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

特許第5205472号
(P5205472)

(45)発行日　平成25年6月5日(2013.6.5)　(24)登録日　平成25年2月22日(2013.2.22)

(51)Int.Cl.　F I
H04W 12/06 (2009.01)　H04W 12/06
H04W 8/02 (2009.01)　H04W 8/02

請求項の数 4　(全 52 頁)

(21)出願番号　特願2010-543313 (P2010-543313)
(86)(22)出願日　平成21年1月21日 (2009.1.21)
(65)公表番号　特表2011-510571 (P2011-510571A)
(43)公表日　平成23年3月31日 (2011.3.31)
(86)国際出願番号　PCT/US2009/031603
(87)国際公開番号　WO2009/092115
(87)国際公開日　平成21年7月23日 (2009.7.23)
審査請求日　平成22年9月21日 (2010.9.21)
(31)優先権主張番号　61/022,127
(32)優先日　平成20年1月18日 (2008.1.18)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　61/025,163
(32)優先日　平成20年1月31日 (2008.1.31)
(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　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(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

最終頁に続く

(54)【発明の名称】機械対機械通信を可能にするための方法および機器

(57)【特許請求の範囲】
【請求項１】
高信頼環境（ＴＲＥ）を有する機械対機械機器（Ｍ２ＭＥ）における方法であって、
認証手順を開始するステップと、
セキュア始動を達成している、前記Ｍ２ＭＥの部分を判断するステップと、
前記部分がセキュア始動の予め定義された状態を満たすとき、前記ＴＲＥによって、前記Ｍ２ＭＥがネットワークに接続するのを可能にするステップであって、これによって、前記ネットワークへ前記Ｍ２ＭＥの有効性を暗示的に示す、可能にするステップと、
前記部分が前記セキュア始動の前記予め定義された状態を満たさないとき、前記ＴＲＥによって、前記Ｍ２ＭＥが前記ネットワークに接続するのを阻止するステップであって、これによって、前記Ｍ２ＭＥの無効性を暗示的に示すステップと、
前記ＴＲＥによって、自律的検証の複数のイベントの各々に対して、前記自律的検証イベントについての情報を含む監査記録をストアするステップと、
前記Ｍ２ＭＥから独立したエンティティから、１つ以上の監査記録に対する要求を受信するステップと
を備えることを特徴とする方法。
【請求項２】
前記部分が前記セキュア始動の前記予め定義された状態を満たす場合、証明書または資格証明を生成するステップをさらに備えることを特徴とする請求項１に記載の方法。
【請求項３】

機械対機械機器（Ｍ２ＭＥ）において、
認証手順を開始するように構成されたプロセッサと、
セキュア始動を達成している、前記Ｍ２ＭＥの部分を判断し、
前記部分がセキュア始動の予め定義された状態を満たすとき、前記Ｍ２ＭＥがネットワークに接続するのを可能にして、これによって、前記Ｍ２ＭＥの有効性を暗示的に示し、
前記部分が前記セキュア始動の前記予め定義された状態を満たさないとき、前記Ｍ２ＭＥが前記ネットワークに接続するのを阻止して、これによって、前記Ｍ２ＭＥの無効性を示し、
自律的検証の複数のイベントの各々に対して、前記自律的検証イベントについての情報を含む監査記録をストアし、および、
前記Ｍ２ＭＥから独立したエンティティから、１つ以上の監査記録に対する要求を受信する
よう構成された高信頼環境と
を備えたことを特徴とするＭ２ＭＥ。

【請求項４】
前記高信頼環境は、前記部分が前記セキュア始動の前記予め定義された状態を満たすとき、証明書または資格証明を生成するようにさらに構成されたことを特徴とする請求項３に記載のＭ２ＭＥ。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、無線通信に関する。

【背景技術】
【０００２】
機械対機械（Ｍ２Ｍ）通信とは、導入されるとき、人間の直接対話を必ずしも必要としない、エンティティ間データ通信の一形態である。Ｍ２Ｍ通信の１つの課題は、人間の任意の直接対話なしに、導入機器を遠隔的に管理できるようにするためのプロトコルを確立することである。

【０００３】
既存のＭ２Ｍ方法体系は、予備構成識別子の無線の保護を欠き、Ｍ２Ｍ対応機器の認証、登録、およびプロビジョニングにおいてＭ２Ｍ対応機器の高信頼状態（ＴＳ：Ｔｒｕｓｔｅｄ　Ｓｔａｔｅ）の情報を利用せず、加入オペレータを安全に変更することをＭ２Ｍ対応機器に保証せず、Ｍ２Ｍ対応機器の予備認証において使用する、認証および鍵合意資格証明が信頼できることを保証せず、安全なソフトウェアおよびファームウェアの更新またはＭ２Ｍ対応機器の再構成を提供せず、Ｍ２Ｍ対応機器への不正変更を検出せず、その不正変更に反応しない。さらに、Ｍ２Ｍ対応機器のユーザ／加入者の役割は定義を欠く。したがって、Ｍ２Ｍの性能、セキュリティおよび信頼性を改善するための方法および機器を提供することが有利になる。

