(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2015-522199
(P2015-522199A)
(43)公表日　平成27年8月3日(2015.8.3)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/71	(2013.01)	G06F 21/71		5B376
G06F 9/445	(2006.01)	G06F 9/06	610A	

審査請求 未請求　予備審査請求 未請求　（全 22 頁）

(21)出願番号	特願2015-521757 (P2015-521757)
(86)(22)出願日	平成25年7月9日 (2013.7.9)
(85)翻訳文提出日	平成27年3月6日 (2015.3.6)
(86)国際出願番号	PCT/US2013/049795
(87)国際公開番号	WO2014/011687
(87)国際公開日	平成26年1月16日 (2014.1.16)
(31)優先権主張番号	61/671,290
(32)優先日	平成24年7月13日 (2012.7.13)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	13/931,708
(32)優先日	平成25年6月28日 (2013.6.28)
(33)優先権主張国	米国 (US)

(71)出願人　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100158805
弁理士　井関　守三
(74)代理人　100194814
弁理士　奥村　元宏

最終頁に続く

(54)【発明の名称】システムオンチップ上にセキュアエレメントコンポーネントの一部分を統合するための方法および装置

(57)【要約】
無線通信のための方法、装置、およびコンピュータプログラム製品が、効率的なＳＥ機能を提供することと関連して提供される。１つの例では、通信デバイスは、プロセッサ、ＲＡＭ、およびＮＶＭと、セキュアなコンポーネントと、非セキュアなコンポーネントとを含むＳＥを含む。ＳＥは、ＳＥに格納された情報を通じてアクセス可能な機能にアクセスするための要求を受信し、セキュアなコンポーネントに格納された、機能と関連づけられた情報の第１の部分を取り出し、非セキュアなコンポーネントに格納された、機能と関連づけられた情報の第２の部分を取得し、情報の第２の取得された部分へのアクセスを可能にするために、情報の第１の取り出された部分を使用して、機能へのアクセスを容易にするように装備されうる。一態様では、セキュアなコンポーネントは、プロセッサおよびＲＡＭを含むことができ、非セキュアなコンポーネントは、実質的にすべてのＮＶＭを含むことができる。

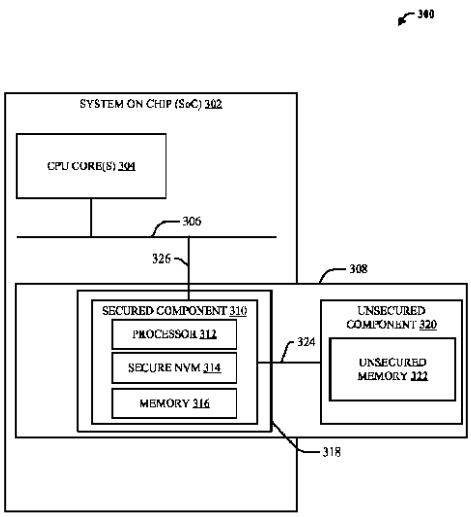

FIG. 3

【特許請求の範囲】
【請求項１】
通信のための装置であって、
プロセッサと、ランダムアクセスメモリ（ＲＡＭ）と、不揮発性メモリ（ＮＶＭ）とを備えるセキュアエレメント（ＳＥ）を備え、ここにおいて、前記ＳＥは、前記ＳＥのセキュアなコンポーネントと、前記ＳＥの非セキュアなコンポーネントとをさらに備え、前記非セキュアなコンポーネントと前記セキュアなコンポーネントは、インタフェースを通じて結合され、前記ＳＥは、
前記ＳＥに格納された情報を通じてアクセス可能な機能にアクセスするための要求を受信し、
前記ＳＥの前記セキュアなコンポーネントに格納された、前記機能と関連づけられた前記情報の第１の部分を取り出し、ここにおいて、前記セキュアなコンポーネントは、前記プロセッサおよび前記ＲＡＭを備える、
前記ＳＥの前記非セキュアなコンポーネントに格納された、前記機能と関連づけられた前記情報の第２の部分を取得し、ここにおいて、前記非セキュアなコンポーネントは、実質的にすべての前記ＮＶＭを備える、
前記情報の前記第２の取得された部分へのアクセスを可能にするために、前記情報の前記第１の取り出された部分を使用して、前記機能へのアクセスを容易にする
ように構成される、装置。
【請求項２】
前記機能は、通信デバイス上に格納されたアプリケーションであり、前記要求は、前記ＳＥと前記通信デバイスの間の暗号的にセキュアなインタフェースを通じて受信される、請求項１に記載の装置。
【請求項３】
前記ＳＥの前記非セキュアなコンポーネント内に含まれる前記ＮＶＭは、標準ＮＶＭを備える、請求項１に記載の装置。
【請求項４】
前記ＳＥの前記セキュアなコンポーネントは、セキュリティシールディングを使用してセキュアにされる、請求項１に記載の装置。
【請求項５】
前記ＳＥの前記セキュアなコンポーネントは、システムオンチップ（ＳｏＣ）に統合される、請求項１に記載の装置。
【請求項６】
前記ＳｏＣは、近距離無線通信コントローラ（ＮＦＣＣ）である、請求項５に記載の装置。
【請求項７】
前記ＳｏＣは、移動局モデム（ＭＳＭ）チップである、請求項５に記載の装置。
【請求項８】
前記ＳｏＣ上の前記ＳＥのフットプリントは、前記ＳｏＣに前記ＳＥの前記セキュアなコンポーネントのみを統合することによって最小化される、請求項５に記載の装置。
【請求項９】
前記ＳＥの前記セキュアなコンポーネントは、６５ｎｍ以下の形状を有する、請求項８に記載の装置。
【請求項１０】
前記セキュアなコンポーネントのためのセキュリティシールディングは、前記ＳｏＣと関連づけられた１つまたは複数の既存の金属層を含む、請求項５に記載の装置。
【請求項１１】
前記ＳＥは、前記ＳＥの前記非セキュアなコンポーネントと前記ＳＥの前記セキュアなコンポーネントの間の高速インタフェースを使用するようにさらに構成される、請求項１に記載の装置。

【請求項１２】
前記ＳＥの前記非セキュアなコンポーネントに格納された、前記機能と関連づけられた前記情報の前記第２の部分は、前記セキュアなコンポーネントに格納された、前記機能と関連づけられた前記情報の前記第１の部分に基づいて、暗号化されたフォーマットで格納される、請求項１に記載の装置。
【請求項１３】
前記ＳＥは、前記情報の前記第１の部分に含まれる１つまたは複数の暗号に基づいて、前記ＳＥの前記セキュアなコンポーネントに含まれる前記プロセッサを使用して、前記情報の前記第２の部分を解読するようにさらに構成される、請求項１２に記載の装置。
【請求項１４】
セキュアエレメント（ＳＥ）を使用する通信の方法であって、
前記ＳＥに格納された情報を通じてアクセス可能な機能にアクセスするための要求を受信することと、ここにおいて、前記ＳＥは、プロセッサと、ランダムアクセスメモリ（ＲＡＭ）と、不揮発性メモリ（ＮＶＭ）とを備える、
前記ＳＥのセキュアなコンポーネントに格納された、前記機能と関連づけられた前記情報の第１の部分を取り出すことと、ここにおいて、前記セキュアなコンポーネントは、前記プロセッサおよび前記ＲＡＭを備える、
前記ＳＥの非セキュアなコンポーネントに格納された、前記機能と関連づけられた前記情報の第２の部分を取得することと、ここにおいて、前記非セキュアなコンポーネントは、実質的にすべての前記ＮＶＭを備える、
前記情報の前記第２の取得された部分へのアクセスを可能にするために、前記情報の前記第１の取り出された部分を使用して、前記機能へのアクセスを容易にすることと
を備える方法。
【請求項１５】
前記機能は、通信デバイス上に格納されたアプリケーションであり、前記要求は、前記ＳＥと前記通信デバイスの間の暗号的にセキュアなインタフェースを通じて受信される、請求項１４に記載の方法。
【請求項１６】
前記ＳＥの前記非セキュアなコンポーネント内に含まれる前記ＮＶＭは、標準ＮＶＭを備える、請求項１４に記載の方法。
【請求項１７】
前記ＳＥの前記セキュアなコンポーネントは、セキュリティシールディングを使用してセキュアにされる、請求項１４に記載の方法。
【請求項１８】
前記ＳＥの前記セキュアなコンポーネントは、システムオンチップ（ＳｏＣ）に統合される、請求項１４に記載の方法。
【請求項１９】
前記ＳｏＣは、近距離無線通信コントローラ（ＮＦＣＣ）である、請求項１８に記載の方法。
【請求項２０】
前記ＳｏＣは、移動局モデム（ＭＳＭ）チップである、請求項１８に記載の方法。
【請求項２１】
前記ＳｏＣ上の前記ＳＥのフットプリントは、前記ＳｏＣに前記ＳＥの前記セキュアなコンポーネントのみを統合することによって最小化される、請求項１８に記載の方法。
【請求項２２】
前記ＳＥの前記セキュアなコンポーネントは、６５ｎｍ以下の形状を有する、請求項２１に記載の方法。
【請求項２３】
前記セキュアなコンポーネントのためのセキュリティシールディングは、前記ＳｏＣと関連づけられた１つまたは複数の既存の金属層を含む、請求項１８に記載の方法。

