスのプロセッサおよび/または他の回路によって実現される場合がある。さらに、プロセッサ、マイクロプロセッサ、回路、コントローラなどの用語は、ロジック、コマンド、命令、ソフトウェア、ファームウェア、機能などを実行することが可能な任意のタイプのロジックまたは回路を指すことを理解されたい。

【００２３】

デバイスがモバイルデバイスまたはワイヤレスデバイスであるとき、それらのデバイスは、任意の適切なワイヤレス通信技術に基づくか、または別の方法でその技術をサポートするワイヤレスネットワークを通じて1つまたは複数のワイヤレス通信リンクを介して通信できることを理解されたい。たとえば、いくつかの態様では、ワイヤレスデバイスおよび他のデバイスは、ワイヤレスネットワークを含むネットワークと関連付けることができる。いくつかの態様では、そのネットワークは、ボディエリアネットワークまたはパーソナルエリアネットワーク(たとえば超広帯域ネットワーク)を含むことができる。いくつかの態様では、ネットワークは、ローカルエリアネットワークまたはワイドエリアネットワークを含む場合がある。ワイヤレスデバイスは、様々なワイヤレス通信技術、プロトコル、またはたとえば3G、LTE、Advanced LTE、4G、CDMA、TDMA、OFDM、OFDMA、WiMAXおよびWiFiなどの規格のうちの1つまたは複数をサポートすることができるか、または別の方法で使用することができる。同様に、ワイヤレスデバイスは、様々な対応する変調方式または多重化方式のうちの1つまたは複数をサポートすることができるか、または別の方法で使用することができる。したがって、ワイヤレスデバイスは、上記または他のワイヤレス通信技術を使用して、1つまたは複数のワイヤレス通信リンクを確立し、その通信リンクを介して通信するのに適した構成要素(たとえばエアインターフェース)を含むことができる。たとえば、デバイスは、ワイヤレス媒体を介して通信するのを容易にする種々の構成要素(たとえば、信号発生器およびシグナルプロセッサ)を含むことができる、関連するトランスミッタおよびレシーバ構成要素(たとえば、トランスミッタおよびレシーバ)を有するワイヤレストランシーバを備えることができる。よく知られているように、それゆえ、モバイルワイヤレスデバイスは、他のモバイルデバイス、携帯電話、他の有線およびワイヤレスコンピュータ、インターネットウェブサイトなどとワイヤレスに通信することができる。

【００２４】

本明細書の教示は、様々な装置(たとえば、デバイス)に組み込む(たとえば、それらの装置内に実装するか、またはそれらの装置によって実行する)ことができる。たとえば、本明細書において教示される1つまたは複数の態様は、電話(たとえば、セルラー電話)、携帯情報端末(「PDA」)、タブレット、モバイルコンピュータ、ラップトップコンピュータ、エンターテインメントデバイス(たとえば、音楽デバイスもしくはビデオデバイス)、ヘッドセット(たとえば、ヘッドフォン、イヤピースなど)、医療デバイス(たとえば、生体センサ、心拍数モニタ、歩数計、EKGデバイスなど)、ユーザI/Oデバイス、コンピュータ、有線コンピュータ、固定コンピュータ、デスクトップコンピュータ、サーバ、店頭デバイス、セットトップボックス、または任意の他の適切なデバイスに組み込まれる場合がある。これらのデバイスは、異なる電力要件およびデータ要件を有する場合がある。

【００２５】

いくつかの態様では、ワイヤレスデバイスは、通信システムのためのアクセスデバイス(たとえばWi-Fiアクセスポイント)を含む場合がある。そのようなアクセスデバイスは、たとえば、有線またはワイヤレスの通信リンクを介しての別のネットワーク(たとえば、インターネットまたはセルラーネットワークなどのワイドエリアネットワーク)への接続を提供することができる。したがって、アクセスデバイスは、別のデバイス(たとえばWiFi局)が他のネットワークまたは何らかの他の機能にアクセスできるようにする場合がある。

【００２６】

様々な異なる技術および技法のいずれかを使用して情報および信号が表現される場合があることを当業者は理解されよう。たとえば上の説明全体を通して参照される場合があるデータ、命令、コマンド、情報、信号、ビット、記号およびチップは、電圧、電流、電磁波、磁場または磁性粒子、光場または光学粒子、あるいはそれらの任意の組合せによって表される場合がある。