【発明の概要】
【０００４】
機械対機械（Ｍ２Ｍ）の安全なプロビジョニングおよび通信を行うための方法および機器を開示する。とりわけ、機械対機械機器（Ｍ２ＭＥ）を一意に識別するための、一時的プライベート識別子または仮接続識別（ＰＣＩＤ：Ｐｒｏｖｉｓｉｏｎａｌ　Ｃｏｎｎｅｃｔｉｖｉｔｙ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）も開示する。さらに、Ｍ２ＭＥを検証し、認証し、プロビジョニングする際に使用するための方法および機器も開示する。開示する検証手順には、開示する自律的検証、半自律的検証、および遠隔的検証が含まれる。このプロビジョニング手順には、Ｍ２ＭＥを再プロビジョニングするための方法が含まれる。ソフトウェアを更新し、Ｍ２ＭＥへの不正変更を検出するための手順も開示する。

【図面の簡単な説明】
【０００５】

より詳細な理解は、例として添付図面とともに示す、以下の説明から得ることができる。

【０００６】

【図１】機械対機械（Ｍ２Ｍ）のプロビジョニングおよび通信のための通信システムの例示的ブロック図を示す図である。

【図２】機械対機械機器（Ｍ２ＭＥ）の例示的ブロック図を示す図である。

【図３】自律的検証手順の流れ図の一例を示す図である。

【図４】半自律的検証手順の流れ図の一例を示す図である。

【図５】別の半自律的検証手順の流れ図の一例を示す図である。

【図６】遠隔的検証手順の流れ図の一例を示す図である。

【図７】Ｍ２ＭＥのプロビジョニング手順または再プロビジョニング手順の一例を示す図である。

【図８】Ｍ２ＭＥのプロビジョニング手順または再プロビジョニング手順の一代替例を示す図である。

【図９】新たに選択されたホームオペレータとともに使用するためのＭ２ＭＥの再プロビジョニング手順の流れ図の一例を示す図である。

【発明を実施するための形態】

【０００７】

本明細書で以下参照するとき、用語「無線送受信ユニット（ＷＴＲＵ）」には、ユーザ機器（ＵＥ）、移動局、固定もしくは移動加入者ユニット、ページャ、携帯電話、ＰＤＡ（携帯情報端末）、コンピュータ、Ｍ２Ｍ機器（Ｍ２ＭＥ）、Ｈｏｍｅ　ＮｏｄｅＢ、または無線環境で動作可能な他の任意の種類のデバイスが含まれるが、これだけに限定されない。本明細書で以下参照するとき、用語「基地局」には、Ｎｏｄｅ－Ｂ、サイトコントローラ、アクセスポイント（ＡＰ）、または無線環境で動作可能な他の任意の種類のインターフェイスデバイスが含まれるが、これだけに限定されない。

【０００８】

図１は、機械対機械（Ｍ２Ｍ）のプロビジョニングおよび通信のための通信システム１００の例示的ブロック図である。通信システム１００は、Ｍ２Ｍ対応機器（Ｍ２ＭＥ）１１０、訪問先ネットワークオペレータ（ＶＮＯ）１１５、登録オペレータ（ＲＯ）１３０、選択ホームオペレータ（ＳＨＯ）１４０、プラットフォーム検証局（ＰＶＡ）１５０を含む。システム１００は、機器製造業者／サプライヤ（Ｅ／Ｓ）（不図示）も含むことができる。

【０００９】

図１では、ＶＮＯ１１５を単一のネットワークエンティティとして示すが、ＵＳＩＭ／ＩＳＩＭアプリケーションの初期登録およびプロビジョニングのためにアクセスされるすべてのアクセスネットワークをＶＮＯとみなす。Ｍ２ＭＥ１１０が、別のＳＨＯに登録されるようになる場合、ＶＮＯ１１５は、ＶＮＯのままである。Ｍ２ＭＥ１１０が、現在ＶＮＯ１１５であるＳＨＯ１４０に登録されるようになる場合、ＶＮＯ１１５はＳＨＯになる。

【００１０】

ＶＮＯ１１５は、Ｍ２ＭＥ１１０に一時的なネットワークアクセスを提供する役割を果たし、そのアクセスでは、アクセス資格証明およびアクセス認証が要求される場合がある。このアクセスは、ＰＣＩＤや他の任意の一時的プライベートＩＤなどの、一時的ネットワークアクセス資格証明に基づくことができる。許容されるとみなす場合、ＶＮＯ１１５は、ＤＲＦ１７０へのオープンネットワークアクセスを提供することができ、そのアクセスでは、少なくともＲＯ１３０のサービスへのアクセスに関しては資格証明または認証は不要である。例えばこの機能は、登録イベントおよびプロビジョニングイベントの後、ＶＮＯ１１５が顧客のＳＨＯになる場合に適用される。登録手順およびプロビジョニング手順を実施した後、ＶＮＯ１１５は、プロビジョンしたＵＳＩＭ／ＩＳＩＭアプリケーションを使用して完全なネットワーク（およびＩＭＳ）アクセスを提供する。

