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

特許第5519773号
(P5519773)

(45)発行日　平成26年6月11日(2014.6.11)　(24)登録日　平成26年4月11日(2014.4.11)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675A
H04L 9/10	(2006.01)	H04L	9/00	621Z
H04W 12/06	(2009.01)	H04W	12/06	

請求項の数 13　(全 24 頁)

(21)出願番号	特願2012-506218 (P2012-506218)
(86)(22)出願日	平成22年4月15日 (2010.4.15)
(65)公表番号	特表2012-524479 (P2012-524479A)
(43)公表日	平成24年10月11日 (2012.10.11)
(86)国際出願番号	PCT/US2010/031226
(87)国際公開番号	WO2010/121020
(87)国際公開日	平成22年10月21日 (2010.10.21)
審査請求日	平成23年12月19日 (2011.12.19)
(31)優先権主張番号	61/169,630
(32)優先日	平成21年4月15日 (2009.4.15)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	61/253,687
(32)優先日	平成21年10月21日 (2009.10.21)
(33)優先権主張国	米国 (US)

(73)特許権者　510030995
インターデイジタル　パテント　ホールディングス　インコーポレイテッド
アメリカ合衆国　１９８０９　デラウェア州　ウィルミントン　ベルビュー　パークウェイ　２００　スイート　３００
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所
(72)発明者　ヨゲンドラ　シー．シャー
アメリカ合衆国　１９３４１　ペンシルベニア州　エクストン　リージェンシー　コート　１０

最終頁に続く

(54)【発明の名称】ネットワークとの通信のためのデバイスの正当化および／または認証

(57)【特許請求の範囲】

【請求項１】

外部の通信エンティティにより認証される能力のあるデバイスであって、

暗号動作のために用いられる認証情報と、

前記認証情報を含む安全な記憶装置を具備する信頼済みコンポーネントと、

１組の不変的ハードウェア・リソースを具備する信頼の基盤と、

前記デバイスの前記動作に必須である少なくとも１つの必須コンポーネントと、

前記デバイスの少なくとも１つの必須ではないコンポーネントと、

を備え、

安全な起動の第１の段階の間、前記信頼の基盤が前記信頼済みコンポーネントの整合性を検証することを試み、前記信頼済みコンポーネントが前記信頼の基盤によって検証されないときに前記信頼の基盤が認証情報へのアクセスを阻止して前記安全な起動を停止し、前記信頼済みコンポーネントの前記整合性が前記信頼の基盤によって検証されたときに前記信頼の基盤が前記安全な起動の制御を前記信頼済みコンポーネントに渡し、

前記信頼済みコンポーネントの前記制御のもと前記安全な起動の第２の段階の間、前記信頼済みコンポーネントが前記少なくとも１つの必須コンポーネントの整合性を検証することを試み、前記少なくとも１つの必須コンポーネントが前記信頼済みコンポーネントによって検証されないときに前記信頼済みコンポーネントが認証情報へのアクセスを阻止して前記安全な起動を停止し、前記少なくとも１つの必須コンポーネントの前記整合性が前記信頼済みコンポーネントによって検証されたときに前記信頼済みコンポーネントが前記

安全な起動の第３の段階を始め、
前記信頼済みコンポーネントの前記制御のもと前記安全な起動の前記第３の段階の間、前記信頼済みコンポーネントが前記少なくとも１つの必須ではないコンポーネントの整合性を検証することを試み、前記少なくとも１つの必須ではないコンポーネントが前記信頼済みコンポーネントによって検証されないときに前記信頼済みコンポーネントは前記少なくとも１つの必須ではないコンポーネントが起動することを防ぎ、前記少なくとも１つの必須ではないコンポーネントが前記信頼済みコンポーネントによって検証されたときに前記信頼済みコンポーネントが前記少なくとも１つの必須ではないコンポーネントを起動する、
ことを特徴とするデバイス。

【請求項２】
前記必須コンポーネントはネットワーク通信モジュールを含むことを特徴とする請求項１に記載のデバイス。

【請求項３】
前記信頼の基盤は、前記信頼済みコンポーネントに関連付けられた信頼済み参照値を安全に格納することを特徴とする請求項１に記載のデバイス。

【請求項４】
前記信頼の基盤は、前記信頼済みコンポーネントの測定値を前記信頼済みコンポーネントに関連付けられた前記信頼済み参照値と比較するように構成され、前記信頼済みコンポーネントの前記測定値が前記信頼済みコンポーネントに関連付けられた前記信頼済み参照値に一致する場合、前記信頼済みコンポーネントの前記整合性が検証されることを特徴とする請求項３に記載のデバイス。

【請求項５】
信頼済みモードにおける動作の間、前記少なくとも１つの必須ではないコンポーネントが前記デバイスによって使用されることを特徴とする請求項１に記載のデバイス。

【請求項６】
前記安全な記憶装置は、前記少なくとも１つの必須ではないコンポーネントに関連付けられた信頼済み参照値をさらに格納することを特徴とする請求項１に記載のデバイス。

【請求項７】
前記信頼済みコンポーネントは、前記安全な記憶装置に格納された前記少なくとも１つの必須ではないコンポーネントに関連付けられた前記信頼済み参照値と前記少なくとも１つの必須ではないコンポーネントの測定値とを比較するように構成され、前記少なくとも１つの必須ではないコンポーネントの前記測定値が前記少なくとも１つの必須ではないコンポーネントに関連付けられた前記信頼済み参照値に一致するときに前記少なくとも１つの必須ではないコンポーネントの前記整合性が検証されることを特徴とする請求項６に記載のデバイス。

【請求項８】
前記信頼の基盤は、それに関連付けられた証明書を具備し、前記証明書は、第三者機関による前記信頼の基盤の整合性の検証を反映することを特徴とする請求項１に記載のデバイス。

【請求項９】
外部の通信エンティティにより認証される能力のあるデバイス中の１つまたは複数のコンポーネントを認証するための方法であって、前記デバイスは、暗号動作のために用いられる認証情報と、前記認証情報を含む安全な記憶装置を具備する信頼済みコンポーネントと、１組の不変的ハードウェア・リソースを有する信頼の基盤と、前記デバイスの前記動作に必須である少なくとも１つの必須コンポーネントと、前記デバイスの少なくとも１つの必須ではないコンポーネントと、を具備し、前記方法は、
安全な起動の第１の段階の間、前記信頼の基盤が前記信頼済みコンポーネントの整合性を検証することを試み、前記信頼済みコンポーネントが前記信頼の基盤によって検証されないときに前記信頼の基盤が認証情報へのアクセスを阻止して前記安全な起動を停止し、

前記信頼済みコンポーネントの前記整合性が前記信頼の基盤によって検証されたときに前記信頼の基盤が前記安全な起動の制御を前記信頼済みコンポーネントに渡す、ことと、

前記信頼済みコンポーネントの前記制御のもと前記安全な起動の第２の段階の間、前記信頼済みコンポーネントが前記少なくとも１つの必須コンポーネントの整合性を検証することを試み、前記少なくとも１つの必須コンポーネントが前記信頼済みコンポーネントによって検証されないときに前記信頼済みコンポーネントが認証情報へのアクセスを阻止して前記安全な起動を停止し、前記少なくとも１つの必須コンポーネントの前記整合性が前記信頼済みコンポーネントによって検証されたときに前記信頼済みコンポーネントが前記安全な起動の第３の段階を始める、ことと、

前記信頼済みコンポーネントの前記制御のもと前記安全な起動の前記第３の段階の間、前記信頼済みコンポーネントが前記少なくとも１つの必須ではないコンポーネントの整合性を検証することを試み、前記少なくとも１つの必須ではないコンポーネントが前記信頼済みコンポーネントによって検証されないときに前記信頼済みコンポーネントは前記少なくとも１つの必須ではないコンポーネントが起動することを防ぎ、前記少なくとも１つの必須ではないコンポーネントが前記信頼済みコンポーネントによって検証されたときに前記信頼済みコンポーネントが前記少なくとも１つの必須ではないコンポーネントを起動する、ことと、

を備えることを特徴とする方法。

【請求項１０】

前記信頼済みコンポーネントの前記整合性を検証する試みは、前記信頼済みコンポーネントの測定値を前記信頼済みコンポーネントに関連付けられた参照値と比較することを含み、前記信頼済みコンポーネントの前記測定値が前記信頼済みコンポーネントに関連付けられた前記信頼済み参照値に一致するときに、前記信頼済みコンポーネントの前記整合性が検証されることを特徴とする請求項９に記載の方法。

【請求項１１】

前記少なくとも１つの必須ではないコンポーネントの整合性を検証する試みは、前記少なくとも１つの必須ではないコンポーネントの測定値を前記少なくとも１つの必須ではないコンポーネントに関連付けられた参照値と比較することを含み、前記少なくとも１つの必須ではないコンポーネントの前記測定値が前記少なくとも１つの必須ではないコンポーネントに関連付けられた前記信頼済み参照値に一致したときに、前記少なくとも１つの必須ではないコンポーネントの前記整合性が検証されることを特徴とする請求項９に記載の方法。

【請求項１２】

前記信頼の基盤は、それに関連付けられた証明書を具備し、前記証明書は、第三者機関による前記信頼の基盤の整合性の検証を反映することを特徴とする請求項９に記載の方法。

【請求項１３】

前記外部の通信エンティティは、前記整合性の測定値が前記外部の通信エンティティにより予期される測定値に一致しない場合、前記デバイスへの少なくともあるアクセスを禁止するように構成されることを特徴とする請求項９に記載の方法。

【発明の詳細な説明】

【技術分野】

【０００１】

＜関連出願の相互参照＞

本出願は、２００９年１０月２１日に出願された米国仮特許出願番号第６１／２５３，６８７号、および２００９年４月１５日に出願された米国特許出願番号第６１／１６９，６３０号の優先権を主張し、ここにこの番号を参照することにより、その開示内容を本明細書の一部とする。

【背景技術】

【０００２】

現今では、携帯電話、フェムトセル（ｆｅｍｔｏｃｅｌｌ）、ホーム・ノード、ケーブル・モデム、ネットワーク・アクセス・ポイント、または同様のものなどのデバイスが通信ネットワークに接続することができる。その接続を介して、デバイスは通信ネットワークを使用して、通話を受信し、かつ／または発信し、インターネットまたは同様のものにアクセスすることができる。残念ながら、そのようなデバイスは例えばネットワークに接続する前に、デバイスにおいて含まれ得るコンポーネントの整合性（ｉｎｔｅｇｒｉｔｙ）を正当化（ｖａｌｉｄａｔｅ）するためのシステムまたは方法を含むことができない。

【発明の概要】

【０００３】

信頼済み（ｔｒｕｓｔｅｄ）コンピューティングを遂行するためのシステムおよび方法を提供することができる。例えば、コンピュータ・デバイス、移動体デバイス、フェムトセル、アクセス・ポイント基地局、Ｈ（ｅ）ＮＢ（ｅｎｈａｎｃｅｄ　Ｈｏｍｅ　Ｎｏｄｅ－Ｂ：拡張ホーム・ノードＢ）などのホーム・ノード、または同様のものなどのデバイスが、信頼済みコンポーネントを含むことができる。信頼済みコンポーネントは、信頼済み第三者機関により検証されることができ、信頼済み第三者機関による検証に基づきそこに格納される検証の証明書を持つことができる。

【０００４】

実施形態の一例によると信頼済みコンポーネントは、安全なコードおよびデータ記憶装置、ならびに安全なアプリケーションの実行を提供することができる信頼の不変的基盤（ｉｍｍｕｔａｂｌｅ　ｒｏｏｔ）などの、信頼の基盤（ｒｏｏｔ　ｏｆ　ｔｒｕｓｔ）を含むことができる。信頼の基盤はまた、例えば段階的な安全な立ち上げなどの安全なブート（ｂｏｏｔ）を介して信頼済みコンポーネントの整合性を検証するように構成することができる。実施形態の一例によるとデバイスは、信頼済みコンポーネントの整合性を信頼の基盤によって検証することができない場合には、第１の方針に従って動作することができ、そして信頼済みコンポーネントの整合性を検証することができる場合には、第２の方針に従って動作することができる。したがって実施形態の一例においては、信頼済みコンポーネントは、デバイス、外部のエンティティ、および通信リンクの実時間の整合性検証を含む、安全な立ち上げおよびランタイム動作を起動することができる。