【請求項２４】
前記取得することは、前記ＳＥの前記非セキュアなコンポーネントと前記ＳＥの前記セキュアなコンポーネントの間の高速インタフェースを使用することを備える、請求項１４に記載の方法。
【請求項２５】
前記ＳＥの前記非セキュアなコンポーネントに格納された、前記機能と関連づけられた前記情報の前記第２の部分は、前記セキュアなコンポーネントに格納された、前記機能と関連づけられた前記情報の前記第１の部分に基づいて、暗号化されたフォーマットで格納される、請求項１４に記載の方法。
【請求項２６】
前記アクセスすることは、前記情報の前記第１の部分に含まれる１つまたは複数の暗号に基づいて、前記ＳＥの前記セキュアなコンポーネントに含まれる前記プロセッサによって、前記情報の前記第２の部分を解読することをさらに備える、請求項２５に記載の方法。
【請求項２７】
通信のための装置であって、
セキュアエレメント（ＳＥ）に格納された情報を通じてアクセス可能な機能にアクセスするための要求を受信するための手段と、ここにおいて、前記ＳＥは、プロセッサと、ランダムアクセスメモリ（ＲＡＭ）と、不揮発性メモリ（ＮＶＭ）とを備える、
前記ＳＥのセキュアなコンポーネントに格納された、前記機能と関連づけられた前記情報の第１の部分を取り出すための手段と、ここにおいて、前記セキュアなコンポーネントは、前記プロセッサおよび前記ＲＡＭを備える、
前記ＳＥの非セキュアなコンポーネントに格納された、前記機能と関連づけられた前記情報の第２の部分を取得するための手段と、ここにおいて、前記非セキュアなコンポーネントは、実質的にすべての前記ＮＶＭを備える、
前記情報の前記第２の取得された部分へのアクセスを可能にするために、前記情報の前記第１の取り出された部分を使用して、前記機能へのアクセスを容易にための手段と
を備える装置。
【請求項２８】
前記機能は、通信デバイス上に格納されたアプリケーションであり、前記要求は、前記ＳＥと前記通信デバイスの間の暗号的にセキュアなインタフェースを通じて受信される、請求項２７に記載の装置。
【請求項２９】
前記ＳＥの前記非セキュアなコンポーネント内に含まれる前記ＮＶＭは、標準ＮＶＭを備える、請求項２７に記載の装置。
【請求項３０】
前記ＳＥの前記セキュアなコンポーネントは、セキュリティシールディングを使用してセキュアにされる、請求項２７に記載の装置。
【請求項３１】
前記ＳＥの前記セキュアなコンポーネントは、システムオンチップ（ＳｏＣ）に統合される、請求項２７に記載の装置。
【請求項３２】
前記ＳｏＣは、近距離無線通信コントローラ（ＮＦＣＣ）である、請求項３１に記載の装置。
【請求項３３】
前記ＳｏＣは、移動局モデム（ＭＳＭ）チップである、請求項３１に記載の装置。
【請求項３４】
前記ＳｏＣ上の前記ＳＥのフットプリントは、前記ＳｏＣに前記ＳＥの前記セキュアなコンポーネントのみを統合することによって最小化される、請求項３１に記載の装置。
【請求項３５】

前記ＳＥの前記セキュアなコンポーネントは、６５ｎｍ以下の形状を有する、請求項３４に記載の装置。

【請求項３６】

前記セキュアなコンポーネントのためのセキュリティシールディングは、前記ＳｏＣと関連づけられた１つまたは複数の既存の金属層を含む、請求項３１に記載の装置。

【請求項３７】

前記取得するための手段は、前記ＳＥの前記非セキュアなコンポーネントと前記ＳＥの前記セキュアなコンポーネントの間の高速インタフェースを使用するようにさらに構成される、請求項３６に記載の装置。

【請求項３８】

前記ＳＥの前記非セキュアなコンポーネントに格納された、前記機能と関連づけられた前記情報の前記第２の部分は、前記セキュアなコンポーネントに格納された、前記機能と関連づけられた前記情報の前記第１の部分に基づいて、暗号化されたフォーマットで格納される、請求項２７に記載の装置。

【請求項３９】

前記アクセスを容易にするための手段は、前記情報の前記第１の部分に含まれる１つまたは複数の暗号に基づいて、前記情報の前記第２の部分を解読するようにさらに構成される、請求項３８に記載の装置。

【請求項４０】

コンピュータプログラム製品であって、

前記ＳＥに格納された情報を通じてアクセス可能な機能にアクセスするための要求を受信することと、ここにおいて、前記ＳＥは、プロセッサと、ランダムアクセスメモリ（ＲＡＭ）と、不揮発性メモリ（ＮＶＭ）とを備える、

前記ＳＥのセキュアなコンポーネントに格納された、前記機能と関連づけられた前記情報の第１の部分を取り出すことと、ここにおいて、前記セキュアなコンポーネントは、前記プロセッサおよび前記ＲＡＭを備える、

前記ＳＥの非セキュアなコンポーネントに格納された、前記機能と関連づけられた前記情報の第２の部分を取得することと、ここにおいて、前記非セキュアなコンポーネントは、実質的にすべての前記ＮＶＭを備える、

前記情報の前記第２の取得された部分へのアクセスを可能にするために、前記情報の前記第１の取り出された部分を使用して、前記機能へのアクセスを容易にすることと

のためのコードを備えるコンピュータ可読媒体、

を備えるコンピュータプログラム製品。

【発明の詳細な説明】

【米国特許法第１１９条に基づく優先権の主張】

【０００１】

本特許出願は、本譲受人にその権利が譲渡され、ここに参照により明確に組み込まれる、２０１２年７月１３日に出願された、「システムオンチップ上にセキュアエレメントコンポーネントの一部分を統合するための方法および装置（“METHODS AND APPARATUSES FOR INTEGRATING A PORTION OF SECURE ELEMENT COMPONENTS ON A SYSTEM ON CHIP”）」と題された仮特許出願第６１／６７１，２９０号の優先権を主張する。

【技術分野】

【０００２】

[0001] 開示される態様は、一般的には、デバイス間および／またはデバイス内の通信に関し、詳細には、セキュアエレメントの一部分がシステムオンチップ（ＳｏＣ）に統合される、セキュアエレメントを使用するための方法およびシステムに関する。

【背景技術】

【０００３】

[0002] 技術の進歩は、より小型で、より強力なパーソナルコンピューティングデバイスをもたらした。例えば、それぞれ小型で、軽く、かつユーザによって容易に持ち運ばれ

ることができる携帯用無線電話、携帯情報端末（ＰＤＡ）、およびページングデバイスなどの無線コンピューティングデバイスを含む様々な携帯用パーソナルコンピューティングデバイスが現在存在している。より具体的には、例えば、携帯用無線電話は、無線ネットワーク上で音声およびデータパケットを通信するセルラ電話をさらに含む。多くのこのようなセルラ電話は、コンピューティング能力における比較的大きな増大とともに製造され、したがって、小型のパーソナルコンピュータおよびハンドヘルドＰＤＡと同等になりつつある。さらに、このようなデバイスは、セルラ通信、無線ローカルエリアネットワーク（ＷＬＡＮ）通信、近距離無線通信（ＮＦＣ：near field communication）等のような、様々な周波数および適用可能なカバレッジエリアを使用する通信を可能にするように製造されている。

【０００４】

[0003] 現在、デバイス内では、いくつかのアプリケーションが、物理的な侵入および／またはソフトウェアの侵入に対する保護を含む、高いレベルのセキュリティを使用するように構成されうる。このようなアプリケーションは、セキュアエレメント（ＳＥ）においてホスト（hosted）されうる。ここで使用される場合、ＳＥは、不正アクセスから保護するために強化された（hardened）完全なコンピューティングプラットフォーム（例えば、ランダムアクセスメモリ（ＲＡＭ）、読取専用メモリ（ＲＯＭ）、不揮発性メモリ（ＮＶＭ）、暗号化アクセラレータ（cryptographic accelerators）、中央処理装置（ＣＰＵ）等）を含みうる。これらのＳＥは、非常に高いレベルのセキュリティを達成しうる一方で、これらはまた、デバイスに統合される場合、比較的コストがかかりうる。例えば、ＳＥは、典型的に個別のシリコンプロセスを使用して作成され、したがって、統合されたＳｏＣ上で可能な費用便益から利益を得られないことがありうる。

【０００５】

[0004] したがって、効率的なＳＥ機能を提供するための改善された方法および装置が望ましくありうる。

【発明の概要】

【０００６】

[0005] 以下は、１つまたは複数の態様の基本的な理解を提供するために、そのような態様の簡略化された概要を示す。この概要は、企図されるすべての態様の広範な概観ではなく、また、すべての態様の主要または重要な要素を特定するようにも、任意またはすべての態様の範囲を定めるようにも意図されない。その唯一の目的は、後に示されるより詳細な説明への前置きとして、簡略化された形式で１つまたは複数の態様のいくつかの概念を示すことである。