【００２７】

本明細書において開示される実施形態に関連して説明される種々の例示的な論理ブロック、モジュール、回路、およびアルゴリズムステップは、電子ハードウェア、コンピュータソフトウェア、または両方の組合せとして実現される場合があることは、当業者はさらに理解されよう。ハードウェアとソフトウェアのこの互換性を明確に示すために、種々の例示的構成要素、ブロック、モジュール、回路、およびステップが、これまでその機能に関して一般的に説明されてきた。そのような機能が、ハードウェアとして実現されるか、ソフトウェアとして実現されるかは、特定の適用例およびシステム全体に課される設計制約によって決まる。当業者は、説明された機能を、特定の適用例ごとに様々なやり方で実施することができるが、そのような実施態様の決定は、本開示の範囲からの逸脱を引き起こすと解釈されるべきではない。

【００２８】

本明細書において開示される実施形態に関連して説明される種々の例示的な論理ブロック、モジュールおよび回路は、汎用プロセッサ、デジタルシグナルプロセッサ(DSP)、特定用途用集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)もしくは他のプログラマブル論理デバイス、個別のゲートもしくはトランジスタロジック、個別のハードウェア構成要素、または本明細書において説明された機能を果たすように設計されたこれらの任意の組合せを用いて、実現されるか、または実行される場合がある。汎用プロセッサはマイクロプロセッサとすることができるが、代替形態では、プロセッサは、任意の従来のプロセッサ、コントローラ、マイクロコントローラ、またはステートマシンとすることができる。プロセッサは、コンピューティングデバイスの組合せ、たとえばDSPとマイクロプロセッサの組合せ、複数のマイクロプロセッサ、DSPコアと連結した1つもしくは複数のマイクロプロセッサ、または任意の他のそのような構成として実現することができる。

【００２９】

本明細書において開示される実施形態との関連において説明された方法またはアルゴリ

ズムのステップは、ハードウェアにおいて直接に、または、プロセッサによって実行されるソフトウェアモジュールにおいて、またはこの2つの組合せにおいて具現化される場合がある。ソフトウェアモジュールは、RAMメモリ、フラッシュメモリ、ROMメモリ、EPROMメモリ、EEPROMメモリ、レジスタ、ハードディスク、リムーバブルディスク、CD-ROM、または当技術分野において知られている任意のその他の形の記憶媒体内に存在することができる。例示的な記憶媒体は、プロセッサが記憶媒体から情報を読み出し、かつ、記憶媒体に情報を書き込むことができるようにプロセッサに結合される。代替形態では、記憶媒体はプロセッサと一体にすることができる。プロセッサおよび記憶媒体はASIC内に存在する場合がある。ASICは、ユーザ端末内に存在する場合がある。代替形態では、プロセッサおよび記憶媒体は、ユーザ端末内の個別の構成要素として存在する場合がある。

【００３０】

1つまたは複数の例示的な実施形態では、説明された機能が、ハードウェア、ソフトウェア、ファームウェア、またはそれらの任意の組合せの形で実現することができる。コンピュータプログラム製品としてソフトウェアにおいて実現される場合、機能は、1つまたは複数の命令またはコードとして、コンピュータ可読媒体上に記憶することができるか、またはコンピュータ可読媒体を介して送信することができる。コンピュータ可読媒体は、ある場所から別の場所へのコンピュータプログラムの転送を容易にする任意の媒体を含む、コンピュータ記憶媒体と通信媒体との両方を含む。記憶媒体は、コンピュータによってアクセス可能である任意の入手可能な媒体とすることができる。限定ではなく例として、そのようなコンピュータ可読媒体は、RAM、ROM、EEPROM、CD-ROMもしくは他の光ディスク記憶装置、磁気ディスク記憶装置もしくは他の磁気記憶デバイス、または命令もしくはデータ構造の形において所望のプログラムコードを搬送もしくは記憶するために使用することができ、コンピュータによってアクセスすることができる任意の他の媒体を含むことができる。また、あらゆる接続もコンピュータ可読媒体と適切に呼ばれる。たとえば、ソフトウェアが、同軸ケーブル、光ファイバケーブル、ツイストペア、デジタル加入者回線(DSL)、または赤外線、無線、およびマイクロ波などのワイヤレス技術を使用して、ウェブサイト、サーバ、または他のリモートソースから送信される場合、同軸ケーブル、光ファイバケーブル、ツイストペア、DSL、または赤外線、無線、およびマイクロ波などのワイヤレス技術は、媒体の定義に含まれる。ディスク(disk)およびディスク(disc)は、本明細書において使用されるときに、コンパクトディスク(disc)(CD)、レーザディスク(disc)、光ディスク(disc)、デジタル多用途ディスク(disc)(DVD)、フロッピーディスク(disk)およびブルーレイディスク(disc)を含み、ディスク(disk)は通常、データを磁気的に再生し、一方、ディスク(disc)は、レーザを用いてデータを光学的に再生する。上記の組合せもコンピュータ可読媒体の範囲の中に含まれるべきである。