【図面の簡単な説明】

【０００５】

【図１】無線通信において使用することができるデバイスの実施形態の一例を例証する図である。

【図２】信頼済みコンポーネントを含むことができるデバイスの実施形態の一例を例証する図である。

【図３】デバイス中に含むことができる信頼済みコンポーネントを確立する方法の実施形態の一例を例証する図である。

【図４】デバイスの信頼可能な環境において含むことができる信頼済みコンポーネントの実施形態の一例を例証する図である。

【図５】デバイス中の１つまたは複数のコンポーネントと通信状態にある信頼済みコンポーネントの実施形態の一例を例証する図である。

【図６】信頼済みコンポーネント中に含むことができるセキュリティ・アクセス・モニタおよびセキュリティ・アクセス表の実施形態の一例を例証する図である。

【図７】安全な立ち上げを通してデバイス中のコンポーネントを正当化する方法の実施形態の一例を表現する図である。

【図８】デバイスの自動正当化の実施形態の一例を例証する図である。

【図９】デバイスの自動正当化のための方法の一例を表現するフロー図である。

【図１０】デバイスの遠隔正当化の実施形態の例を例証する図である。

【図１１】デバイスの遠隔正当化の実施形態の例を例証する図である。

【図１２】デバイスの遠隔正当化のための方法の一例を表現するフロー図である。

【図１３】半自動正当化の実施形態の一例を例証する図である。

【発明を実施するための形態】
【０００６】
図１は、無線通信において使用することができるデバイス１００の実施形態の一例を表現する。実施形態の例によるとデバイス１００は、コンピュータ・デバイス、センサ・ノード、移動体デバイス、フェムトセル、アクセス・ポイント基地局、Ｈ（ｅ）ＮＢなどのホーム・ノード、基地局、または、ネットワークにアクセスしかつ／もしくはアクセスが限定されるかあるいは利用可能でない場合があるセル通信可能範囲などのサービス可能範囲を拡張することができる他の任意の適切なデバイス、であることができる。図１において示されるようにデバイス１００は、コンピュータ・デバイス、携帯電話、ＰＤＡ（Ｐｅｒｓｏｎａｌ Ｄａｔａ Ａｓｓｉｓｔａｎｔ：携帯情報端末）、センサ・ノード、または同様のものなどの、１つまたは複数のユーザ・デバイス１０２と通信状態にあることができる。
【０００７】
デバイス１００はまた、ネットワーク１０４などの外部の通信エンティティと通信状態にあることができる。一実施形態によるとネットワーク１０４は、ＤＳＬネットワーク、ケーブル・ネットワーク、または同様のものなどの広帯域ネットワークであることができる。実施形態の例によるとネットワーク１０４などの外部の通信エンティティは、ＰＶＥ（Ｐｌａｔｆｏｒｍ Ｖａｌｉｄａｔｉｏｎ Ｅｎｔｉｔｙ：プラットホーム正当化エンティティ）１０５、ＳｅＧＷ（Ｓｅｃｕｒｉｔｙ ＧａｔｅＷａｙ：セキュリティ・ゲートウェイ）１０６、ＨＭＳ（Ｈｏｍｅ ｎｏｄｅ Ｍａｎａｇｅｍｅｎｔ Ｓｙｓｔｅｍ：ホーム・ノード管理システム）１０７、および／またはＯＡＭ（Ｏｐｅｒａｔｉｏｎｓ Ａｎｄ Ｍａｎａｇｅｍｅｎｔ：運用管理）コンポーネント１０９を含む複数のコンポーネントを含むことができる。図１において示されるようにデバイス１００がネットワーク１０４を使用して、電話呼、テキスト・メッセージ、電子メール・メッセージ、インターネットを介する通信などのデータ・セッション、または同様のものなど無線通信を開始し、かつ／または確立することができるように、デバイス１００はＳｅＧＷ（Ｓｅｃｕｒｉｔｙ ＧａｔｅＷａｙ：セキュリティ・ゲートウェイ）１０６を介してネットワーク１０４と通信状態にあることができる。例えばユーザは、ユーザ・デバイス１０２と対話し、受信者との電話呼などの無線通信を起動することができる。ユーザ・デバイス１０２がデバイス１００の通信範囲内に入った場合には、ユーザ・デバイス１０２は、デバイス１００を使用して受信者と無線通信を起動することができる。例えばユーザ・デバイス１０２は、無線通信を起動するためにデバイス１００に要求または情報を送信または提供することができる。デバイス１００は次に、ユーザおよび受信者の間で電話呼などの通信セッションを確立することができるように、そのような要求または情報を例えばネットワーク１０４に送信することができる。
【０００８】
実施形態の例によるとその中にコンポーネントを含むデバイス１００の整合性は、ネットワーク１０４、ユーザ・デバイス１０２、および／またはＵＳＢ（Ｕｎｉｖｅｒｓａｌ Ｓｅｒｉａｌ Ｂｕｓ：ユニバーサル・シリアル・バス）接続、ブルートゥース（Ｂｌｕｅｔｏｏｔｈ）接続、ファイヤ・ワイヤ（ｆｉｒｅ ｗｉｒｅ）接続、または同様のものなどの別の外部の通信エンティティにより、デバイス１００を認証することができる前に検証することができる。例えばデバイス１００は、危険に曝された（ｃｏｍｐｒｉｓｅｄ）認証情報、物理攻撃、構成設定攻撃、プロトコル攻撃、ネットワーク攻撃、ユーザ・データ攻撃、識別子秘匿攻撃、無線リソース管理攻撃、または同様のものなどの様々な安全面での脆弱性（ｓｅｃｕｒｉｔｙ ｆｌａｗ）に曝される場合がある。例えばネットワーク１０４、ユーザ・デバイス１０２、および／または別の外部の通信エンティティが、そのような安全面での脆弱性から影響を受けることを防止するために、デバイス１００およびその中のコンポーネントの整合性が、デバイス１００およびその中のコンポーネントが、安全面での脆弱性に曝されていなかったであろうことを確実にするために検証され、またはさもなくば信頼済み状態から失墜させられる。

【０００９】
図２は、信頼済みコンポーネントを含むことができるデバイス１００の実施形態の一例を表現する。図２において示されるようにデバイス１００は、プロセッサ１１０、メモリ１１２、送受信機１１４、電源１１６、およびアンテナ１１８を含むことができる。
【００１０】
プロセッサ１１０は、信頼済みコンポーネントをロードしそして実行することを含むことができる安全なブートを、信頼の基盤により開始するための命令；信頼済みコンポーネントの整合性を検証するための命令；および信頼済みコンポーネントの整合性が検証されるかに依存する特定の方針に従って動作するための命令；などの、信頼済みコンピューティングを遂行するための命令を実行することができる標準化されたプロセッサ、専用化されたプロセッサ、マイクロ・プロセッサ、または同様のものを含むことができる。信頼済みコンポーネント１２０の整合性を検証することができない場合、プロセッサ１１０が動作する方針には、ネットワーク１０４などの外部の通信エンティティによりデバイス１００を認証するために必要となる場合がある認証情報または証明書などの情報へのアクセスを防止することを含めることができる。例えばデバイス１００は、限定的ではなく、デバイス認証、証明書準拠の認証、またはＥＡＰ－ＡＫＡ準拠の何れの認証技法をも含む、何れかの適切な認証技法を使用して、ネットワーク１０４などの外部の通信エンティティにより認証するために認証情報を使用することがきる。
【００１１】
上で説明されたように、デバイス１００はさらにメモリ１１２を含むことができる。一実施形態においてはメモリ１１２は、プロセッサ１１０により実行することができる命令、コード、データ、または他の任意の適切な情報をも格納することができる。実施形態の一例によるとメモリ１１２はＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ：ランダム・アクセス・メモリ）、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ：読み出し専用メモリ）、キャッシュ、Ｆｌａｓｈ（フラッシュ）メモリ、ハード・ディスク、または他の任意の適切な記憶デバイスを含むことができる。図２において示されるように一実施形態においては、メモリ・コンポーネント１１２をプロセッサ１１０と統合することができる。別の実施形態によるとメモリ１１２は、プロセッサ１１０と通信状態にある分離したコンポーネントであることができる。
【００１２】
デバイス１００はまた、プロセッサ１１２およびアンテナ１１８と通信状態にあることができる送受信機１１４を含むことができる。実施形態の一例によると送受信機１１４およびアンテナ１１８は、電話呼、テキスト・メッセージ、電子メール・メッセージ、インターネットを介する通信などのデータ・セッション、または同様のものなどの無線通信、および／または有線通信、の送信および／または受信を容易にすることができる。
【００１３】
図２において示されるように一実施形態においては、デバイスはさらに電源１１６を含む。電源１１６は、デバイス１００のコンポーネントを含むデバイス１００に電力を供給することができるバッテリー電源、ＡＣ／ＤＣ電源、環境発電（ｅｎｅｒｇｙ　ｈａｒｖｅｓｔｉｎｇ）電源、または同様のものであることができる。例えば電源１１６は、その中にコンポーネントを含むデバイス１００がここに説明されるように機能することができるように、プロセッサ１１０、メモリ１１２、送受信機、アンテナ１１８、または他の任意のコンポーネントに電力を供給することができる。
【００１４】
上で説明されたようにデバイス１００はまた、信頼済みコンポーネント１２０を含むことができる。実施形態の一例によると信頼済みコンポーネント１２０は、信頼の基盤に根拠を置くことができ、そして低レベルおよび高レベルのアプリケーションに対して安全な実行環境を提供することができる信頼の連鎖（ｃｈａｉｎ　ｏｆ　ｔｒｕｓｔ）に準拠することができる。
【００１５】

一実施形態によると信頼済みコンポーネント１２０は、コンポーネントの信頼性および整合性を検査することができた後に、データおよびアプリケーションをロードすることができる。信頼済みコンポーネント１２０はさらに、ロードされたアプリケーションが改ざんに対して安全であることができる実行環境を提供することができる。実施形態の例においては、例えばＵＩＣＣ（ＵＭＴＳ　Ｉｄｅｎｔｉｔｙ　Ｃｉｒｃｕｉｔ　Ｃａｒｄ）の事業者保証などの信頼済み第三者機関によって信頼済みコンポーネント１２０を保証することができ、これについては以下でさらに詳細に説明されることになる。さらに加えて信頼済みコンポーネント１２０は、デバイス１００を信頼可能であることができることを表すことができ、そしてネットワーク事業者またはネットワークは検証可能な方法にて信頼済みコンポーネントを有するとしてデバイス１００を認識し、信頼性のレベルを確立することができる。

【００１６】

信頼済みコンポーネント１２０のハードウェアおよび／またはソフトウェアを含むそれぞれのコンポーネントは、安全でありおよび信頼可能であるとして保証することができる。信頼済みコンポーネント１２０は例えば、信頼済みコンポーネント１２０の信頼性を検証することができるように、プラットホーム設計と共に配信することができる物理保証処理およびセキュリティ証明書を含むことができる。一実施形態においては、そのような信頼済みハードウェアおよび／またはソフトウェアの歩進的包含（ｉｎｃｒｅｍｅｎｔａｌ　ｉｎｃｌｕｓｉｏｎ）を使用して、信頼済みコンポーネント１２０の信頼の連鎖を生成することができ、これについては以下にさらに詳細に説明されることになる。