【０００７】

[0006] １つまたは複数の態様およびその対応する開示に従って、様々な態様が、効率的なＳＥ機能を提供することに関連して説明される。１つの例では、通信デバイスは、プロセッサ、ＲＡＭ、およびＮＶＭと、セキュアなコンポーネントと、非セキュアな（unsecured）コンポーネントとを含むＳＥを含む。一態様では、非セキュアなコンポーネントとセキュアなコンポーネントは、インタフェースを通じて結合される。ＳＥは、ＳＥに格納された情報を通じてアクセス可能な機能にアクセスするための要求を受信し、ＳＥのセキュアなコンポーネントに格納された、機能と関連づけられた情報の第１の部分を取り出し、ＳＥの非セキュアなコンポーネントに格納された、機能と関連づけられた情報の第２の部分を取得し、情報の第２の取得された部分へのアクセスを可能にするために、情報の第１の取り出された部分を使用して、機能へのアクセスを容易にするように装備されうる。一態様では、セキュアなコンポーネントは、プロセッサおよびＲＡＭを含むことができ、非セキュアなコンポーネントは、実質的にすべてのＮＶＭを含むことができる。

【０００８】

[0007] 関連する態様によると、効率的なＳＥ機能を提供するための方法が提供される。この方法は、ＳＥに格納された情報を通じてアクセス可能な機能にアクセスするための要求を受信することを含みうる。一態様では、ＳＥは、プロセッサ、ＲＡＭ、およびＮＶ

Ｍを含みうる。さらに、この方法は、ＳＥのセキュアなコンポーネントに格納された、機能と関連づけられた情報の第１の部分を取り出すことを含みうる。一態様では、セキュアなコンポーネントは、プロセッサおよびＲＡＭを含みうる。さらに、この方法は、ＳＥの非セキュアなコンポーネントに格納された、機能と関連づけられた情報の第２の部分を取得することを含みうる。一態様では、非セキュアなコンポーネントは、実質的にすべてのＮＶＭを含みうる。さらに、この方法は、情報の第２の取得された部分へのアクセスを可能にするために、情報の第１の取り出された部分を使用して、機能へのアクセスを容易にすることを含みうる。

【０００９】

[0008] 別の態様が、効率的なＳＥ機能を提供することを可能にされた通信装置に関連する。この通信装置は、ＳＥに格納された情報を通じてアクセス可能な機能にアクセスするための要求を受信するための手段を含みうる。一態様では、ＳＥは、プロセッサ、ＲＡＭ、およびＮＶＭを含みうる。さらに、この通信装置は、ＳＥのセキュアなコンポーネントに格納された、機能と関連づけられた情報の第１の部分を取り出すための手段を含みうる。一態様では、セキュアなコンポーネントは、プロセッサおよびＲＡＭを含みうる。さらに、この通信装置は、ＳＥの非セキュアなコンポーネントに格納された、機能と関連づけられた情報の第２の部分を取得するための手段を含みうる。一態様では、非セキュアなコンポーネントは、実質的にすべてのＮＶＭを含みうる。さらに、この通信装置は、情報の第２の取得された部分へのアクセスを可能にするために、情報の第１の取り出された部分を使用して、機能へのアクセスを容易にするための手段を含みうる。

【００１０】

[0009] 別の態様が、通信装置に関連する。この装置は、プロセッサ、ＲＡＭ、およびＮＶＭと、ＳＥのセキュアなコンポーネントと、ＳＥの非セキュアなコンポーネントとを含むＳＥを含みうる。このＳＥは、ＳＥに格納された情報を通じてアクセス可能な機能にアクセスするための要求を受信するように構成されうる。さらに、このＳＥは、ＳＥのセキュアなコンポーネントに格納された、機能と関連づけられた情報の第１の部分を取り出すように構成されうる。一態様では、セキュアなコンポーネントは、プロセッサおよびＲＡＭを含みうる。さらに、このＳＥは、ＳＥの非セキュアなコンポーネントに格納された、機能と関連づけられた情報の第２の部分を取得するように構成されうる。一態様では、非セキュアなコンポーネントは、実質的にすべてのＮＶＭを含みうる。さらに、このＳＥは、情報の第２の取得された部分へのアクセスを可能にするために、情報の第１の取り出された部分を使用して、機能へのアクセスを容易にするように構成されうる。

【００１１】

[0010] なお別の態様が、コンピュータプログラム製品に関連し、これは、ＳＥに格納された情報を通じてアクセス可能な機能にアクセスするための要求を受信するためのコードを含むコンピュータ可読媒体を有しうる。一態様では、ＳＥは、プロセッサ、ＲＡＭ、およびＮＶＭを含みうる。さらに、このコンピュータ可読媒体は、ＳＥのセキュアなコンポーネントに格納された、機能と関連づけられた情報の第１の部分を取り出すためのコードを含みうる。一態様では、セキュアなコンポーネントは、プロセッサおよびＲＡＭを含みうる。さらに、このコンピュータ可読媒体は、ＳＥの非セキュアなコンポーネントに格納された、機能と関連づけられた情報の第２の部分を取得するためのコードを含みうる。一態様では、非セキュアなコンポーネントは、実質的にすべてのＮＶＭを含みうる。さらに、このコンピュータ可読媒体は、情報の第２の取得された部分へのアクセスを可能にするために、情報の第１の取り出された部分を使用して、機能へのアクセスを容易にするためのコードを含みうる。

【００１２】

[0011] 前述した目的および関連する目的を達成するために、１つまたは複数の態様は、以下に十分に説明され、かつ特許請求の範囲において具体的に示される特徴を備える。以下の説明および添付図面は、１つまたは複数の態様のある特定の例示的な特徴を詳細に記載する。しかしながら、これらの特徴は、様々な態様の原理が用いられうる様々な方法

のうちのほんの少数を示し、本説明は、すべてのこのような態様およびそれらの同等物を含むように意図される。

【図面の簡単な説明】

【００１３】

[0012] これら開示される態様は、開示される態様を限定するためでなく、例示するために提供される添付図面と併せて以下に説明され、ここで、同様の表記は同様の要素を示す。

【図１】図１は、一態様による、誘導ベース（induction based）の通信システムの簡略化されたブロック図である。

【図２】図２は、一態様による、誘導ベースのシステムの簡略化された概略図である。

【図３】図３は、一態様による、統合されたＳＥを備えたＳｏＣのブロック図である。

【図４】図４は、一態様による、ＳｏＣに統合されたＳＥを使用するための実例的な方法を説明するフローチャートである。

【図５】図５は、本開示による通信デバイスの態様のブロック図である。

【図６】図６は、一態様による、効率的なＳＥ機能を提供するための実例的な通信デバイスのブロック図を例示する。

【詳細な説明】

【００１４】

[0019] 様々な態様が、ここで図面を参照して説明される。以下の記述では、説明の目的で、多くの特定の詳細が、１つまたは複数の態様についての完全な理解を提供するために記載される。しかしながら、このような（複数を含む）態様は、これら特定の詳細なしで実現されうることが明らかでありうる。

【００１５】

[0020] 一般に、通信デバイスは、ＳＥの使用を通じて様々な機能にアクセスしうる。ＳＥは、典型的に不正アクセスから保護するために強化された、情報を格納するための環境を提供する。さらに、ＳＥは、それに限定されるものではないが、ＲＡＭ、ＲＯＭ、ＮＶメモリ（ＮＶＭ）、暗号化アクセラレータ、ＣＰＵ等のような、様々なコンポーネントを含みうる。ここに説明されるように、ＳＥのコンポーネントのうちの１つまたは複数が、分離されて、ＳｏＣに含まれる（例えば、統合される）ことができる、システムアーキテクチャが示される。したがって、統合されたおよびより低いコストのアーキテクチャを使用して、従来のモノリシックＳＥ設計と同等のセキュリティのレベルが達成されうる。

【００１６】

[0021] 図１は、本発明の様々な典型的な実施形態による、誘導ベースの通信システム１００を例示する。入力電力１０２は、エネルギー伝送（energy transfer）を提供するための放射界（radiated field）１０６を発生させるために送信機１０４に供給される。受信機１０８は、放射界１０６に結合し、出力電力１１０に結合されたデバイス（図示せず）によって蓄積または消費するための出力電力１１０を発生する。送信機１０４と受信機１０８の両方は、距離１１２だけ分離されている。１つの典型的な実施形態では、送信機１０４および受信機１０８は相互共振関係（mutual resonant relationship）に従って構成され、受信機１０８の共振周波数と送信機１０４の共振周波数とが非常に近い場合、受信機１０８が放射界１０６の「近距離場（near-field）」に位置するとき、送信機１０４と受信機１０８の間の伝送損失は最小になる。

【００１７】

[0022] 送信機１０４は、エネルギー送信のための手段を提供するための送信アンテナ１１４をさらに含み、受信機１０８は、エネルギー受信のための手段を提供するための受信アンテナ１１８をさらに含む。送信アンテナおよび受信アンテナは、それに関連づけられるアプリケーションおよびデバイスに従ってサイズ決定される。上述したように、効率的なエネルギー伝送は、エネルギーの大部分を電磁波で遠距離場に伝搬するのではなく、送信アンテナの近距離場におけるエネルギーの大部分を受信アンテナに結合することによって行われる。この近距離場にある場合、結合モードが、送信アンテナ１１４と受信アン