【００３１】

開示された実施形態のこれまでの説明は、当業者が本発明を作製または使用できるようにするために提供される。これらの実施形態に対する種々の変更形態が、当業者には容易に理解され、本明細書において規定される一般原理は、本発明の趣旨または範囲から逸脱することなく他の実施形態に適用することができる。したがって、本発明は、本明細書において示される実施形態に限定されるものではなく、本明細書において開示される原理および新規の特徴に一致する最も広い範囲を与えられるべきである。

【符号の説明】

【００３２】

100 コンピューティングデバイス
105 バス
110 プロセッサ
112 通常モード
114 セキュアモード
115 入力デバイス
120 出力デバイス

121 ディスプレイデバイス
125 非一時的記憶デバイス
130 通信サブシステム
135 作業メモリ
137 セキュアメモリ
140 オペレーティングシステム
145 アプリケーション
310 信頼ゾーン
312 セキュアブートローダ
320 セキュアオーセンティケータ
325 最初のブートアップ
325 シリアル番号
327 固有ダイジェスト
330 固有ダイジェストエントリ
340 認証される
342 認証されない
400 プロセス
402 アプリケーション
404 ヘッダ
410 セキュアハッシュアルゴリズム
415 計算されたアプリケーションダイジェスト
450 認証される
455 認証されない