【００１７】

このように実施形態の例によると信頼済みコンポーネント１２０は、識別子およびアクセス制御ならびに秘匿制御などの情報に対する直接的制御を提供するために使用することができる信頼の尺度（ｍｅａｓｕｒｅ　ｏｆ　ｔｒｕｓｔ）をユーザおよび事業者に提供することができる。信頼済みコンポーネント１２０は、例えば、デバイスが信頼可能であるかについての安全かつ確実な測定、報告、および検証；ユーザ・アプリケーションの安全かつ信頼性のある動作；ユーザの識別子または仮想識別子などのデータの信頼性、秘密性、整合性、可用性、および秘匿性に対する安全かつ信頼性のある保護；ユーザ情報の浸透およびそれへのアクセスの粒状性制御（ｇｒａｎｕｌａｒ　ｃｏｎｔｒｏｌ）；または同様のもの；を提供することができる。

【００１８】

一実施形態においては、信頼済みコンポーネント１２０がまた、整合性もしくは信頼性状態の保護、例えば機密データ（ｓｅｎｓｉｔｉｖｅ　ｄａｔａ）、暗号、タイム・スタンプの安全な記憶装置、ソフトウェアの安全な実行、または同様のものを提供することができるように、信頼済みコンポーネント１２０はデバイス１００の中に、論理的に分離したエンティティ、ならびに１組の機能群およびリソース群を含むことができる。

【００１９】

実施形態の一例によると信頼済みコンポーネント１２０が提供することができる整合性または信頼性状態の保護には、信頼性状態の測定、検証、および保護を含むことができる。信頼済みコンポーネント１２０は例えば、整合性方針の実施、デバイス１００のセキュリティに重大な影響を及ぼす機能の基礎を形成することができるハードウェア機能の可用性および整合性の保護、デバイス１００の認証、信頼済みコンポーネント１２０および／またはデバイス１００の検証、または同様のものを提供することができる。

【００２０】

上で説明されたように、信頼済みコンポーネント１２０は様々な情報の安全な記憶装置を提供することができる。信頼済みコンポーネント１２０は例えば、認証情報、信頼済み参照値などの基準整合性指標、機密データ、または他の任意の適切な機密情報を格納するための安全な記憶装置を含むことができる。一実施形態によると機密データには、鍵、暗号アルゴリズム、または他の任意の適切な機密の機能もしくはデータを含むセキュリティに敏感な機能を含むことができる。

【００２１】
信頼済みコンポーネント１２０は、例えば暗号化、暗号解読、署名生成および正当化、ならびにハッシュ計算を含む暗号方式をさらに提供することができる。信頼済みコンポーネント１２０は、例えば、対称鍵準拠の暗号化および解読、非対称鍵準拠の暗号化および解読、ハッシュ値生成および検証、乱数生成、ならびに、デジタル署名の生成および検証を含む、デバイス認証または他のセキュリティに敏感な機能などの暗号機能を遂行することができる。信頼済みコンポーネント１２０はさらに加えて、信頼済みコンポーネント１２０が種（ｓｅｅｄ）、周期性、または同様なものなどのＰＲＮＧ（Ｐｓｅｕｄｏ Ｒａｎｄｏｍ Ｎｕｍｂｅｒ Ｇｅｎｅｒａｔｉｏｎ：擬似乱数生成）値の保護および生成に備えることができるようＰＲＮＧを含むことができる、乱数生成を提供することができる。上で説明されたように信頼済みコンポーネント１２０はまた、鍵または暗号アルゴリズムなど、暗号方式において使用することができる、そこに格納されたセキュリティに敏感な機能およびデータを有することができる安全な記憶装置を提供することができる。

【００２２】
一実施形態においては、信頼済みコンポーネント１２０は、例えばメッセージおよびデータの安全かつ信頼性のあるタイム・スタンプを含むタイム・スタンプ、暗号化にて署名されたスタンプ、または同様のものを提供することができる。信頼済みコンポーネント１２０はまた、実時間クロックなど実時間での尺度を提供することができる、デバイス１００におけるコンポーネントの整合性に対する保護を提供することができる。

【００２３】
信頼済みコンポーネント１２０は、デバイス１００の機能およびデータをその他のものから切り離し、そしてその機能およびデータを不正アクセスおよび改ざんから保護することによって、命令を含むソフトウェア実行ファイルなどの機能およびデータを保護することができる。さらに加えて、信頼済みコンポーネント１２０の中の機能によって作り出されたデータを含む機能の実行は、信頼済みでない場合がある他のコンポーネントなどの外部のエンティティにとってはアクセス不能とすることができる。セキュリティに重大な影響を及ぼす機能または機密のデータなどのデータは、例えば、信頼済みコンポーネント１２０の暗号化境界により提供された切り離された環境の中の安全な記憶装置に格納することができ、そしてユーザがアクセス可能なバスおよびインターフェイスを通しての外部からの探査（ｐｒｏｂｉｎｇ）から保護することができる。信頼済みコンポーネント１２０はまた、予め定義することができる抽出方針およびデータを使用して、制御されたアクセス・ポートを通してセキュリティ・パラメータの抽出を可能にすることができる。

【００２４】
信頼済みコンポーネント１２０はさらに、デバイス１００の識別子と結合することができる信頼可能な一意なＩＤ（ＩＤｅｎｔｉｔｙ：識別子）を含むことができ、そしてデバイス１００の識別子と互換性を持って使用することができる。信頼可能な一意なＩＤは、公開であることができ、そして秘密鍵など秘密に関連付けることができ、このことは信頼済みコンポーネント１２０のみが知ることができ、そして信頼済みコンポーネント１２０の外に明らかにすることはできない。信頼可能な一意なＩＤは、例えば鍵対の内の公開鍵としてメッセージに署名するために使用することができる。実施形態の一例によると信頼可能な一意なＩＤは、デバイス１００の識別子の生成機構と同一のエンティティでない場合がある鍵対の生成機構が提供する場合がある。したがって一実施形態においては、そのような識別子の間のマッピングを、例えばデバイス１００の識別子に物理的にかつ論理的に結合された信頼可能な一意なＩＤに準拠して提供することができる。例えば信頼可能な一意なＩＤおよび関連付けられた秘密鍵は、信頼の基盤の一部として製造者により予め提供することができ、そして図３に関して以下で説明されるように証明書に関連付けることができる。

【００２５】
一実施形態においては、信頼済みコンポーネント１２０は、ＨＰＭ（Ｈｏｓｔｉｎｇ Ｐａｒｔｙ Ｍｏｄｕｌｅ：ホスティング機関モジュール）ＩＤを安全に格納することが

できる。ＨＰＭ　ＩＤは、デバイス１００およびＨＰＭ（Ｈｏｓｔｉｎｇ　Ｐａｒｔｙ　Ｍｏｄｕｌｅ：ホスティング機関モジュール）を結合し、かつ認証するために信頼済みコンポーネント１２０に転送することができる。事業者方針などの方針または規則に準拠してＨＰＭ　ＩＤ記憶装置を構成することができる。信頼済みコンポーネント１２０は、信頼済みコンポーネント１２０をＨＰＭに関連付けるために、または、事業者もしくはユーザが構成することができるＨＰＭデータに信頼済みコンポーネント１２０を関連付けるために、追加的セキュリティ機能およびアルゴリズムを提供することができる。したがって実施形態の一例によると信頼済みコンポーネント１２０は、デバイス１００がホスティング機関を認証することを可能にすることができ、そしてホスティング機関の認証と同様にデバイス１００の認証にかかわった認証情報およびエンティティ間の結合の証拠を提供することができる。

【００２６】

信頼済みコンポーネント１２０にはさらに、セキュリティに敏感な機能、暗号鍵、およびデバイス１００の識別子に関連する場合がある他の認証情報を準備することができる。実施形態の一例によると、１つまたは複数のコンポーネントの識別子を安全に認証し、かつ標準化されたプロトコルを使用して外部のエンティティまたはコンポーネントを許可するべく信頼済みコンポーネント１２０を構成することができるように、セキュリティに敏感な機能、暗号鍵、および安全な帯域外処理を使用して暗号化動作のために使用することができるデバイス識別子に関連付けられたデバイス識別子および秘密鍵などの他の認証情報を信頼済みコンポーネント１２０に提供することができる。したがって一実施形態においては、外部のエンティティが、信頼可能な一意なＩＤまたはデバイス１００の識別子を有効で許可された信頼済みコンポーネント１２０に属するとして正当化することができるかもしれない。

【００２７】

実施形態の一例によると信頼済みコンポーネント１２０は、ソフトウェア実行ファイルのデータおよびハードウェア機能を互いに分離することができる、事業者が構成可能な機能分離を備えることができる。さらに、標準化された安全なプロトコルを通して信頼済みコンポーネント１２０を検証する能力のあるネットワーク１０４などのネットワークによる認証に基づき、そのような機能に対する二次的識別子を、信頼済みコンポーネント１２０中に埋め込むことができる。一実施形態においては、信頼済みコンポーネント１２０は、デバイス１００を配備することができた後に事業者が構成可能な追加的機能をダウンロードすることができる。

【００２８】

信頼済みコンポーネント１２０はさらに、安全なブートなどの安全な立ち上げ処理において初期化することができるインターフェイスなど、１つまたは複数のインターフェイスを含み、これについては、以下により詳細に説明されることになる。実施形態の一例によると、１つまたは複数のインターフェイスが保護されていないインターフェイスを含む場合がある。保護されていないインターフェイスは、信頼済みコンポーネント１２０とデバイス１００の一般的なリソースまたはコンポーネントとの間の通信を容易にすることができる。また保護されていないインターフェイスは、信頼済みコンポーネント１２０によって暗号によって保護することができているデータであり安全な記憶装置に格納することができていないデータへのアクセスを提供する場合がある。

【００２９】

１つまたは複数のインターフェイスはまた、保護されたインターフェイスを含むことができる。保護されたインターフェイスは、信頼済みコンポーネント１２０中の様々なコンポーネントまたはモジュールの間で伝達されるデータの整合性および秘匿性の保護を提供することができる。例えば一実施形態においては、保護されたインターフェイスは、その保護されたインターフェイスを使用することができる様々なコンポーネントの間の暗号化通信を提供することができるセキュリティ・プロトコルを使用することができる。セキュリティ・プロトコルは、信頼済みコンポーネント１２０がそれにより通信することができ

るコンポーネントの認証などのセキュリティ関連の尺度、ならびにメッセージ認証および秘匿性を含むことができる。

【００３０】

図３は、デバイスに含むことができる信頼済みコンポーネントを確立する方法の実施形態の一例を例証する。上で説明されたように図２のデバイス１００中に、信頼済みコンポーネント１２０などの信頼済みコンポーネントを含むことができる。実施形態の一例によると、ネットワーク１０４などの外部のエンティティに対してデバイス１００が信頼可能であるかを検証、または立証するために、信頼済みコンポーネント１２０を使用することができる。そのような検証は、デバイス１００の動作機能および／またはアプリケーションと同様に、サプライ・チェーンなどの信頼の連鎖を正当化することを含むことができる。

【００３１】

実施形態の一例においては、信頼済みコンポーネント１２０は、デバイス１００に対して、ハードウェア準拠の信頼の基盤および信頼可能である環境を提供することができ、そしてセキュリティおよび機能性に対しては独立の信頼済み第三者機関２０２が試験することができる。そして、信頼済み第三者機関２０８が試験に基づき信頼済みコンポーネント１２０を保証することができる。実施形態の一例によると、デバイス１００がデバイス１００の保証を立証するためにアタッチすることができるネットワーク１０４などの、外部の何れの通信エンティティにも通信することができるデジタル証明書を使用して保証を配信することができる。

【００３２】

さらに加えて、コード及び実行可能コード・イメージのデータ・コンポーネントのダイジェストまたはハッシュなどの信頼済み参照値を取り入れることができるコードおよびデータ・イメージを開発するために開発ツール２０４を使用することができる。実施形態の一例によると信頼済み参照値は、デバイス１００中に含まれるコードの整合性を検証するために使用することができ、そして危険に曝されたコードまたはデータを検出することができる。