テナ１１８との間に生じうる。この近距離結合が行われうるアンテナ１１４および１１８の周りのエリアを、本明細書では結合モード領域と呼ぶ。

【００１８】

[0023] 図２は、近距離場誘導ベースの通信システムの簡略化された概略図を示す。送信機２０４は、発振器２２２と、電力増幅器２２４と、フィルタおよび整合回路２２６とを含む。発振器は、調整信号２２３に応答して調整されうる、所望の周波数で信号を発生するように構成される。発振器信号は、制御信号２２５に応答する増幅量で電力増幅器２２４によって増幅されうる。フィルタおよび整合回路２２６は、高調波または他の不要な周波数をフィルタ除去し、送信機２０４のインピーダンスを送信アンテナ２１４に整合させるために含まれうる。

【００１９】

[0024] 受信機２０８は、図２に示されるようにバッテリ２３６を充電するため、または受信機に結合されたデバイス（図示せず）に電力供給するために、ＤＣ電力出力を発生するための整流器およびスイッチング回路２３４と整合回路２３２とを含みうる。整合回路２３２は、受信機２０８のインピーダンスを受信アンテナ２１８に整合させるために含まれうる。受信機２０８および送信機２０４は、（例えば、Ｂｌｕｅｔｏｏｔｈ（登録商標）、Ｚｉｇｂｅｅ（登録商標）、セルラ等の）別個の通信チャネル２１９上で通信しうる。

【００２０】

[0025] 図３を参照すると、一態様によるＮＦＣシステムアーキテクチャ３００のブロック図が例示される。ＮＦＣシステムアーキテクチャ３００は、共有バス３０６の使用を通じて１つまたは複数のＣＰＵコア３０４のための処理を可能にするように構成されうるＳｏＣ ３０２を含みうる。一態様では、ＳｏＣ ３０２は、移動局モデム（ＭＳＭ）チップを表しうる。別の態様では、ＳｏＣ ３０２は、ＮＦＣコントローラ（ＮＦＣＣ）を表しうる。

【００２１】

[0026] ＮＦＣシステムアーキテクチャ３００は、ＳＥ ３０８をさらに含む。一態様では、ＳＥ ３０８は、加入者識別モジュール（ＳＩＭ）カード、セキュアデジタル（ＳＤ）カード、マイクロＳＤカード、および／または埋め込まれたＳＥ ３０８でありうる。ＳＥ ３０８は、セキュアなコンポーネント３１０および非セキュアなコンポーネント３２０を含みうる。セキュアなコンポーネント３１０および非セキュアなコンポーネントは、インタフェース３２４を通じて結合されうる。一態様では、インタフェース３２４は、暗号化をサポートするバスインタフェースを使用するように構成されうる。別の態様では、インタフェース３２４は、標準の高速インタフェースでありうる。このような態様では、インタフェース３２４は、処理のために、ＳＥ ３０８の非セキュアなメモリ３２２からセキュアなコンポーネント３１０へのコード、アプレット等の効率的なローディングを提供する。

【００２２】

[0027] セキュアなコンポーネント３１０は、プロセッサ３１２、セキュアＮＶＭ ３１４、およびメモリ３１６を含みうる。一態様では、プロセッサ３１２は、ＳＥ ３０８と関連づけられた専用プロセッサ３１２でありうる。別の態様では、プロセッサ３１２は、ＳＥ ３０８内のセキュリティおよび保全性を維持することを支援するための追加のセキュリティ保護（例えば、暗号化、署名等）を有するＳｏＣ ３０２を通じて利用可能なプロセッサでありうる。一態様では、セキュアＮＶＭ ３１４は、保護から利益を得ることができる様々なアイテム（例えば、ルート鍵、証明書（certificates）等）を格納するために十分なメモリを含みうる。一態様では、メモリ３１６は、非セキュアなメモリ３２２に格納された情報の効率的なローディングおよび処理を可能するための十分な記憶能力を含みうる。

【００２３】

[0028] さらに、セキュアなコンポーネント３１０は、セキュリティシールディング（

security shielding）３１８を使用してセキュアにされうる。一態様では、セキュリティシールディング３１８は、ハードウェア攻撃および／またはソフトウェア攻撃（例えば、差分電力解析（ＤＰＡ）、単純電力解析（ＳＰＡ）、レーザー攻撃、電圧変化、温度変化、レーザー探査等）に対する様々な予防措置を提供しうる。セキュリティシールディング３１８の予防措置は、それに限定されるものではないが、内部動作の監視（observation）をより困難にするための金属層、パッケージが開かれた場合に動作を不能にする光センサ、同様の動作のための複数のハードウェアパス等を含みうる。一態様では、セキュリティシールディング３１８は、セキュリティシールディングの形態（forms）についてのデジタルまたはアナログＩＰをインプリメントするために、ＳｏＣ ３０２と関連づけられた既存の金属層を使用しうる。

【００２４】

[0029] 非セキュアなコンポーネント３２０は、非セキュアなメモリ３２２を含みうる。一態様では、非セキュアなメモリ３２２は、セキュア記憶装置、標準ＮＶＭ、ＲＡＭ、任意のメモリ記憶デバイス、またはこれらの任意の組み合わせを提供するタスクに特化されうる。一態様では、非セキュアなメモリ３２２は、約１．２Ｍバイトの空間で構成されうる。別の態様では、非セキュアなメモリ３２２は、ＳＥ ３０８を通じてアクセス可能な様々な機能と関連づけられるコード、アプレット等を格納するために使用されうる。このような態様では、非セキュアなメモリ３２２は、アプリケーション（例えば、コンピュータコード）およびデータの不揮発性記憶のために使用されることができ、セキュアＮＶＭ ３１４は、アプリケーションと関連づけられた鍵システムを格納するために使用されることができる。一態様では、外部インタフェースを介した攻撃に対してコードおよびデータのセキュリティおよび保全性を維持することを支援するために、データは、それがＳｏＣ ３０２を出るたびに、（セキュアにするために）暗号化され、（保全性を保証するために）署名されうる。したがって、非セキュアなメモリ３２２における情報は、セキュアなコンポーネント３１０内で使用される暗号化動作によって提供される能力の程度までセキュアでありうる。

【００２５】

[0030] 一動作態様（operational aspect）では、ＳＥ ３０８は、「コモンクライテリア（Common Criteria）」として知られるガイドラインのもとでセキュアであると認証されうる。これらのガイドラインは、その中でセキュリティが評価される、定義されるべき評価対象（ＴＯＥ：Target of Evaluation）を評価する。図３に図示されるように、セキュアなコンポーネント３１０と非セキュアなコンポーネント３２０とを含むＳＥ ３０８は、ＴＯＥとして評価されうる。言い換えれば、現在使用されているＴＯＥと適度に類似しうるＴＯＥを保持するために、セキュアなコンポーネント３１０とＳｏＣ ３０２の他のコンポーネントとの間のインタフェース３２６は、最小化されうる。このような態様では、インタフェース３２６は、ある特定のｅＦｕｓｅデータがＳＥ ３０８のみに利用可能であることを可能にするように構成されうる。別の態様では、インタフェース３２６は、ＳｏＣ ３０２の内部（ＲＡＭ）メモリに対して暗号的にセキュアであることができ、したがって、他のプロセッサ（例えば、ＳｏＣ ３０２におけるＣＰＵコア３０４）によるＳＥ ３０８の動作の監視を阻止する。別の態様では、セキュアなコンポーネント３１０は、ＳｏＣ ３０２上の他のコンポーネント（例えば、３０４）からの分離された電力領域および／または電力管理を使用しうる。なお別の態様では、セキュアなコンポーネント３１０は、例えば、バイナリ汎用非同期送受信回路（ＵＡＲＴ：universal asynchronous receiver/transmitter）インタフェースを使用して、他のプロセッサ（例えば、３０４）とのインタフェースを制約しうる。

【００２６】

[0031] したがって、ＳＥ ３０８の様々な機能が、ＳｏＣ ３０２上の小さなシリコン形状（geometries）で効率的にインプリメントされうるセキュアなコンポーネント３１０と、より大きくよりコストのかかる形状でより効率的にインプリメントされうる非セキュアなコンポーネント３２０とに分割されうる、ＮＦＣシステムアーキテクチャ３００が示