【図１】

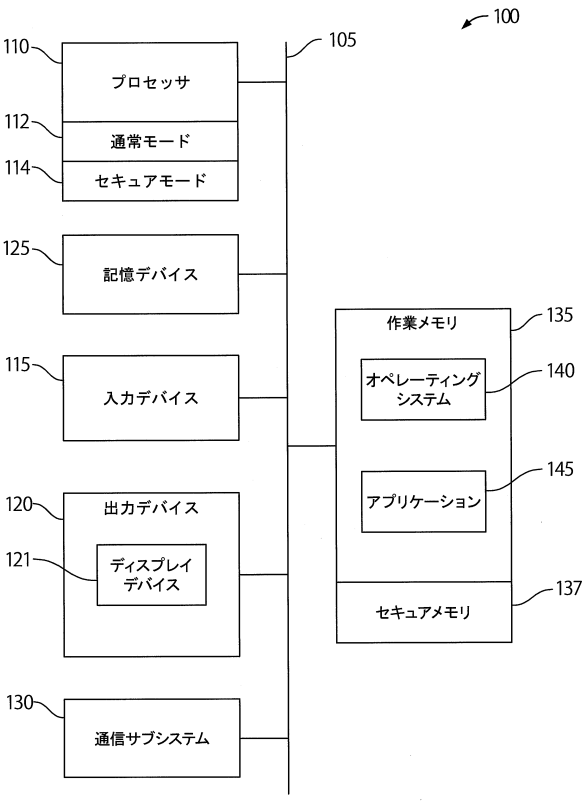

FIG.1

【図２】

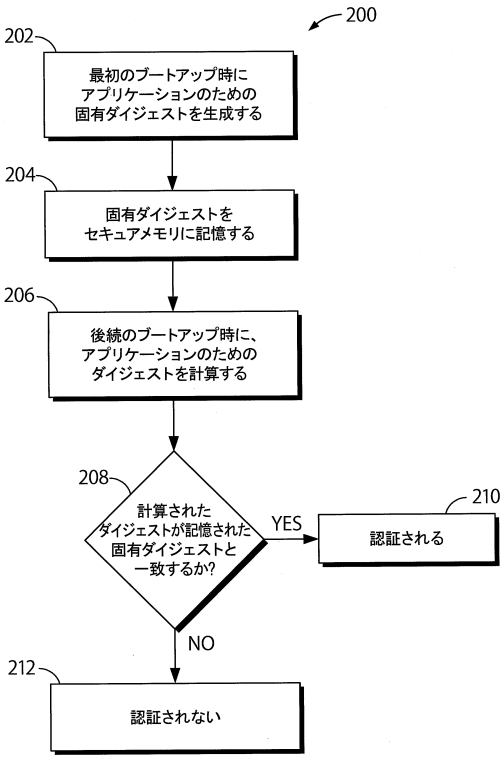

FIG.2

【図３】

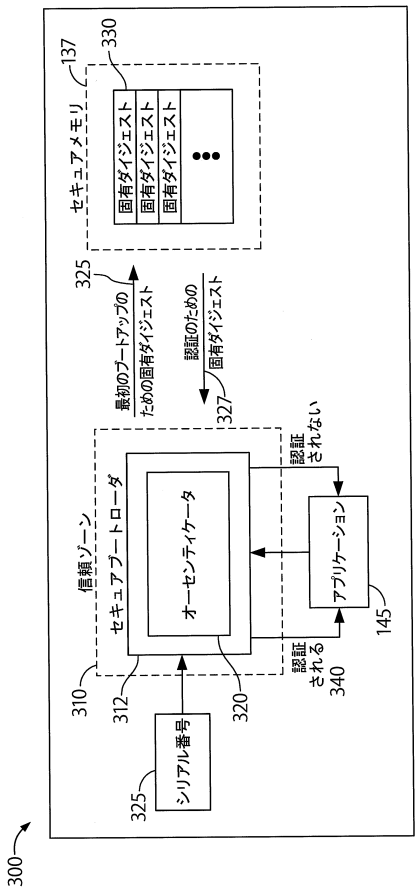

FIG.3

【図４】

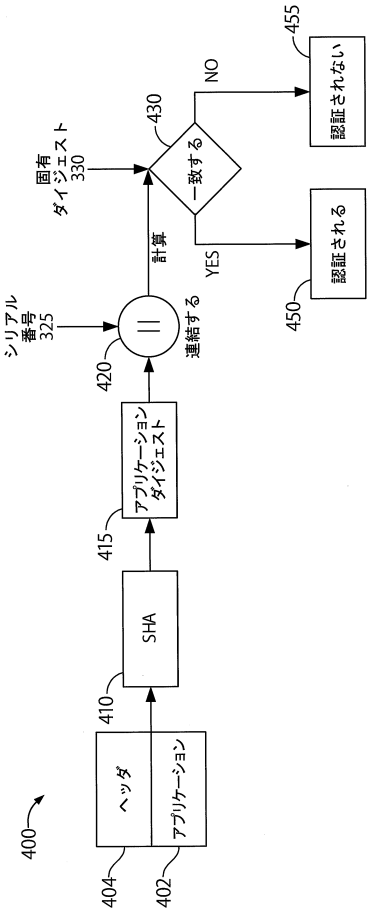

FIG.4

フロントページの続き

(72)発明者　カジ・ワイ・バシール
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　スレシュ・ボラプラガダ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

審査官　青木　重徳

(56)参考文献　特開２０１３－０４６１２２（ＪＰ，Ａ）
特表２００９－５３３７４２（ＪＰ，Ａ）
米国特許出願公開第２０１０／０２９３６１４（ＵＳ，Ａ１）
米国特許出願公開第２００８／０１２６７７９（ＵＳ，Ａ１）
米国特許第０５９４４８２１（ＵＳ，Ａ）
欧州特許出願公開第２３６９５１８（ＥＰ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４４
Ｇ０６Ｆ　２１／１２
Ｈ０４Ｌ　９／３２