【００３３】

コード・イメージを、さらに信頼済み第三者機関２０８が保証することができ、そしてデバイス１００がデバイス１００の保証を立証するためにアタッチすることができるネットワーク１０４などの外部の何れの通信エンティティにも通信することができるデジタル証明書により配信することができる。

【００３４】

図３において示されるように、独立した試験機構２０６が信頼済みコンポーネント１２０およびコードをセキュリティ機能および機能性に対して試験することができ、そして信頼済みコンポーネント１２０およびコード・イメージに対してデジタル証明書を生成するためにＣＡ（Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ：認証局）２０８に入力を提供することができる。

【００３５】

そして無線機器製造者などのデバイス製造者２１０は、信頼済みコンポーネント１２０を設計に組み込むことができ、そして保証されたコード・イメージをロードすることができる。デバイス製造者２１０は例えば、信頼済みコンポーネント１２０ならびに保証されたコードおよび信頼済み参照値を受け取ることができる。そしてデバイス製造者２１０は、信頼済みコンポーネント１２０ならびに保証されたコードおよび信頼済み参照値を含むことができるデバイス１００などのデバイスを生成することができる。

【００３６】

デバイス１００が例えばネットワーク１０４にアタッチする場合、デバイス１００は、信頼済みコンポーネント１２０およびコード・イメージに対する証明書ならびに様々な整合性測定値をネットワーク１０４に報告、または提供し、ネットワークによりデバイス１０４を正当化することができる。ネットワーク１０４は、例えばデバイス１００がネット

ワーク１０４に通信リンクを確立することをネットワーク１０４が可能にすることができるように、デバイス１００が信頼可能であろうということを検証することができる。

【００３７】

図４は、例えばデバイス１００の信頼可能な環境中に含むことができる、信頼済みコンポーネント１２０の実施形態の一例を示す。一実施形態によるとデバイス１００は、信頼済みコンポーネント１２０、及び信頼可能な環境の一部でない場合がある他のコンポーネントを含むことができる。上で説明されたように例えば、信頼済みコンポーネント１２０は、整合性または信頼性状態の保護、例えば機密データの安全な記憶装置、暗号、タイム・スタンプ、ソフトウェアの安全な実行、または同様なものに対して信頼済み環境を信頼済みコンポーネント１２０が提供することができるように、デバイス１００の中に、論理的に分離したエンティティならびに１組の機能群およびリソース群を含むことができる。図４において示されるように信頼済みコンポーネント１２０は特に、ＨＳＣ（Ｈｉｇｈ Ｓｅｃｕｒｉｔｙ Ｃｏｒｅ：高セキュリティのコア）１２２、ＭＳＥ（Ｍｏｄｕｌａｒ Ｓｅｃｕｒｉｔｙ Ｅｎｖｉｒｏｎｍｅｎｔ：モジュール型セキュリティ環境）１２４、信頼済みインターフェイス１２６、コア・インターフェイス１２８、およびコアＩＦＭ（ｃｏｒｅ ＩｎｔｅｒＦａｃｅ Ｍａｎａｇｅｒ：コア・インターフェイス・マネージャ）１３０を含むことができる。図４において例証された信頼済みコンポーネント１２０の実施形態はホーム・ノードＢデバイスにおける１つの実施方法を表現するが、実施方法をそのように限定するものではなく、かつ上で議論したように有線または無線の通信能力を有する任意のコンピュータ・デバイスにおいても信頼済みコンポーネント１２０を実施することができることが理解される。

【００３８】

実施形態の一例によるとＨＳＣ１２２は、信頼の基盤１３２、信頼済みコア１３４、およびＴｒＥ ＩＦＭ（Ｔｒｕｓｔｅｄ ＩｎｔｅｒＦａｃｅ Ｍａｎａｇｅｒ：信頼済みインターフェイス・マネージャ）１３６を含むことができる。信頼の基盤１３２は、デバイス１００、信頼済みコンポーネント１２０、およびＨＳＣ１２２にアクセス可能であることができる。一実施形態によると信頼の基盤１３２が、デバイスの安全なブートなどの安全な立ち上げ処理の間、信頼済みコア１３４および／または信頼済みインターフェイス・マネージャ１３６の整合性を確実にすることができるように、信頼の基盤１３２は、物理的にデバイス１００に結合することができる１組の不変的、不動的（ｉｒｒｅｍｏｖａｂｌｅ）ハードウェア・リソースを含むことができる。信頼の基盤１３２は例えば、スマートフォン（ｓｍａｒｔ ｐｈｏｎｅ）のＢＩＯＳ（Ｂａｓｉｃ Ｉｎｐｕｔ／Ｏｕｔｐｕｔ Ｓｙｓｔｅｍ：基本入／出力システム）と同様な機能性を含むことができる書込み保護されたＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ：読み出し専用メモリ）ユニットであることができる。信頼の基盤１３２はまた、例えば信頼済みコンポーネント１２０の正当化または検証のための情報を安全に格納することができる。信頼の基盤１３２は例えば、信頼済みコンポーネント１２０に関連付けられた信頼済み参照値などの参照指標を安全に格納することができる。実施形態の一例によると、信頼済みコンポーネント１２０中に含むことができる例えば暗号を使用して、信頼の基盤１３２コードを安全な認証情報を通して暗号化しそして／または解読することができる。

【００３９】

上で説明されたように、ＨＳＣ１２２は信頼済みコア１３４を含むことができる。実施形態の一例によると信頼済みコア１３４は、整合性測定、検証、報告および実施、自動または半自動の正当化などの信頼済みコンポーネントに対する機能；暗号化、解読、署名生成および正当化、ならびにハッシュ値計算などの暗号機能；正当化データの安全なタイム・スタンプのための機能；または同様のもの；の内の１つまたは複数を提供することができる。信頼済みコア１３４はまた、機密事項、鍵、正当化または検証に対して使用することができるコンポーネントに関連付けられた信頼済み参照値などの参照指標、暗号動作に対して使用することができるデバイス識別子およびデバイス識別子に関連付けられた秘密鍵などの認証情報、または、他の任意の情報若しくはデータ、の安全な記憶装置を提供す

ることができる。一実施形態においては信頼済みコア１３４によって、安全なブートなどの拡張された安全な立ち上げ処理を実施することができ、これについては以下でさらに詳細に説明されることになる。

【００４０】

信頼済みインターフェイス・マネージャ１３６は例えば、信頼済みコンポーネント１２０およびデバイス１００の他のコンポーネントの間の通信を提供することができる、信頼済みインターフェイス１２６を管理することができる。実施形態の一例によると信頼済みインターフェイス・マネージャ１３６は、１つまたは複数の方針に基づき信頼済みインターフェイス１２６を管理することができる。

【００４１】

信頼済みコンポーネント１２０はまた、コア・インターフェイス・マネージャ１３０を含むことができる。信頼済みコア・インターフェイス・マネージャ１３０は、ＨＳＣ１２２およびＭＳＥ１２４の間に通信を提供することができ、そして信頼済みインターフェイス・マネージャ１３６および信頼済みコア１３４の間に通信を提供することができるコア・インターフェイス１２８を管理することができる。信頼済みコア・インターフェイス・マネージャ１３０は例えば、信頼済みコア１３４および関連付けられたリソースへのアクセスを制御することができ、そして上で説明されたように、ソフトウェアおよび関連データなどの実行可能モジュールをＭＳＥ１２４にロードすることができる。実施形態の一例によると、ＨＳＣ１２２中に信頼済みコンポーネント１２０を含むことができる。さらに加えて、信頼済みコア１３４によって実施することができる拡張された安全な立ち上げ処理によって、コア・インターフェイス・マネージャ１３０の整合性を保護しかつ／または検証することができる。コア・インターフェイス・マネージャはまた、拡張された安全な立ち上げ処理を介して検証し次第、ＨＳＣ１２２および／またはＭＳＥ１２４を始動することができる。

【００４２】

ＨＳＣ１２２はまた、暗号ユニット、信頼の基盤１３２、物理的に安全にされた記憶装置、またはデバイス１００に結合することができる同様のものなどの物理的コンポーネントを含むことができる。一実施形態によると物理的コンポーネントおよび物理的に安全にされた記憶装置は、分離した、頑強なハードウェア・ユニットを含むことができる。物理的コンポーネントはまた、単純（ｓｉｍｐｌｅ）および差分（ｄｉｆｆｅｒｅｎｔｉａｌ）電力消費量解析、探査、または同様のものなどの物理的攻撃に対して保護されることができる。実施形態の一例によると、特定アプリケーションにより必要とされるかもしれない程度までそのような保護を提供することができる。ＨＳＣ１２２はさらに、不正アクセスまたは改ざんからＨＳＣ１２２中のデータを保護することができるインターフェイスを含むことができ、そして信頼済みコア１３４へのアクセスを制御することができる。このように実施形態の一例においては、物理的コンポーネント、物理的に安全にされた記憶装置、およびインターフェイスによりＨＳＣ１２２のセキュリティを保証することができる。

【００４３】

ＭＳＥ１２４は、ＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ：オペレーティング・システム）検証モジュール、時刻同期化モジュール、正当化モジュール、または同様のものなどのアプリケーションの実行のための信頼可能な環境を提供することができる。例えばコア・インターフェイス・マネージャ１３０は、デバイス１００中に含むことができるアプリケーション・モジュールを、１つまたは複数の方針または規則に基づきＭＳＥ１２４にロードすることができる。一実施形態においては、ロードすることができるそれぞれのアプリケーション・モジュールは、他のそのような環境から論理的に分離しかつ切り離すことができるＭＳＥ１２４中の保護された環境において実行することができる。信頼済みコア１３４はまたモジュールをＭＳＥ１２４にロードする前に、コア・インターフェイス・マネージャ１３０を介してモジュールの整合性を検証することができる。

【００４４】

実施形態の一例によるとＭＳＥ１２４は、セキュリティに重大な影響を及ぼすアプリケーションなどのアプリケーションのために１つまたは複数の方針または規則に基づき信頼済みコア１３４の拡張を可能にすることができる。安全方針に準拠し、信頼済みコンポーネントの外にあるエンティティに対して、信頼済みコンポーネント１２０のリソースへのアクセス制御を可能にすることができる信頼済みコア１３４および信頼済みインターフェイス・マネージャ１３６を介してロードされたアプリケーションの整合性を検証することによって、ＭＳＥ１２４のセキュリティを保証することができる。

【００４５】

上で説明されたように、予め定義された信頼可能な状態にてデバイス１００を起動することができることを保証するための安全なブートなどの安全な立ち上げ処理を介して信頼済みコンポーネント１２０を安全に始動することができる。実施形態の一例においては、安全なブートなどの安全な立ち上げ処理は、ＨＳＣ１２２、ＭＳＥ１２４、信頼済みインターフェイス１２６、コア・インターフェイス１２８、およびコア・インターフェイス・マネージャ１３０を始動することを含むことができる。一実施形態においては特に、信頼の基盤１３２はＯＳカーネルに対するブート・ローダーなどのＯＳ（Ｏｐｅｒａｔｉｎｇ Ｓｙｓｔｅｍ：オペレーティング・システム）の信頼済み要素を安全に始動することができる。一実施形態によるとブート・ローダーは、実行するためにロードされたコードおよび／またはコンポーネント、ならびにそのロードされたコードおよび／またはコンポーネントの整合性が検証されているか否かの表示を含むことができる。ブート・ローダーは例えば、コードおよび／またはコンポーネントのリストを含むことができ、このリストは、メモリにロードしておくことができ、何のコードおよび／またはコンポーネントをロードしそしてその整合性を検証することが必要であろうかを知るためにそのブート・ローダーを使用することができるように、例えばコードおよび／またはコンポーネントの整合性が検証されているか否かを含むことができる。

【００４６】

信頼の基盤１３２はまた、信頼済みコア１３４が、ＨＳＣ１２２またはＭＳＥ１２４を含む信頼済みコンポーネント１２０の他のコンポーネントを始動することができるように、例えば安全なブートを介して信頼済みコア１３４を安全に始動することができる。