される。
【００２７】
[0032] 図４は、提示される主題事項の様々な態様による様々な手法（methodologies）を例示する。説明の簡略化の目的で、これら手法は、一連の動作またはシーケンスステップとして説明および示されるが、いくつかの動作は、ここに説明および示されるものとは異なる順序で生じ、および／または他の動作と同時並行に生じうるので、特許請求される主題事項は、動作の順序によって限定されないことが理解および認識されるべきである。例えば、当業者であれば、手法が、状態図でのような一連の相互関係がある状態またはイベントとして代替的に表されうることを理解および認識するであろう。さらに、特許請求される主題事項に従って手法をインプリメントするために、すべての例示される動作が必要とされるわけではない。加えて、以下および本明細書の全体にわたって開示される手法は、このような手法をコンピュータにトランスポートすることおよび伝送することを容易にするために、製造品上に記憶されることが可能であることが、さらに認識されるべきである。ここで使用される場合、製造品という用語は、任意のコンピュータ可読デバイス、キャリア、または媒体からアクセス可能なコンピュータプログラムを包含するように意図される。
【００２８】
[0033] ここで図４を参照すると、ＳｏＣと少なくとも部分的に統合されたＳＥを使用するためのプロセス４００を説明する実例的なフローチャートが例示される。一態様では、プロセス４００は、ＳＥ（例えば、ＳＥ ５６０）を含む通信デバイス（例えば、通信デバイス５００）によって実行されうる。
【００２９】
[0034] ブロック４０２において、ＳＥは、（例えば、アプリケーションのような）機能にアクセスするための要求を受信しうる。一態様では、この要求は、アプリケーションの起動、１つまたは複数のセンサから取得された測定値に応答して、別のデバイスから受信されたデータに応答して等で受信されうる。一態様では、この要求は、アプリケーションの起動、１つまたは複数のセンサから取得された測定値、別のデバイスから受信されたデータ等に応答して受信されうる。一態様では、この要求は、ＳＥと通信デバイスの間の暗号的にセキュアなインタフェースを通じて受信されうる。
【００３０】
[0035] ブロック４０４において、ＳＥは、ＳＥのセキュアなコンポーネントから機能と関連づけられた情報の一部分を取り出しうる。一態様では、この情報は、セキュアな方法で、要求された機能にアクセスすることと関連づけられた鍵、証明書等を含みうる。別の態様では、ＳＥのセキュアなコンポーネントは、それに限定されるものではないが、ＭＳＭチップ、ＮＦＣＣ等のようなＳｏＣに統合されうる。一態様では、ＳｏＣ上のＳＥのフットプリントは、ＳｏＣにＳＥのセキュアなコンポーネントのみを統合することによって最小化されうる。別の態様では、ＳＥのセキュアなコンポーネントは、６５ｎｍ以下の形状を有しうる。
【００３１】
[0036] ブロック４０６において、ＳＥは、ＳＥの非セキュアなコンポーネントにおける記憶装置から、機能と関連づけられた情報の一部分を取得しうる。一態様では、非セキュアなコンポーネントは、ＳＥを通じてアクセス可能な様々な機能と関連づけられるコード、アプレット等を格納しうる標準ＮＶＭを含みうる。別の態様では、情報の取り出された部分は、ＳＥのセキュアなコンポーネントに高速インタフェースを通じて通信されうる。このような態様では、取り出された部分は、ＳＥのセキュアなコンポーネントにおいて利用可能なメモリ内に配置されうる。一態様では、ＳＥの非セキュアなコンポーネントに格納された情報の部分は、セキュアなコンポーネントに格納された情報の部分に基づいて、暗号化されたフォーマットで格納されうる。
【００３２】
[0037] ブロック４０８において、ＳＥは、ＳＥのセキュアなコンポーネントからの情

報とＳＥの非セキュアなコンポーネントから取得された情報に基づいて、機能へのアクセスを容易にしうる。ＳＥの非セキュアなコンポーネントに格納された情報の部分が暗号化されたフォーマットで格納されうる態様では、アクセスを容易にすることは、情報を解読（decrypting）することを含みうる。

【００３３】

[0038] したがって、プロセス４００は、ＳｏＣに少なくとも部分的に統合されたＳＥを使用するための方法を提供する。

【００３４】

[0039] 図３を参照しながら、ここで図５も参照すると、通信デバイス５００の実例的なアーキテクチャが例示される。図５に図示されるように、通信デバイス５００は、例えば、受信アンテナ（図示せず）から信号を受信し、受信された信号に対して典型的な動作（例えば、フィルタ、増幅、ダウンコンバート等）を実行し、調整された信号をデジタル化してサンプルを得る受信機５０２を備える。受信機５０２は、受信されたシンボルを復調し、チャネル推定のためにプロセッサ５０６にそれらを供給しうる復調器５０４を備えうる。プロセッサ５０６は、受信機５０２によって受信された情報を分析すること、および／または、送信機５２０による送信のための情報を生成すること専用のプロセッサ、通信デバイス５００の１つまたは複数のコンポーネントを制御するプロセッサ、および／または、受信機５０２によって受信された情報を分析し、送信機５２０による送信のための情報を生成することと、通信デバイス５００の１つまたは複数のコンポーネントを制御することとの両方を行うプロセッサでありうる。さらに、信号は、プロセッサ５０６によって処理された信号を変調しうる変調器５１８を通じて、送信機５２０による送信のために準備されうる。

【００３５】

[0040] 通信デバイス５００は、プロセッサ５０６に動作可能に結合され、かつ、送信されるデータ、受信されたデータ、利用可能なチャネルに関する情報、ＴＣＰフロー、分析された信号および／または干渉強度と関連づけられたデータ、割り当てられたチャネルや電力やレート等に関する情報、および、チャネルを推定し、このチャネルを介して通信するためのその他任意の適切な情報を格納しうる、メモリ５０８を追加で備えうる。さらに、ＮＦＣシステムの制御を支援するように構成されうるプロセッサ５０６および／またはデバイスホスト５３４を備えうる。

【００３６】

[0041] 一態様では、プロセッサ５０６、ＮＦＣＣ ５３０、および／またはＳＥ ５６０は、ＳＥ ５６０に格納された情報を通じてアクセス可能な機能にアクセスするための要求を受信するための手段と、ＳＥ ５６０のセキュアなコンポーネント５６２に格納された、機能と関連づけられた情報の第１の部分を取り出すための手段と、ＳＥ ５６０の非セキュアなコンポーネント５６４に格納された、機能と関連づけられた情報の第２の部分を取得するための手段と、情報の第２の取得された部分へのアクセスを可能にするために、情報の第１の取り出された部分を使用して、機能へのアクセスを容易にするための手段とを提供しうる。一態様では、ＳＥ ５６０は、プロセッサ５０６、ＲＡＭ、およびＮＶＭを含みうる。一態様では、セキュアなコンポーネント５６２は、プロセッサおよびＲＡＭを含みうる。一態様では、非セキュアなコンポーネント５６４は、実質的にすべてのＮＶＭを含みうる。

【００３７】

[0042] ここに説明されるデータストア（例えば、メモリ５０８）は、揮発性メモリまたはＮＶＭのいずれかでありうるか、あるいは揮発性メモリとＮＶＭの両方を含みうることが認識されるであろう。限定ではなく例として、ＮＶＭは、読取専用メモリ（ＲＯＭ）、プログラマブルＲＯＭ（ＰＲＯＭ）、電気的プログラマブルＲＯＭ（ＥＰＲＯＭ）、電気的消去可能ＰＲＯＭ（ＥＥＰＲＯＭ）、またはフラッシュメモリを含みうる。揮発性メモリは、外部キャッシュメモリとして動作するランダムアクセスメモリ（ＲＡＭ）を含みうる。限定ではなく例として、ＲＡＭは、シンクロナスＲＡＭ（ＳＲＡＭ）、ダイナミッ

クＲＡＭ（ＤＲＡＭ）、シンクロナスＤＲＡＭ（ＳＤＲＡＭ）、ダブルデータレートＳＤＲＡＭ（ＤＤＲ ＳＤＲＡＭ）、エンハンストＳＤＲＡＭ（ＥＳＤＲＡＭ）、シンクリンクＤＲＡＭ（ＳＬＤＲＡＭ）、およびダイレクトラムバスＲＡＭ（ＤＲＲＡＭ）などの多くの形態で利用可能である。主題のシステムおよび方法のメモリ５０８は、それに限定されることなく、これらのタイプのメモリおよびその他任意の適切なタイプのメモリを備えうる。

【００３８】

[0043] 別の態様では、通信デバイス５００は、ＮＦＣコントローラインタフェース（ＮＣＩ）５５０を含みうる。１つの態様では、ＮＣＩ ５５０は、ＮＦＣ対応アンテナ（NFC enabled antenna）（例えば、５０２、５２０）とＮＦＣコントローラ５３０の間の通信を可能にするように動作可能でありうる。ＮＣＩ ５５０は、リスニング（listening）モードおよび／またはポーリング（polling）モードで機能するように設定可能でありうる。

【００３９】

[0044] 別の態様では、通信デバイス５００は、１つまたは複数のセキュアエレメント５６０を含みうる。１つの態様では、１つまたは複数のセキュアエレメント５６０は、ＮＦＣコントローラ５３０に結合されことができ、および／または、ＮＦＣコントローラ５３０内に少なくとも部分的に統合されることができる。１つの態様では、１つまたは複数のセキュアエレメント５６０は、ＭＳＭチップ（例えば、プロセッサ５０６）に結合されことができ、および／または、ＭＳＭチップ内に少なくとも部分的に統合されることができる。１つの態様では、１つまたは複数のセキュアエレメント５６０は、セキュアエレメントまたは近距離場コントローラ実行環境（ＮＦＣＥＥ）でありうる。１つの態様では、１つまたは複数のセキュアエレメント５６０は、それに限定されるものではないが、ＳＩＭ、ＣＳＩＭ等のような様々なモジュールを有するＵＩＣＣを含みうる。別の態様では、１つまたは複数のセキュアエレメント５６０は、図４で説明されたプロセスを実行するように構成されうる。

【００４０】

[0045] ＳＥ ５６０は、セキュアなコンポーネント５６２および非セキュアなコンポーネント５６４を含みうる。セキュアなコンポーネント５６２と非セキュアなコンポーネントは、インタフェースを通じて結合されうる。一態様では、このインタフェースは、暗号化をサポートするバスインタフェースを使用するように構成されうる。別の態様では、このインタフェースは、標準の高速インタフェースでありうる。このような態様では、このインタフェースは、処理のために、ＳＥ ５６０の非セキュアなメモリ３２２からセキュアなコンポーネント５６２へのコード、アプレット等の効率的なローディングを提供する。

【００４１】

[0046] セキュアなコンポーネント５６２は、セキュアメモリ５６８を含みうる。一態様では、セキュアメモリ５６８は、保護から利益を得ることができる様々なアイテム（例えば、ルート鍵、証明書等）を格納するために十分なメモリを含みうる。一態様では、セキュアメモリ５６８は、５～１０ｋビットの空間を含みうる。一態様では、セキュアメモリ５６８は、非セキュアなメモリ５６４に格納された情報の効率的なローディングおよび処理を可能にするための十分な格納能力を含みうる。

【００４２】

[0047] さらに、セキュアなコンポーネント５６２は、セキュリティシールディング５６６を使用してセキュアにされうる。一態様では、セキュリティシールディング５６６は、それに限定されるものではないが、内部動作の監視をより困難にするための金属層、パッケージが開かれた場合に動作を不能にする光センサ、同様の動作のための複数のハードウェアパス等のような、ハードウェアベースの攻撃に対する様々な予防措置を行いうる。一態様では、セキュリティシールディング５６６は、セキュリティシールディングの形態についてデジタルまたはアナログＩＰをインプリメントするために、ＳｏＣと関連づけら

れた既存の金属層を使用しうる。

【００４３】

[0048] 非セキュアなコンポーネント５６４は、非セキュアなメモリ５７０を含みうる。一態様では、非セキュアなメモリ５７０は、セキュア記憶装置、標準ＮＶＭ、またはこれらの任意の組み合わせを提供するタスクに特化されうる。一態様では、非セキュアなメモリ５７０は、約１．２Ｍバイトの空間で構成されうる。別の態様では、非セキュアなメモリ５７０は、ＳＥ ５６０を通じてアクセス可能な様々な機能と関連づけられるコード、アプレット等を格納するために使用されうる。このような態様では、非セキュアなメモリ５７０は、アプリケーション（例えば、コンピュータコード）およびデータの不揮発性記憶のために使用されることができ、セキュアメモリ５６８は、アプリケーションと関連づけられた鍵システムを格納するために使用されることができる。一態様では、外部インタフェースを介した攻撃に対してコードおよびデータのセキュリティおよび保全性を維持することを支援するために、データは、それがＳＥ ５６０を出るたびに、（セキュアにするために）暗号化され、（保全性を保証するために）署名されうる。したがって、非セキュアなメモリ５７０における情報は、セキュアなコンポーネント５６２内で使用される暗号化動作によって提供される能力の程度までセキュアでありうる。

【００４４】

[0049] 加えて、通信デバイス５００は、ユーザインタフェース５４０を含みうる。ユーザインタフェース５４０は、通信デバイス５００への入力を発生させるための入力メカニズム５４２と、通信デバイス５００のユーザによる消費のための情報を発生させるための出力メカニズム５４４とを含みうる。例えば、入力メカニズム５４２は、キーまたはキーボード、マウス、タッチスクリーンディスプレイ、マイクロフォン等のようなメカニズムを含みうる。さらに、例えば、出力メカニズム５４４は、ディスプレイ、オーディオスピーカ、触覚フィードバックメカニズム、パーソナルエリアネットワーク（ＰＡＮ）トランシーバ等を含みうる。例示される態様では、出力メカニズム５４４は、画像またはビデオのフォーマットのメディアコンテンツを示すように動作可能なディスプレイ、またはオーディオフォーマットのメディアコンテンツを示すためのオーディオスピーカを含みうる。

【００４５】

[0050] 図６は、通信デバイスに少なくとも部分的に統合されうるＳＥ ３０８との効率的な機能を容易にするように動作可能な実例的な通信システム６００のブロック図を図示する。例えば、通信システム６００は、通信デバイス（例えば、通信デバイス５００）の内部に少なくとも部分的に存在しうる。さらに、ＳＥ ３０８は、通信デバイス（例えば、通信デバイス５００）の内部に少なくとも部分的に存在しうる。システム６００は、プロセッサ、ソフトウェア、またはこれらの組み合わせ（例えば、ファームウェア）によってインプリメントされる機能を表す機能ブロックであることができる、機能ブロックを含むものとして表されていることを認識されたい。システム６００は、連携して動作しうる電気コンポーネントの論理グルーピング６０２を含む。

【００４６】

[0051] 例えば、論理グルーピング６０２は、ＳＥに格納された情報を通じてアクセス可能な機能にアクセスするための要求を受信するための手段を提供しうる電気コンポーネントを含みうる。例えば、受信するための手段は、ＳＥ ３０８のプロセッサ３１２およびセキュアなコンポーネント３１０、および／または通信デバイス５００のプロセッサ５０６を含みうる。

【００４７】

[0052] さらに、論理グルーピング６０２は、ＳＥのセキュアなコンポーネントに格納された、機能と関連づけられた情報の第１の部分を取り出すための手段を提供しうる電気コンポーネント６０６を含みうる。一態様では、セキュアなコンポーネントは、プロセッサおよびＲＡＭを含みうる。例えば、取り出すための手段６０６は、セキュアなコンポーネント３１０、セキュアＮＶＭ ３１４、および／またはＳＥ ３０８のプロセッサ３１２

を含みうる。

【００４８】

[0053] さらに、論理グルーピング６０２は、ＳＥの非セキュアなコンポーネントに格納された、機能と関連づけられた情報の第２の部分を取得するための手段を提供しうる電気コンポーネント６０８を含みうる。一態様では、非セキュアなコンポーネントは、実質的にすべてのＮＶＭを含みうる。例えば、取得するための手段６０８は、セキュアなコンポーネント３１０、非セキュアなコンポーネント３２０、セキュアＮＶＭ ３１４、非セキュアなメモリ３２２、および／またはＳＥ ３０８のプロセッサ３１２を含みうる。一態様では、取得するための手段６０８は、ＳＥの非セキュアなコンポーネントとＳＥのセキュアなコンポーネントの間の高速インタフェースを使用するように構成されうる。

【００４９】

[0054] さらに、論理グルーピング６０２は、情報の第２の取得された部分へのアクセスを可能にするために、情報の第１の取り出された部分を使用して、機能へのアクセスを容易にするための手段を提供しうる電気コンポーネント６１０を含みうる。一態様では、アクセスを容易にするための手段６１０は、セキュアなコンポーネント３１０、非セキュアなコンポーネント３２０、セキュアＮＶＭ ３１４、非セキュアなメモリ３２２、および／またはＳＥ ３０８のプロセッサ３１２を含みうる。

【００５０】

[0055] 任意の態様では、論理グルーピング６０２は、機能と関連づけられた情報を解読するための手段を提供しうる電気コンポーネント６１２を含みうる。例えば、解読するための手段６１２は、セキュアなコンポーネント３１０および／またはＳＥ ３０８のプロセッサ３１２を含みうる。

【００５１】

[0056] さらに、システム６００は、電気コンポーネント６０４、６０６、６０８、６１０、および６１２と関連づけられた機能を実行するための命令を保持し、かつ電気コンポーネント６０４、６０６、６０８、６１０、６１２等によって使用または取得されるデータを格納するメモリ６１４を含みうる。一態様では、メモリ６１４は、メモリ５０８を含むことができ、および／または、メモリ５０８内に含まれることができる。メモリ６１４の外部にあるように示されているが、電気コンポーネント６０４、６０６、６０８、６１０、および６１２のうちの１つ以上が、メモリ６１４の内部に存在しうることも理解されるべきである。１つの例では、電気コンポーネント６０４、６０４、６０６、６０８、６１０、および６１２は、少なくとも１つのプロセッサを含みうる、あるいは、各電気コンポーネント６０４、６０４、６０６、６０８、６１０、および６１２は、少なくとも１つのプロセッサの対応するモジュールでありうる。さらに、追加または代替の例では、電気コンポーネント６０４、６０６、６０８、６１０、および６１２は、コンピュータ可読媒体を含むコンピュータプログラム製品であることができ、ここで、各電気コンポーネント６０４、６０６、６０８、６１０、および６１２は、対応するコードであることができる。

【００５２】

[0057] 本願で使用される場合、「コンポーネント」、「モジュール」、「システム」等の用語は、それに限定されるものではないが、ハードウェア、ファームウェア、ハードウェアとソフトウェアの組み合わせ、ソフトウェア、または実行中のソフトウェアのような、コンピュータ関連エンティティを含むように意図される。例えば、コンポーネントは、それに限定されるものではないが、プロセッサで実行中のプロセス、プロセッサ、オブジェクト、プログラムとして実行可能なファイル（executable）、実行スレッド、プログラム、および／またはコンピュータでありうる。例として、コンピューティングデバイスで実行中のアプリケーションとコンピューティングデバイスの両方が、コンポーネントでありうる。１つまたは複数のコンポーネントが、プロセスおよび／または実行スレッド内に存在することができ、１つのコンポーネントが、１つのコンピュータでローカライズされることができ、および／または、２つ以上のコンピュータ間で分散されることができる