【００４７】

安全なブートなどの安全な立ち上げ処理は、コンポーネントまたは要素を始動することができる前に、それぞれのコンポーネントまたは要素の、整合性を測定することまたは信頼性状態を検証することを含むことができる。例えば測定された整合性値を信頼済み参照値などの予め定められた参照指標と比較し、測定された整合性値が予め定められた参照指標と適合するか否かを判定することができる。実施形態の一例においては、例えば特定のハッシュ・アルゴリズムを使用してコンポーネントに関してハッシュを計算することによって、そのコンポーネントに関する予め定められた参照指標が獲得されている場合がある。安全な立ち上げ処理の間にそのコンポーネントの整合性を確実にするために、その後にその同一のハッシュ・アルゴリズムをデバイスが採用し、そのコンポーネントに関して再びハッシュを計算することができる。新しいハッシュは、測定された整合性値を定義する。実施形態の一例によると測定された整合性値が予め定められた参照指標に一致する場合には、コンポーネントの整合性を検証することができ、そしてコンポーネントを始動することができる。あるいはまた、測定された整合性値が予め定められた参照指標に一致しない場合には、コンポーネントの整合性を検証することはできず、そして結果としてコンポーネントを始動することはできない。安全な立ち上げ処理はさらに、信頼済みコンポーネント１２０を使用して、デバイス１００の他のコンポーネント、例えばオペレーティング・システムを安全に始動することを含むことができる。

【００４８】

一実施形態においては、その中にコンポーネントを含む信頼済みコンポーネント１２０が安全なブートなどの安全な立ち上げ処理を介して始動したかもしれない後に、信頼の基盤１３２は不変的、不動的（ｉｒｒｅｍｏｖａｂｌｅ）のままで留まることができる。し

かしながら信頼済みコア１３４がデバイス１００の改ざんを検出することができるなら、信頼済みコア１３４は、それ自体および／または信頼済みコンポーネント１２０の他のコンポーネントを動作不能にすることができる。

【００４９】

図５は、デバイス中の１つまたは複数のコンポーネントと通信状態にある信頼済みコンポーネントの実施形態の一例を例証する。図５に示されるように実施形態の他の例によると、信頼済みコンポーネント１２０はセキュリティ・アクセス・モニタ１４０を含むことができる。セキュリティ・アクセス・モニタ１４０は、信頼済みコンポーネント１２０中に含むことができるハードウェアおよび／またはソフトウェア・コンポーネント、ならびに信頼済みコンポーネント１２０の外部であることができるハードウェアおよび／またはソフトウェア・コンポーネントへのゲートウェイであることができる。

【００５０】

実施形態の一例によるとセキュリティ・アクセス・モニタ１４０は、連鎖型の（ｃｈａｉｎ　ｂａｓｅｄ）および／または実時間の整合性検証を提供することに関与することができるＭＭＵ（Ｍｅｍｏｒｙ　Ｍａｎａｇｅｍｅｎｔ　Ｕｎｉｔ：メモリ管理ユニット）と同様であることができる。セキュリティ・アクセス・モニタ１４０はさらに、メモリへのアクセスを許容または拒絶することができ、ＤＭＡ（Ｄｉｒｅｃｔ　Ｍｅｍｏｒｙ　Ａｃｃｅｓｓ：ダイレクト・メモリ・アクセス）へのアクセスを許容または拒絶することができ、周辺機器へのアクセスを許容または拒絶することができ、ハードウェアおよびソフトウェアのために使用されるセキュリティ保護機能を定義することができ、信頼済み記憶内容を特定することができ、動的な実時間のアドレス再マッピング（ｒｅｍａｐｐｉｎｇ）を提供することができ、かつ／または状態に基づくアクセス管理を提供することができる。一実施形態においてはセキュリティ・アクセス・モニタ１４０は、メモリ、周辺機器、または同様のものへのアクセスを制御するために使用することができ、ならびに連鎖型のおよび／または実時間の整合性検証の間に使用することができるセキュリティ・アクセス表を含むことができ、これについては以下にさらに詳細に説明されることになる。

【００５１】

信頼済みコンポーネント１２０はまた、ハッシュ関数１４２を含むことができる。信頼済みコンポーネント１２０は例えば、コードまたは命令に関して、そのようなコードもしくは命令、コンポーネント、データ、または同様のものが上で説明されたようにアクセス可能になることができる前に、コンポーネント、データ、または同様のものを検証するために実行することができるハッシュ関数１４２を実行することができる。実施形態の例においては、ハッシュ関数１４２は、例えばＭＤ５アルゴリズム、およびＳＨＡ－１、ＳＨＡ－２５６、ＳＨＡ－５１２、または他のＳＨＡ型アルゴリズムなどのＳＨＡ（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ：安全なハッシュ・アルゴリズム）を含む、ハッシュ・アルゴリズムの組み合わせを支援することができる。

【００５２】

ハッシュ関数１４２はまた、セキュリティ・アクセス・モニタ１４０によって提供されたデータを処理することができ、そしてデータの署名またはハッシュを生成させることができる。一実施形態によると生成された署名またはハッシュは、例えばセキュリティ・アクセス・モニタ１４０などの信頼済みコンポーネント１２０のコンポーネント中に格納することができる期待される信頼済み参照指標または値（すなわち事前に計算されたハッシュ）と検証のために比較することができ、これについては以下にさらに詳細に説明することになる。例えば、生成された署名または例えばハッシュ関数１４２によって提供された結果としてのハッシュ値を、例えば予め定められた参照指標などの参照ハッシュ値または期待される信頼済み参照値と比較することによって、ソフトウェア・コードもしくは命令、コンポーネント、データ、または同様のものの整合性を検証することができる。署名またはハッシュ値が適合しない場合であるなら、ソフトウェア・コードもしくはプログラムもしくは命令、コンポーネント、データ、または同様のものが改ざんされているかも知れない。

【００５３】
図５に示されるように、信頼済みコンポーネント１２０はさらに解読エンジン１４４および暗号化エンジン１４６を含むことができる。実施形態の一例によると解読エンジン１４４は、例えばデバイス１００の１つまたは複数のコンポーネントの整合性を検証するために使用することができるコードまたは命令を解読することができる。解読エンジン１４４はまた、例えばプロセッサ１１０により使用することができる信頼済みコンポーネント１２０の外部であることができるコンポーネントなどのデバイスのコンポーネントからのデータ、または例えば安全なメモリ１４８に格納されたデータを解読することができる。暗号化エンジン１４６は実施形態の一例においては、安全なメモリ１４８中に格納することができ、かつ／または信頼済みコンポーネント１２０の外部であり得る１つまたは複数のコンポーネントに提供することができるコードもしくは命令およびデータに対して、ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）およびＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）などの１つまたは複数の暗号化アルゴリズムを使用して、暗号化などの秘匿性および整合性保護を提供することができる。
【００５４】
信頼済みコンポーネントはさらに、安全な時計１５０および改ざん検出コンポーネント１５２を含むことができる。安全な時計１５０は、安全な時刻準拠プロトコルまたは時限アクセス管理などの、時刻維持（ｔｉｍｅ　ｋｅｅｐｉｎｇ）機能のために使用することができる実時間時計を提供することができる。安全なタイミング、不適当な機能性、不安全な改ざんの可能性を検証するために、またはプロセッサを、例えばフリーズまたはハングアップから保護するために、安全な時計１５０をまた使用することができる。
【００５５】
実施形態の一例によると改ざん検出コンポーネント１５２は、デバイス１００のコンポーネントについての不安全なまたは権限のないアクセスまたは改ざんを検出し、そして報告することができる。改ざん検出コンポーネント１５２は例えば、専用ユニットを含むことができる。専用ユニットは、信頼済みコンポーネント１２０中に含むことができる一連のモジュールを含むことができ、ハードウェアまたはソフトウェアおよびデータについての不安全なアクセスまたは改ざんの可能性を検出し、かつ報告することができる。実施形態の例によると改ざん検出コンポーネント１５２は、温度測定、時刻整合性測定、電圧測定、鍵保護、または同様のものを含むことができる。
【００５６】
図５に示されるように信頼済みコンポーネント１２０は、鍵生成機構１５４および乱数生成機構１５６を含むことができる。実施形態の一例によると鍵生成機構１５４は、例えば解読エンジン１４４および／または暗号化エンジン１４６によって使用され、コードもしくは命令およびデータを解読し、かつ／または暗号化することができるセキュリティ鍵を生成し、かつ／または提供することができる。同様に乱数生成機構１５６を、例えばデバイス１００の１つまたは複数のコンポーネントの認証、および／または例えば鍵生成機構１５４による鍵の生成の間に使用することができる乱数またはランダム値を生成し、かつ／または提供するために使用することができる。
【００５７】
実施形態の一例によると、不安全なハードウェアまたはソフトウェアなどの不安全なコンポーネントからの、ブート・プログラム、立ち上げプログラム、信頼済みチケット・センター・プログラム、暗号化されたユーザ・プログラムおよび／またはデータ、または同様のものを含む安全なコードおよびデータを切り離すために、信頼済みコンポーネント１２０をまた、使用することができる。例えば、安全なコードおよびデータへのアクセスを切り離すかまたは制御するために、セキュリティ・アクセス・モニタ１４０を使用することができる。安全な周辺機器およびＤＭＡ（Ｄｉｒｅｃｔ　Ｍｅｍｏｒｙ　Ａｃｃｅｓｓ：ダイレクト・メモリ・アクセス）ブロックへのアクセスを制御するために、セキュリティ・アクセス・モニタ１４０をまた、使用することができる。
【００５８】

図６は、信頼済みコンポーネントに含むことができるセキュリティ・アクセス・モニタおよびセキュリティ・アクセス表の実施形態の一例を例証する。上で説明されたようにセキュリティ・アクセス・モニタ１４０は例えば、デバイス１００の１つまたは複数のコンポーネントの整合性を判定するために使用することができるセキュリティ・アクセス表１６０を含むことができる。例えば一実施形態においてはセキュリティ・アクセス表１６０は、期待される信頼済み参照値、またはデバイスの１つまたは複数のコンポーネントに関して計算することができる予め定められたまたは格納されたハッシュ値などの予め定められた参照指標を含むことができる。上で説明されたように一実施形態においては信頼済みコンポーネント１２０は、コンポーネントに対して生成された署名または測定値を期待される信頼済み参照値または予め定められた参照指標と比較し、その署名または測定値が、期待される値または予め定められた測定基準に一致するか否かを判定することができる。署名または測定値が期待される値または予め定められた測定基準に一致するなら、コンポーネントの整合性を検証することができる。

【００５９】

実施形態の一例によると、デバイス１００を始動するか、または再ブート（ｒｅ－ｂｏｏｔ）することができるときに、セキュリティ・アクセス・モニタ１４０は、アドレス可能な内容および内部のコンポーネントならびに／または信頼済みコンポーネント１２０の内容を整合性に関して検証することができる。整合性を検証するとプロセッサ１１０は、変更することができない頑強なＡＳＩＣハードウェアおよび／またはソフトウェアを含むことができるブートのＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ：読み出し専用メモリ）コードの実行を開始することができる。実施形態の一例においては、頑強なＡＳＩＣハードウェアおよびソフトウェアは、信頼済みコンポーネント１２０のための信頼の基盤１３２を提供することができる。

【００６０】

図７は、デバイス１００などのデバイスにおいて安全な立ち上げを通してコンポーネントを正当化する方法の実施形態の一例を表現する。図７に示されるようにデバイスの安全な立ち上げは、信頼の連鎖を構築することによって、信頼の基盤１３２などの信頼の基盤から複数の段階における全機能状態にまで進行することができる。段階１においては、安全なブートなどの安全な立ち上げにおける信頼の基盤１３２から信頼済みコンポーネント１２０を構築することができる。例えば、安全なブートを介して信頼済みコンポーネント１２０の整合性を検証するように信頼の基盤１３２を構成することができる。段階１において信頼済みコンポーネント１２０の整合性を検証することができないなら、信頼の基盤１３２は第１の方針に従って動作することができる。例えば信頼の基盤１３２は、デバイス認証を含む暗号動作のために使用することができるデバイス識別子及びそのデバイス識別子に関連付けられた秘密鍵などの認証情報へのアクセスを防止しまたは限定することができ、または、信頼済みコンポーネント１２０および／またはデバイス１００中に格納された他の情報へのアクセスを外部のコンポーネントに対して限定しまたは防止することができる。さらに加えて、段階１において信頼済みコンポーネント１２０の整合性を検証することができないなら、安全な立ち上げが止まる場合があり、そしてその後の段階においてデバイス１００中の他のコンポーネントが検証されない場合がある。

【００６１】

あるいはまた、段階１において信頼済みコンポーネント１２０の整合性を検証することができるなら、信頼の基盤１３２は、第２の方針に従って動作することができる。例えば、信頼の基盤は信頼済みコンポーネント１２０に制御を渡すことができる。そして信頼済みコンポーネント１２０は、安全な立ち上げの段階２を遂行することができる。実施形態の一例によると、段階２において信頼済みコンポーネント１２０は、デバイス１００の動作に不可欠である場合があるさらなるコンポーネントを検証し、ロードし、そして始動することができる。例えば段階２においては信頼済みコンポーネント１２０は、通信スタック、プロトコル・スタック、および／またはネットワーク通信モジュールの整合性を検証することができる。信頼済みコンポーネント１２０は次に、検証された整合性を有するこ

とができる通信スタック、プロトコル・スタック、および／またはネットワーク通信モジュールなどのコンポーネントのそれぞれを、ロードし、そして始動することができる。実施形態の一例によると段階２において、通信スタック、プロトコル・スタック、および／またはネットワーク通信モジュールの整合性を検証することができないなら、デバイス１００は、第１の方針および／または定義することができる他の任意の適切な方針に従って動作することができる。

【００６２】

段階２において基本的コンポーネントの整合性を検証することができるなら、信頼済みコンポーネント１２０は次に、安全な立ち上げの段階３を遂行することができる。実施形態の一例によると段階３において、信頼済みコンポーネント１２０はさらなるコンポーネントを検証し、ロードし、そして始動することができる。例えば段階３においては信頼済みコンポーネント１２０は、アプリケーション、オペレーティング・システム・コンポーネント、他のハードウェア・コンポーネント、または同様のものの整合性を検証することができる。信頼済みコンポーネント１２０は次に、検証された整合性を有することができるアプリケーション、オペレーティング・システム・コンポーネント、他のハードウェア・コンポーネント、または同様のものなどのコンポーネントのそれぞれをロードし、そして始動することができる。実施形態の一例によると段階３において１つまたは複数のコンポーネントの整合性を検証することができないなら、デバイス１００は、第１の方針および／または定義することができる他の任意の適切な方針に従って動作することができる。

【００６３】

図７に示されるように実施形態の一例によると信頼済みコンポーネント１２０が、コンポーネントを、それぞれのコンポーネントの測定値またはハッシュなどの値１４５を取得し、そしてデバイス１００中に格納することができる期待されるまたは予め定められた信頼済み参照値または測定値１４７とそのような測定値または値を検証エンジン１４９を介して比較することにより、検証することができる。実施形態の一例によると、期待されるまた予め定められた信頼済み参照値または測定値１４７を、デバイス１００中にダイジェストしそして格納することができる証明書中に、安全に設定しまたは供給することができる。コンポーネントの測定値または値が、期待されるまたは予め定められた信頼済み参照値もしくは測定値、またはコンポーネントに関連付けられた証明書に一致するなら、コンポーネントの整合性を検証することができる。しかしながらコンポーネントの測定値または値が期待されるまたは予め定められた測定値またはコンポーネントに関連付けられた証明書に一致しないなら、コンポーネントの整合性を検証することはできない。

【００６４】

図８は、デバイス１００の自動正当化の実施形態の一例を例証する。一実施形態によるとデバイス１００の立ち上げの間に、デバイス１００の自動正当化を実行するか、または遂行することができる。デバイス１００は例えば上で説明されたように、直接的に測定値を評価し、デバイス１００の１つまたは複数のコンポーネントの整合性を検証することができ、その結果、検証することができないコンポーネントを始動することはできない。一実施形態によると上で説明されたように、デバイス１００中の１つまたは複数のコンポーネントの整合性を検証することができない場合には、安全なデータ、安全な機能、または同様のものへのアクセスを防止することもまたできる。さらに加えて、デバイス１００の１つまたは複数のコンポーネントの整合性を検証することができなかった場合には、デバイス１００をネットワーク１０４により認証することはできず、その結果、デバイス１００がネットワーク１０４に接続することを防止することができ、またはそのデバイスをネットワークにより認証するために使用することができる認証情報を信頼済みコンポーネントがリリースすることができない。

【００６５】

図９は、デバイス１００の自動正当化のための方法３００の一例のフロー図を表現する。図９に示されるように、３０５にて例えば信頼の基盤１３２が上で説明されたように信頼済みコンポーネント１２０の整合性を検証することができる。実施形態の一例によると

、信頼の基盤１３２が起動することができる段階的な安全なブートの一部として信頼済みコンポーネント１２０の整合性を検証することができる。

【００６６】

次に３１０にて、信頼済みコンポーネント１２０の整合性を検証することができるか否かに関して判定をすることができる。例えば上で説明されたように、信頼の基盤１３２は測定値を評価し、例えば信頼の基盤１３２中に格納することができる信頼済みコンポーネント１２０に関連付けられた信頼済み参照値と信頼済みコンポーネント１２０の測定値を比較することによって、コンポーネント１２０の整合性を検証することができる。実施形態の一例によると、信頼の基盤１３２により起動することができる段階的な安全なブートの一部として判定を為すことができる。

【００６７】

信頼済みコンポーネント１２０の整合性を検証することができない場合には３１５にて、第１の方針に従ってデバイス１００は動作することができる。第１の方針は例えば、信頼済みコンポーネント１２０中に含まれる情報へのアクセスを限定しそして／または防止することができる。したがって一実施形態においては、信頼済みコンポーネントの整合性を検証することができない場合には、例えばネットワーク１０４によりデバイス１００を認証するために使用する場合がある情報へのアクセスを防止することができる。

【００６８】

信頼済みコンポーネント１２０の整合性を検証することができる場合には３２０にて、デバイス１００は第２の方針に従って動作することができる。上で説明されたように例えば、信頼済みコンポーネント１２０の整合性を検証することができる場合には、信頼の基盤１３２は信頼済みコンポーネント１２０に制御を渡し、第２の方針により定義されるようにデバイス１００中の他のコンポーネントを検証することができる。このようにして、例えばネットワークなどの外部の通信エンティティによりそれ自体を認証するなど、デバイスが意図したように動作することを許容され、デバイスが外部の通信エンティティと通信することを可能にすることができる。

【００６９】

図１０～図１１は、デバイス１００の遠隔正当化の実施形態の一例を例証する。例えばデバイス１００は、例えばネットワーク１０４のセキュリティ・ゲートウェイ１０６への初期接続を確立することができる。一実施形態によるとデバイス１００は、デバイス１００中に含まれる１つまたは複数のコンポーネントに関連付けられた測定値をセキュリティ・ゲートウェイ１０６への接続を介してネットワーク１０４に提供することができる。

【００７０】

次に例えばＰＶＥ１０５を使用するネットワーク１０４は、上で説明されたように例えば信頼済み参照値などの予め定められた参照指標に対して受信された測定値を比較することによって、予め定められた参照指標に対して受信された測定値を評価し、デバイス１００中の１つまたは複数のコンポーネントの整合性をその比較に基づいて検証することができないかを含む、１つまたは複数の例外に遭遇する場合があるか否かを判定することができる。一実施形態において、１つまたは複数の例外に遭遇する場合であるなら、ネットワーク１０４はデバイス１００へのアクセスを拒絶することができる。別の実施形態によると１つまたは複数の例外に遭遇している場合であるなら、ネットワーク１０４はデバイス１００に、限定されたネットワーク・アクセスまたは隔離されたアクセス（ｑｕａｒａｎｔｉｎｅｄ　ａｃｃｅｓｓ）を許可することができる。ネットワーク１０４はさらに、例外の１つまたは複数が、デバイスの基本的機能に重大な影響を及ぼさないコンポーネントである非コア（ｎｏｎ－ｃｏｒｅ）・コンポーネントに関連するエラーである場合であるなら、１つまたは複数の修復策を実行するためにデバイス１００に要求を供給することができる。デバイス１００は例えば、修復的要求に対応して予め定められた状態に戻ることができる。

【００７１】

図１２は、デバイス１００の遠隔正当化のための方法４００の一例のフロー図を表現す

る。図１２に示されるように４０５にて、上で説明されたように信頼済みコンポーネント１２０の整合性を信頼の基盤が検証することができる。

【００７２】

次に４１０にて、信頼済みコンポーネント１２０がデバイス１００の他のコンポーネントに対してハッシュ計算などの整合性測定値を生成することができる。

【００７３】

デバイス１００をネットワーク１０４により正当化するために４１５にて、例えば信頼済みコンポーネント１２０が、ネットワーク１０４に整合性測定値を提供することができる。上で説明されたように例えばＰＶＥ１０５を使用するネットワーク１０４が、次に例えば上で説明されたように例えば受信された測定値を予め定められた参照指標と比較することによって、予め定められた参照指標に対して受信された測定値を評価し、デバイス１００中の１つまたは複数のコンポーネントの整合性をその比較に基づいて検証することができないかを含む、１つまたは複数の例外に遭遇する場合があるか否かを判定することができる。

【００７４】

図１３は、半自動正当化の実施形態の一例を例証する。デバイス１００は例えば、上で説明されたように信用状態の測定値を評価することができ、そして測定値の評価の結果を格納することができる。デバイス１００は次に、例えばネットワーク１０４のセキュリティ・ゲートウェイ１０６への初期接続を確立することができる。一実施形態によるとデバイス１００は、評価の結果をセキュリティ・ゲートウェイ１０６との接続を介してネットワーク１０４に提供することができる。デバイス１００はまた、測定値の部分集合をネットワーク１０４にセキュリティ・ゲートウェイ１０６との接続を介して提供することができる。さらに加えて、実施形態の一例によるとデバイス１００は、ネットワーク１０４からの要求に対応して測定値を評価し、そして提供することができる。

【００７５】

ネットワーク１０４は次に、デバイス１００中の１つまたは複数のコンポーネントの整合性測定結果に基づき、詳細に設定された（ｆｉｎｅ　ｇｒａｉｎｅｄ）アクセス制御の判定を行うことができる。ネットワーク１０４は例えば、次に例えばＰＶＥ１０５を使用してデバイス１００中の１つまたは複数のコンポーネントの整合性を検証することができなかったか否かなどの評価の間に、１つまたは複数の例外を判定することができる。一実施形態においては、１つまたは複数の例外に遭遇している場合であるなら、ネットワーク１０４はデバイス１００へのアクセスを拒絶することができる。別の実施形態によると、１つまたは複数の例外に遭遇している場合であるなら、ネットワーク１０４はデバイス１００に、限定されたネットワーク・アクセスまたは隔離された（ｑｕａｒａｎｔｉｎｅｄ）アクセスを許可することができる。ネットワーク１０４はさらに、不適合の１つまたは複数が、非コア・コンポーネント検証エラーである場合であるなら、１つまたは複数の修復策を実行するためにデバイス１００に要求を供給することができる。デバイス１００は例えば、修復的要求に対応して予め定められた状態に戻ることができる。