。加えて、これらのコンポーネントは、その上に記憶された様々なデータ構造を有する様々なコンピュータ可読媒体から実行されうる。これらコンポーネントは、信号を介して、ローカルシステム、分散システム内の別のコンポーネントと相互作用し、および／またはインターネットのようなネットワークを介して他のシステムと相互作用する１つのコンポーネントからのデータのような、１つまたは複数のデータパケットを有する信号に従うことなどによって、ローカルプロセスおよび／またはリモートプロセスを介して通信しうる。

【００５３】

[0058] さらに、本明細書では、様々な態様が、端末に関連して説明され、それは、有線端末または無線端末でありうる。端末はまた、システム、デバイス、加入者ユニット、加入者局、移動局、モバイル、モバイルデバイス、遠隔局、モバイル機器（ＭＥ）、遠隔端末、アクセス端末、ユーザ端末、端末、通信デバイス、ユーザエージェント、ユーザデバイス、またはユーザ機器（ＵＥ）と称されうる。無線端末は、セルラ電話、衛星電話、コードレス電話、セッション開始プロトコル（ＳＩＰ）電話、無線ローカルループ（ＷＬＬ）局、携帯情報端末（ＰＤＡ）、無線接続機能を有するハンドヘルドデバイス、コンピューティングデバイス、または、無線モデムに接続されたその他の処理デバイスでありうる。さらに、本明細書では、様々な態様が、基地局に関連して説明される。基地局は、（複数を含む）無線端末と通信するために利用されることができ、また、アクセスポイント、ノードＢ、またはいくつかのその他の用語で称されることもできる。

【００５４】

[0059] さらに、「または（“or”）」という用語は、排他的な「または」ではなく、包括的な「または」を意味するように意図される。すなわち、別段の規定がない限り、または文脈から明白でない限り、「ＸはＡまたはＢを使用する」という句は、自然な包括的置換のいずれかを意味するものとする。つまり、「ＸはＡまたはＢを使用する」という句は、ＸがＡを使用する場合、ＸがＢを使用する場合、またはＸがＡとＢの両方を使用する場合のいずれによっても満たされる。さらに、本願および添付の特許請求の範囲で使用される冠詞「ａ」および「ａｎ」は、別段の規定がない限り、または単数形を示すことが文脈から明白でない限り、概して「１つまたは複数」を意味するものと解釈されるべきである。

【００５５】

[0060] 本明細書で説明された技術は、ＣＤＭＡ、ＴＤＭＡ、ＦＤＭＡ、ＯＦＤＭＡ、ＳＣ－ＦＤＭＡおよび他のシステムなどの、様々な無線通信システムのために使用されうる。「システム」および「ネットワーク」という用語は、しばしば交換可能に用いられる。ＣＤＭＡシステムは、ユニバーサル地上無線アクセス（ＵＴＲＡ）、ｃｄｍａ２０００等のような無線技術をインプリメントしうる。ＵＴＲＡは、広帯域ＣＤＭＡ（Ｗ－ＣＤＭＡ）およびＣＤＭＡのその他の変形を含む。さらに、ｃｄｍａ２０００は、ＩＳ－２０００規格、ＩＳ－９５規格、およびＩＳ－８５６規格をカバーする。ＴＤＭＡシステムは、グローバル移動体通信システム（ＧＳＭ）（登録商標）のような無線技術をインプリメントしうる。ＯＦＤＭＡシステムは、発展型ＵＴＲＡ（Ｅ－ＵＴＲＡ）、ウルトラモバイルブロードバンド（ＵＭＢ）、ＩＥＥＥ ８０２．１１（Ｗｉ－Ｆｉ）、ＩＥＥＥ ８０２．１６（ＷｉＭＡＸ）、ＩＥＥＥ ８０２．２０、フラッシュ－ＯＦＤＭＡ等のような無線技術をインプリメントしうる。ＵＴＲＡおよびＥ－ＵＴＲＡは、ユニバーサルモバイルテレコミュニケーションシステム（ＵＭＴＳ）の一部である。３ＧＰＰロングタームエボリューション（ＬＴＥ）は、Ｅ－ＵＴＲＡを使用するＵＭＴＳのリリースであり、これは、ダウンリンク上でＯＦＤＭＡを使用し、アップリンク上でＳＣ－ＦＤＭＡを使用する。ＵＴＲＡ、Ｅ－ＵＴＲＡ、ＵＭＴＳ、ＬＴＥおよびＧＳＭは、「第３世代パートナシッププロジェクト」（３ＧＰＰ）と名付けられた機関からの文書に説明されている。さらに、ｃｄｍａ２０００およびＵＭＢは、「第３世代パートナシッププロジェクト２」（３ＧＰＰ２）と名付けられた機関からの文書に説明されている。さらに、このような無線通信システムは、対になっていない無認可スペクトル、８０２．ｘｘ無線ＬＡＮ、ＢＬＵＥＴＯＯ

ＴＨ（登録商標）、近距離無線通信（ＮＦＣ－Ａ、ＮＦＣ－Ｂ、ＮＦＣ－Ｆ等）、およびその他任意の短距離または長距離の無線通信技術をしばしば使用するピアツーピア（例えば、モバイルツーモバイル）アドホックネットワークシステムを追加で含みうる。

【００５６】

[0061] 様々な態様または特徴が、多数のデバイス、コンポーネント、モジュール等を含みうるシステムに関して示される。様々なシステムは、追加のデバイス、コンポーネント、モジュール等を含んでもよく、および／または図面に関連して説明されたすべてのデバイス、コンポーネント、モジュール等を含まなくてもよいことが理解および認識されるべきである。これらの手法の組み合わせも使用されうる。

【００５７】

[0062] ここで開示された態様に関連して説明された様々な例示的な論理、論理ブロック、モジュール、および回路は、汎用プロセッサ、デジタル信号プロセッサ（ＤＳＰ）、特定用途向け集積回路（ＡＳＩＣ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）またはその他のプログラマブル論理デバイス、ディスクリートゲートまたはトランジスタロジック、ディスクリートハードウェアコンポーネント、あるいはここに説明された機能を実行するように設計されたこれらの任意の組み合わせで、インプリメントまたは実行されうる。汎用プロセッサは、マイクロプロセッサでありうるが、代替において、このプロセッサは、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（state machine）でありうる。プロセッサはまた、例えば、ＤＳＰとマイクロプロセッサの組み合わせ、複数のマイクロプロセッサ、ＤＳＰコアと連携した１つまたは複数のマイクロプロセッサ、あるいはその他任意のこのような構成である、コンピューティングデバイスの組み合わせとしてインプリメントされうる。さらに、少なくとも１つのプロセッサは、上述されたステップおよび／または動作の１つまたは複数を実行するように動作可能な１つまたは複数のモジュールを含みうる。

【００５８】

[0063] さらに、ここに開示された態様に関連して説明された方法またはアルゴリズムのステップおよび／または動作は、直接ハードウェアで、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で、またはこれら２つの組み合わせで、具現化（embodied）されうる。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、リムーバルディスク、ＣＤ－ＲＯＭ、または当該技術分野において周知のその他任意の形状の記憶媒体内に存在しうる。実例的な記憶媒体は、プロセッサが記憶媒体から情報を読み取り、また、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うる。代替において、記憶媒体は、プロセッサと一体化されうる。さらに、いくつかの態様では、プロセッサおよび記憶媒体は、ＡＳＩＣ内に存在しうる。さらに、ＡＳＩＣは、ユーザ端末内に存在しうる。代替において、プロセッサおよび記憶媒体は、ユーザ端末内にディスクリートコンポーネントとして存在しうる。さらに、いくつかの態様では、方法またはアルゴリズムのステップおよび/または動作は、コンピュータプログラム製品に組み込まれうる、機械可読媒体および/またはコンピュータ可読媒体上のコードおよび/または命令の1つまたは任意の組み合わせ、あるいはそのセットとして存在しうる。

【００５９】

[0064] １つまたは複数の態様では、説明された機能は、ハードウェア、ソフトウェア、ファームウェア、またはこれらの任意の組み合わせでインプリメントされうる。ソフトウェアでインプリメントされる場合、これら機能は、コンピュータ可読媒体上で、１つまたは複数の命令またはコードとして送信または記憶されうる。コンピュータ可読媒体は、１つの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されうる任意の利用可能な媒体でありうる。限定ではなく例として、このようなコンピュータ可読媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、ＣＤ－ＲＯＭまたは他の光ディスク記憶装置、磁気ディスク記憶装置またはその他の磁気記憶デバイス、あるいは、デ