【００７６】

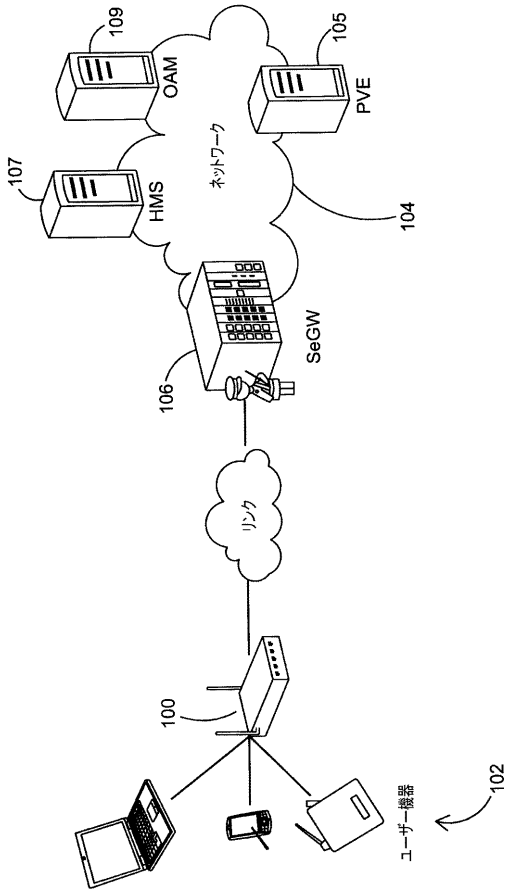
様々な図についての好適実施形態に関連して様々な実施形態を説明してきたが、それから逸脱することなく、様々な実施形態の同一の機能を遂行させるために、他の同様の実施形態を使用することができ、または説明された実施形態への修正および追加を為すことができることを理解されたい。したがって、実施形態を何れかの唯一の実施形態に限定するべきではなく、むしろ幅および範囲において添付された請求の範囲に従って解釈するべきである。

【００７７】

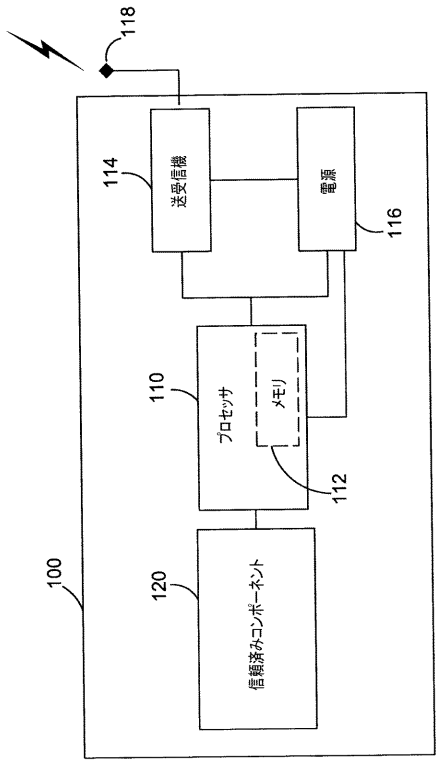
さらに加えてここに説明された様々な技法は、ハードウェアもしくはソフトウェアにまたは適当な場合には両方の組み合わせに関連して実施することができることを理解するべきである。したがって、ここに説明された主題の方法および装置、またはそのある態様または部分は、フロッピー・ディスク、ＣＤ－ＲＯＭ、ハード・ドライブ、または他の任意

の機械読取り可能な記憶装置媒体などの、具体的な媒体中に具現化された、プログラム符号（すなわち命令）の形体を取ることができ、ここでプログラム符号がコンピュータなどの機械によってロードされそして実行されると、その機械はここに説明された主題を実施するための装置となる。プログラム符号が媒体上に格納される場合には、対象の動きを集合的に遂行する１つまたは複数の媒体上に対象のプログラム符号が格納されることになる場合があるが、しかし１つまたは複数の媒体が全体としてその動きを遂行するためのプログラムを含むが、－単一の媒体より多い媒体がある場合に、－何れかの特定のプログラムの部分が何れかの特定の媒体上に格納されるべきという要件は全くない。プログラマブル・コンピュータ・デバイス上でのプログラム符号実行（そのプログラム符号は、デバイス中に予め格納するか、またはＯＭＡ　ＤＭもしくはＴＲ０６９などの遠隔デバイス管理プロトコルを通してデバイスに安全に通信することができる）の場合には、コンピュータ・デバイスは一般に、プロセッサ、プロセッサにより読出し可能な記憶媒体（揮発性および非揮発性のメモリおよび／または記憶要素を含む）、少なくとも１つの入力デバイス、および少なくとも１つの出力デバイスを含む。１つまたは複数のプログラムは、例えばＡＰＩ、再利用可能な制御、または同様なものの使用により、ここに説明された主題に関連して説明された処理を実施または利用することができる。そのようなプログラムは、望ましくは高水準手続き型またはオブジェクト指向プログラム言語にて実施され、コンピュータ・システムと通信する。しかしながら必要であるなら、アセンブラまたは機械語にてプログラムを実施することが可能である。何れの場合においても言語は、コンパイル型（ｃｏｍｐｉｌｅｄ）またはインタープリター型（ｉｎｔｅｒｐｒｅｔｅｄ）の言語であり、そしてハードウェア実施方法と結合することができる。

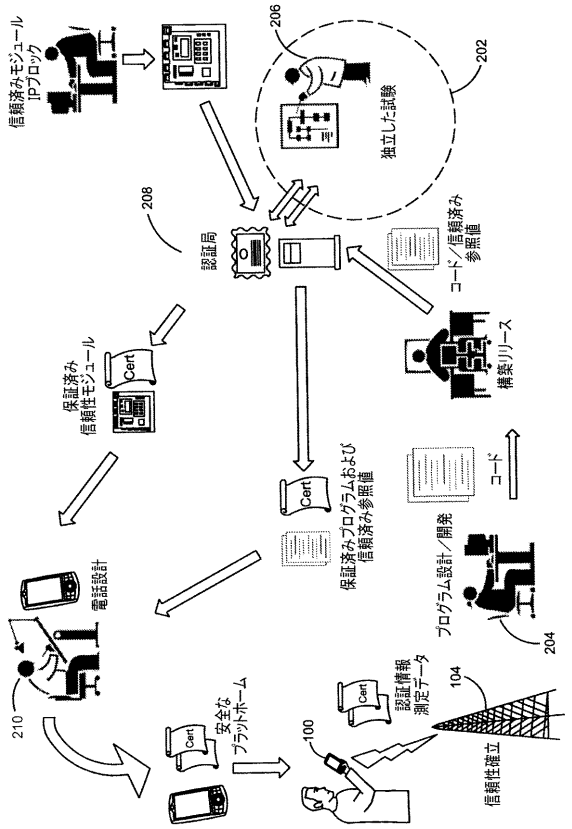
【図１】



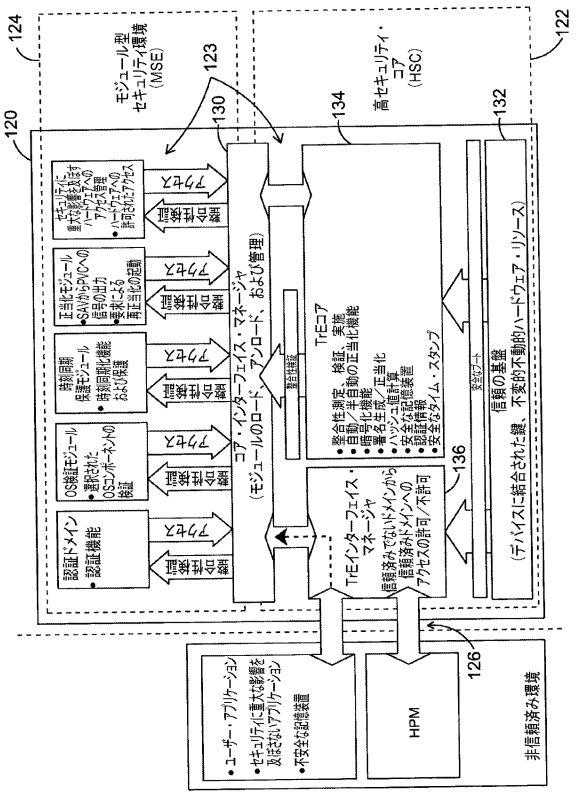
【図２】



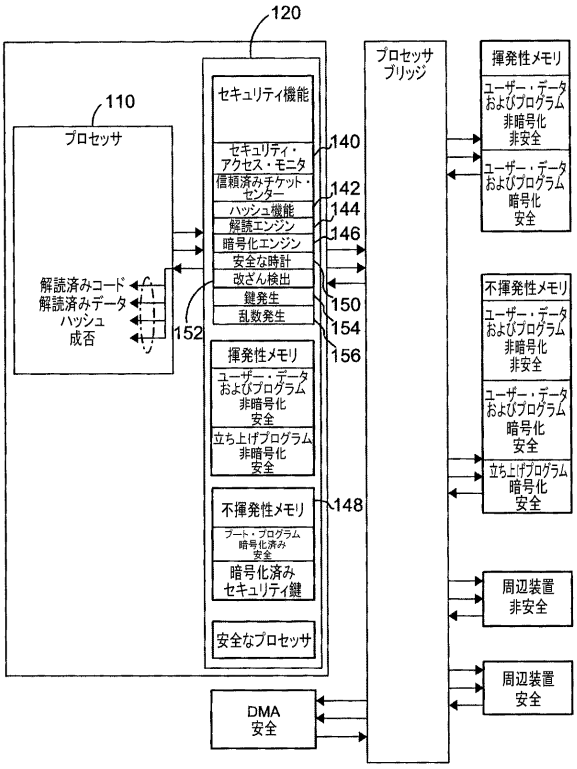
【図３】


信頼済みモジュール IPブロック
206
202
独立した試験
208
認証局
コード／信頼済み参照値
保証済み信頼性モジュール
Cert
構築リリース
保証済みプログラムおよび信頼済み参照値
コード
プログラム設計／開発
204
電話設計
210
安全なプラットホーム
100
104
認証情報測定データ
信頼性確立

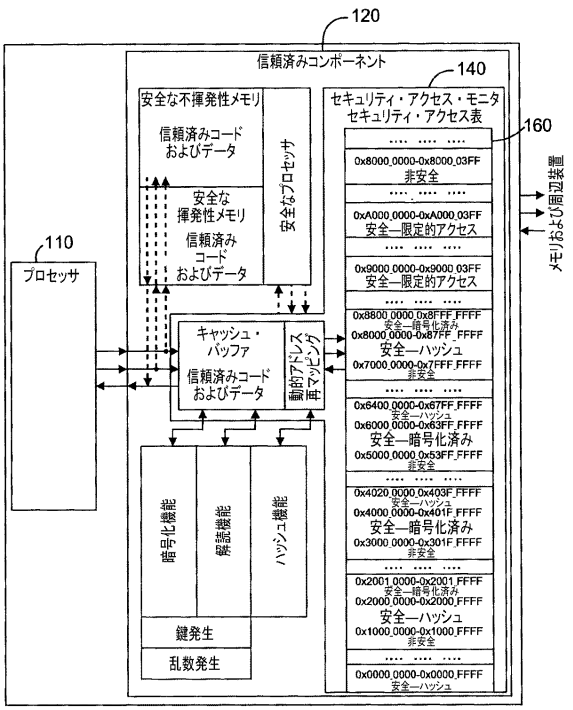
【図４】


124
モジュール型セキュリティ構築 (MSE)
123
高セキュリティ・コア (HSC)
122
120
130
134
132
TrEコア
検証、実施
自動／半自動の正当化機能
ハッシュ値計算
安全な情報記憶装置
安全なタイム・スタンプ
信頼の基盤
(デバイスに結合された鍵、不変的不動的ハードウェア・リソース)
コア・インターフェイス・マネージャ
(モジュールのロード、アンロード、および管理)
TrEインターフェイス・マネージャ
信頼済みでないドメインから信頼済みドメインへのアクセスの許可／不許可
136
126
HPM
非信頼済み構築
ユーザー・アプリケーション
セキュリティに重大な影響を及ぼさないアプリケーション
不安な記憶装置