ータ構造または命令の形式で所望のプログラムコードを記憶または伝送するために使用可能であり、かつコンピュータによってアクセスされうるその他任意の媒体を備えうる。また、任意の接続も、コンピュータ可読媒体と称されうる。例えば、ソフトウェアが、同軸ケーブル、光ファイバーケーブル、ツイストペア、デジタル加入者回線（ＤＳＬ）、または赤外線、電波、およびマイクロ波のようなワイヤレス技術を使用して、ウェブサイト、サーバ、またはその他の遠隔ソースから送信される場合には、この同軸ケーブル、光ファイバーケーブル、ツイストペア、ＤＳＬ、または赤外線、電波、およびマイクロ波のような無線技術は、媒体の定義に含まれる。ここで使用される場合、ディスク（disk）およびディスク（disc）は、コンパクトディスク（ＣＤ）、レーザーディスク（登録商標）、光ディスク、デジタル多目的ディスク（ＤＶＤ）、フロッピー（登録商標）ディスクおよびブルーレイ（登録商標）ディスクを含み、ここでディスク（disks）は、通常磁気的にデータを再生し、一方ディスク（discs）は、通常レーザーを用いて光学的にデータを再生する。上記の組み合わせもまた、コンピュータ可読媒体の範囲内に含まれるべきである。

【００６０】

[0065] 上記の開示は、例示的な態様および/または態様を説明している一方で、説明された態様および／または添付の特許請求の範囲によって定義された態様の範囲から逸脱することなく、様々な変更および修正が本明細書で行われうることに留意されたい。さらに、説明された態様および/または態様の要素は、単数形で説明または特許請求されうるが、単数形に限定することが明記されていない限り、複数形が企図される。さらに、任意の態様および/または態様の全部または一部は、別段の規定がない限り、任意の他の態様および/または態様の全部または一部とともに利用されうる。

【図１】

図1

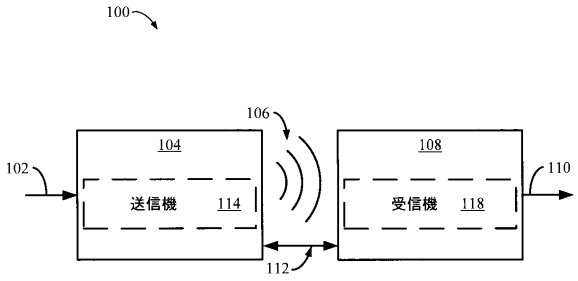

FIG. 1

【図２】

図2

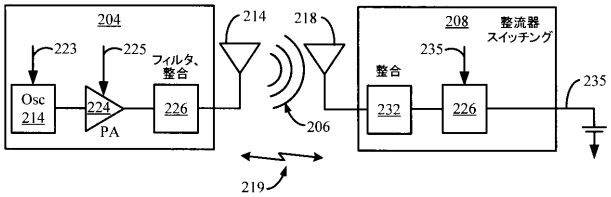

FIG. 2

【図３】

図３

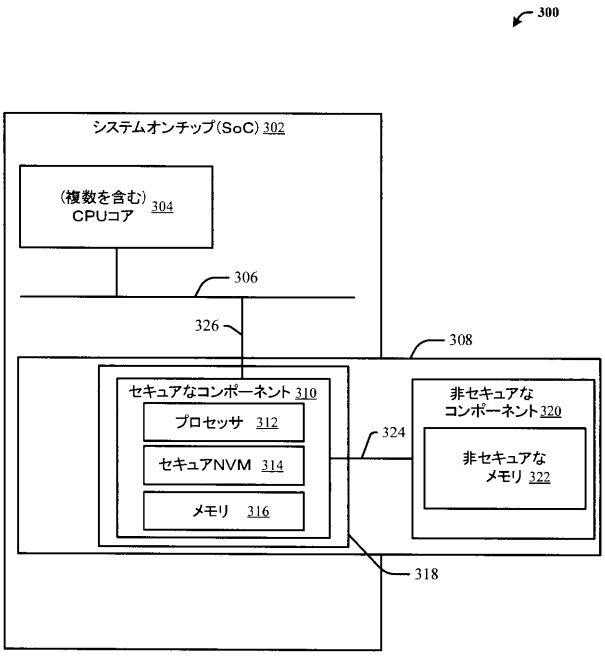

FIG. 3

【図４】

図４

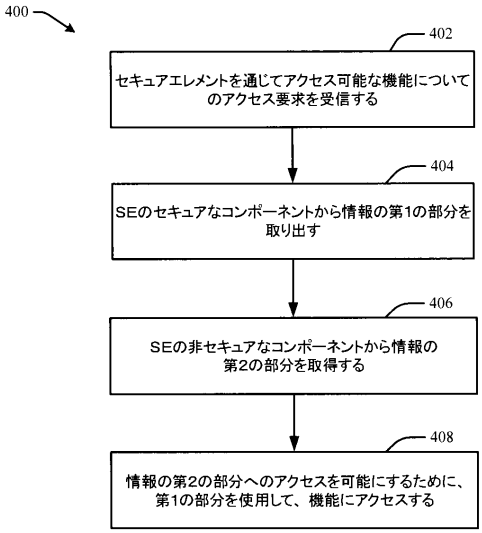

FIG. 4

【図５】

図５

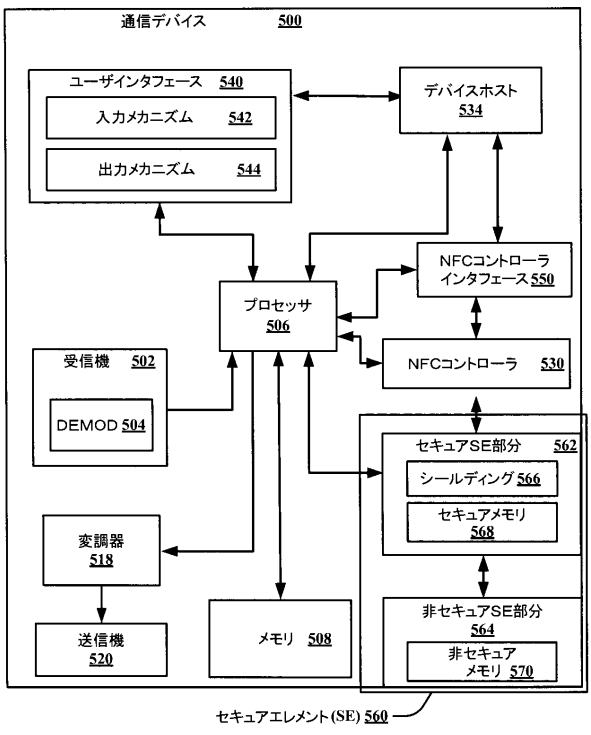

FIG. 5

【図６】

図６

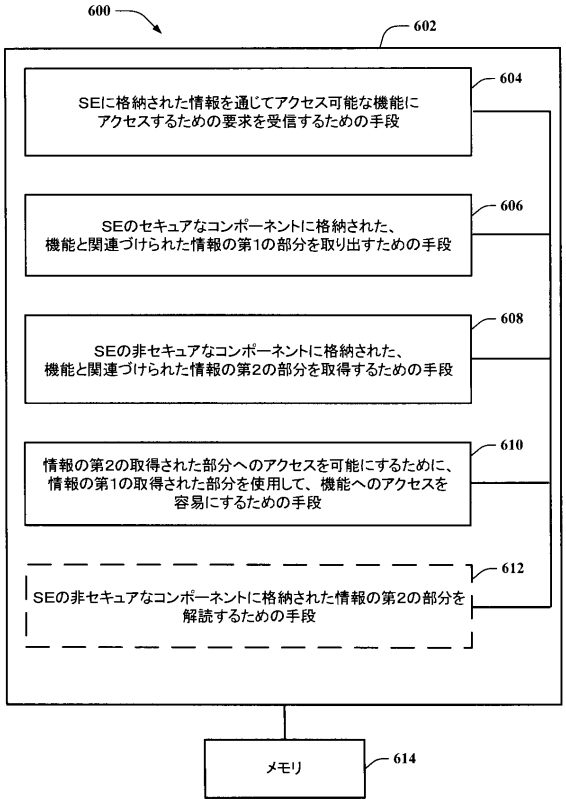

FIG. 6

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/049795

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/72 G06F21/87
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/030907 A1 (DARIEL DANI [IL]) 12 February 2004 (2004-02-12) the whole document -----	1-40
X	WO 2011/097482 A1 (MAXLINEAR INC [US]; LECLERCQ MAXIME [US]) 11 August 2011 (2011-08-11) paragraphs [0022] - [0030] figure 4 -----	1-40

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 September 2013	18/09/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Segura, Gustavo

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2013/049795

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004030907 A1	12-02-2004	AU 2003247146 A1	25-02-2004
		CN 1679273 A	05-10-2005
		CN 101950343 A	19-01-2011
		CN 102737180 A	17-10-2012
		JP 2005535958 A	24-11-2005
		US 2004030907 A1	12-02-2004
		US 2006112282 A1	25-05-2006
		WO 2004015740 A2	19-02-2004
WO 2011097482 A1	11-08-2011	US 2012036372 A1	09-02-2012
		WO 2011097482 A1	11-08-2011

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC

(72)発明者 バーティア、ネーラジ
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 オドノギュー、ジェレミー
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５

Ｆターム(参考) 5B376 AA01 AA10 AA21 AA31 GA03