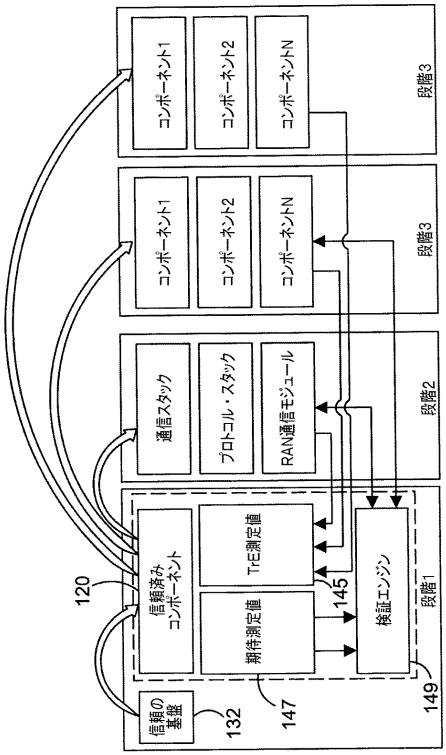
【図５】


120
110
プロセッサ
解読済みコード
解読済みデータ
ハッシュ成否
セキュリティ機能
140
セキュリティ・アクセス・モニタ
142
信頼済みチケット・センター
144
ハッシュ機能
解読エンジン
146
暗号化エンジン
安全な時計
改ざん検出
150
鍵発生
152
乱数発生
154
156
揮発性メモリ
ユーザー・データおよびプログラム 非暗号化 安全
立ち上げプログラム 非暗号化 安全
不揮発性メモリ
148
ブート・プログラム 暗号化済み 安全
暗号化済みセキュリティ鍵
安全なプロセッサ
DMA 安全
プロセッサブリッジ
揮発性メモリ
ユーザー・データおよびプログラム 非暗号化 非安全
ユーザー・データおよびプログラム 暗号化 安全
不揮発性メモリ
ユーザー・データおよびプログラム 非暗号化 非安全
ユーザー・データおよびプログラム 暗号化 安全
立ち上げプログラム 暗号化 安全
周辺装置 非安全
周辺装置 安全

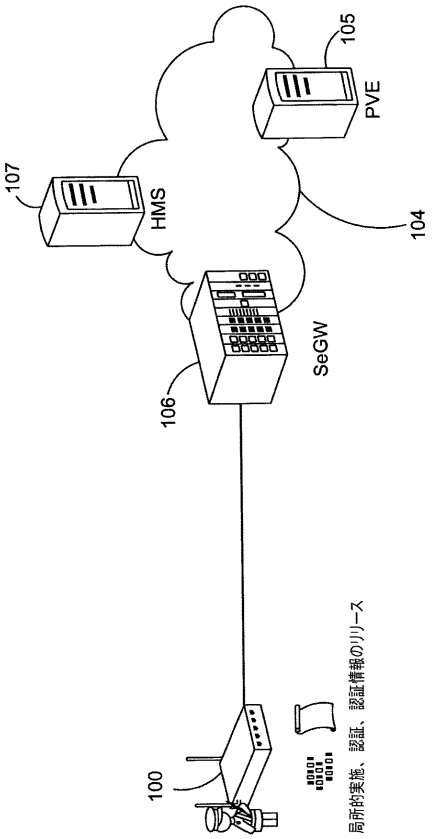
【図６】


120
信頼済みコンポーネント
140
安全な不揮発性メモリ
信頼済みコードおよびデータ
安全なプロセッサ
安全な揮発性メモリ
信頼済みコードおよびデータ
セキュリティ・アクセス・モニタ
セキュリティ・アクセス表
160
110
プロセッサ
キャッシュ・バッファ
信頼済みコードおよびデータ
動的アドレスマッピング
暗号化機能
解読機能
ハッシュ機能
鍵発生
乱数発生
0x8000_0000-0x8000_03FF 非安全
0xA000_0000-0xA000_03FF 安全—限定的アクセス
0x9000_0000-0x9000_03FF 安全—限定的アクセス
0x8800_0000_0x8FFF_FFFF 安全—暗号化済み
0x8000_0000-0x87FF_FFFF 安全—ハッシュ
0x7000_0000-0x7FFF_FFFF 非安全
0x6400_0000-0x67FF_FFFF 安全—ハッシュ
0x6000_0000-0x63FF_FFFF 安全—暗号化済み
0x5000_0000_0x53FF_FFFF 非安全
0x4020_0000_0x403F_FFFF 安全—ハッシュ
0x4000_0000-0x401F_FFFF 安全—暗号化済み
0x3000_0000-0x301F_FFFF 非安全
0x2001_0000-0x2001_FFFF 安全—暗号化済み
0x2000_0000-0x2000_FFFF 安全—ハッシュ
0x1000_0000-0x1000_FFFF 非安全
0x0000_0000-0x0000_FFFF 安全—ハッシュ
メモリおよび周辺装置

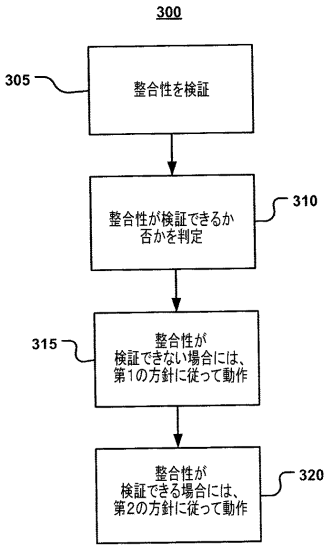
【図７】


コンポーネント1
コンポーネント2
コンポーネントN
段階3
コンポーネント1
コンポーネント2
コンポーネントN
段階3
通信スタック
プロトコル・スタック
RAN通信モジュール
段階2
信頼済みコンポーネント
TrE測定値
期待測定値
検証エンジン
段階1
信頼の基盤
120
132
145
147
149

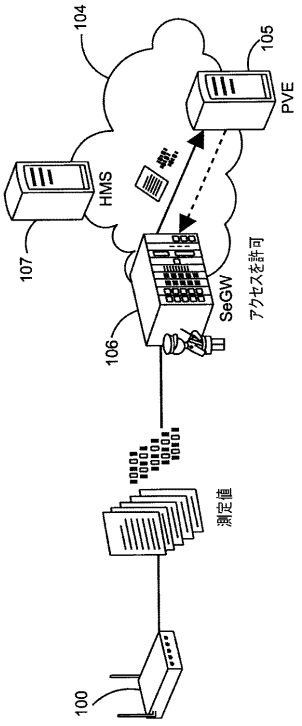
【図８】


105
PVE
107
HMS
104
SeGW
106
100
局所的実施、認証、認証情報のリリース

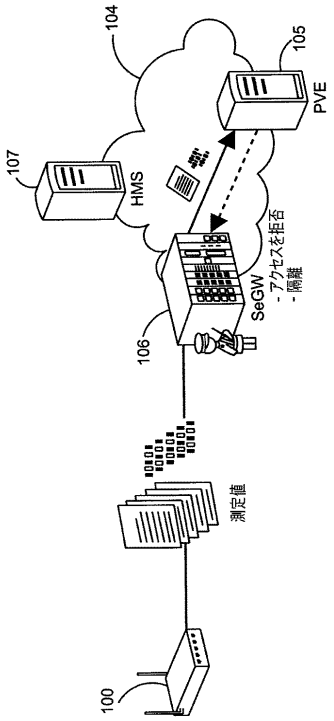
【図９】


300
305
整合性を検証
整合性が検証できるか否かを判定
310
315
整合性が検証できない場合には、第1の方針に従って動作
整合性が検証できる場合には、第2の方針に従って動作
320

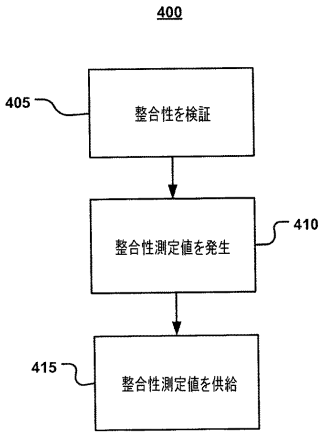
【図１０】


104
105
PVE
HMS
107
SeGW
106
アクセスを許可
測定値
100

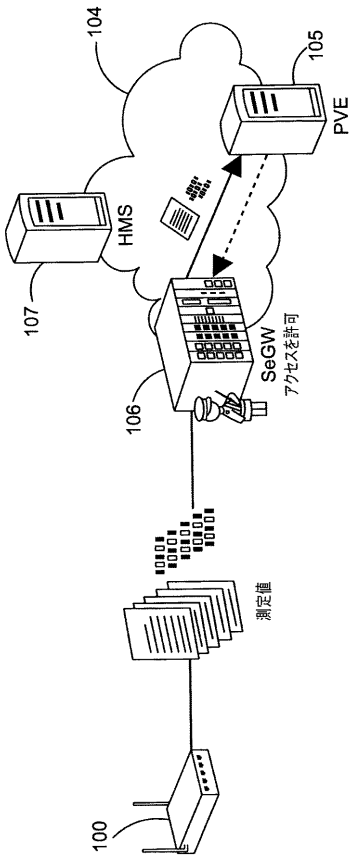
【図１１】


104
105
PVE
107
HMS
SeGW
- アクセスを拒否
- 隔離
106
測定値
100

【図１２】


400
405
整合性を検証
410
整合性測定値を発生
415
整合性測定値を供給

【図１３】


104
105
PVE
HMS
107
SeGW
アクセスを許可
106
測定値
100

フロントページの続き

(72)発明者 インヒョク チャ
アメリカ合衆国 １９０６７ ペンシルベニア州 ヤードリー サウスリッジ サークル ５１０
(72)発明者 アンドレアス ユー. シュミット
ドイツ ６５９２９ フランクフルト アム マイン トイトーネンウェグ ３７
(72)発明者 アンドレアス レイチェル
ドイツ ６０３８５ フランクフルト ハイデストラッセ １３１
(72)発明者 サミアン ジェイ. カウル
アメリカ合衆国 １９４２８ ペンシルベニア州 コンショホッケン キャンベル ドライブ １０８
(72)発明者 ジョセフ グレドン
アメリカ合衆国 １８９１４ ペンシルベニア州 チャルフォント ビリングスリー ドライブ １５９

審査官 青木 重徳

(56)参考文献 特開２００８－２９９４５７（ＪＰ，Ａ）
特開２００６－１７９００７（ＪＰ，Ａ）
特表２００７－５０５５８２（ＪＰ，Ａ）
特表２００３－５０１９４６（ＪＰ，Ａ）
国際公開第２００９／０１５５８０（WO，Ａ１）
古濱佐知子，“プラットフォーム信頼性に基づくアクセス制御フレームワーク”，２００６年暗号と情報セイキュリティシンポジウム，日本，２００６年暗号と情報セキュリティシンポジウム実行委，２００６年 1月１７日，３Ｂ２ アクセス制御，３Ｂ２－５
“TCG SpecificationArchitecture Overview”, [online], ２００４年 4月２８日, Specification, Revision 1.2, [retrieved on 2013-02-18]. Retrieved from the Internet, ＵＲＬ, <http://class.ee.iastate.edu/tyagi/cpre681/papers/TCG_1_0_Architecture_Overview.pdf>
“TCG Mobile Reference Architecture”, [online], ２００７年 6月１２日, Specification version 1.0, Revision 1, [retrieved on 2013-02-18]. Retrieved from the Internet, ＵＲＬ, <http://www.trustedcomputinggroup.org/files/temp/644597BE-1D09-3519-AD5ADDAFA0B539D2/MPWG%20tcg-mobile-reference-architecture-1.pdf>
“What is TCG's Trusted Network Connect”, Network Access Control Interoperability Lab [onlin, ２００７年 4月２９日, 4 in a Series, [retrieved on 2012-08-09]. Retrieved from the Internet, ＵＲＬ, <http://www.opus1.com/nac/teamwhitepapers/2008-04whatistcgtnc.pdf>

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｈ０４Ｌ ９／１０
Ｈ０４Ｗ １２／０６