【００１１】
図示のように、ＲＯ１３０は、ＩＣＦ１６０、発見および登録機能（ＤＲＦ）１７０、ならびにダウンロードおよびプロビジョニング機能（ＤＰＦ）１８０を含む。しかし、このＩＣＦ１６０、ＤＲＦ１７０、およびＤＰＦ１８０は、別個のエンティティに位置し、または１つのエンティティにまとめることができることも当業者は理解されよう。
【００１２】
ＩＣＦ１６０は、操作上のネットワークアクセスの登録およびプロビジョニングのために、通信ネットワークへの一時アクセスを許可する資格証明を検証する役割を果たす機能または機関である。ＩＣＦ１６０の機能には、各Ｍ２ＭＥ１１０ごとに、一時的ネットワークアクセス資格証明および任意の一時的プライベート識別子を発行することが含まれる。これらは、初期一時的ネットワークアクセスを認証し、ＵＳＩＭ／ＩＳＩＭアプリケーションのプロビジョニング手順を行うことを可能にするために使用することができる。ＩＣＦ１６０は、以下に詳細に論じるプロビジョニング手順および再プロビジョニング手順のために、ダウンロード可能なＭ２Ｍの鍵、構成、およびアプリケーションで、無線によりＭ２ＭＥ１１０をプロビジョンするように構成することもできる。
【００１３】
ＩＣＦ１６０は、Ｍ２ＭＥ１１０を事前構成する端末サプライヤに、ＩＣＦ１６０が発行する資格証明を提供するように構成することもできる。これらの資格証明を提供するために、ＩＣＦ１６０は、資格証明をＭ２ＭＥ１１０に埋め込む役割を果たす組織に対し、それらの資格証明を安全に伝送するように構成されなければならない。ＩＣＦ１６０は、資格証明をデータベースに登録し、依拠当事者による要求時にそれらの資格証明の検証を実行するように構成することもできる。これは認証ベクトルおよび／または他の関連データを、依拠当事者に安全に伝送することを含むことができる。Ｍ２ＭＥ１１０をＳＨＯ１４０に成功裏に登録する前、すべてのアクセスネットワークが訪問先ネットワークとみなされることに留意すべきである。このことは、ネットワークを一切変更することなく、従来のネットワークを介してＳＨＯ１４０にトランスペアレントに接続することを可能にする。
【００１４】
ＤＲＦ１７０は、特定のＳＨＯ１４０を購入後に選択すること、およびそのＳＨＯ１４０にＭ２ＭＥ１１０を登録することを可能にする機能である。ＤＲＦ１７０は、独立したサービスとすることができ、あるいは、ＳＨＯ１４０であって、ＳＨＯ１４０のＲＯ１３０には、ＳＨＯ１４０の３ＧＰＰネットワークを介してのみ接触可能とすることができる、またはインターネットを介して直接接触可能であり、例えばＭ２ＭＥ１１０内の機能を使用して発見可能とすることができる、ＳＨＯ１４０が運営することもできる。
【００１５】
ＤＲＦ１７０は、少なくとも次の使用関連機能をサポートすべきであり、その機能とはつまり、（１）サプライヤからＭ２ＭＥ１１０が届けられた後、顧客がＳＨＯ１４０を選択できるようにする機能、（２）一時的に認証されたネットワークアクセスまたは限定されたオープンネットワークアクセスを使用し、Ｍ２ＭＥ１１０がＲＯ１３０にＩＰ接続できるようにする機能、（３）Ｍ２ＭＥ１１０がまだどのＳＨＯ１４０にも関連していないものとして、訪問先ネットワークオペレータを介し、ＵＳＩＭ／ＩＳＩＭアプリケーションのプロビジョニングが行われることを、Ｍ２ＭＥ１１０が要求できるようにする機能、（４）そのプロビジョニング要求を承認し、Ｍ２ＭＥ１１０をＤＰＦ１８０がプロビジョンすることを許可する機能、および（５）Ｍ２ＭＥ１１０の所有者が、Ｍ２ＭＥ１１０を登録することをサポートする機能である。
【００１６】
上述した使用関連機能をサポートするために、ＤＲＦ１７０は、Ｍ２ＭＥ１１０とＳＨＯ１４０との関連付けをサポートすることができる。あるいは、ＤＲＦ１７０は、ＶＮＯのネットワークが提供するＩＰ接続を使用して、直接発見可能かつアドレス可能とすることができる。どちらの場合にも、ＤＲＦ１７０は、Ｍ２ＭＥ１１０の高信頼環境（ＴＲＥ

）２３０の真正性の証明としてＭ２ＭＥ１１０が保持する資格証明を、ＰＶＡ１５０を介して検証することをサポートする必要がある。ＤＲＦ１７０は、許可および監査のために、ＤＰＦ１８０への接続もサポートする必要がある。検証は、資格証明についてだけでなく、ＴＲＥ２３０、およびＴＲＥ２３０がそのように望む場合、オプションでＭ２ＭＥ１１０全体についても行えることにも留意すべきである。例えば検証には、Ｍ２ＭＥ機能の信頼性を確立することが含まれ得る。

【００１７】

ＤＲＦ１８０は、ＵＳＩＭ／ＩＳＩＭの資格証明、ファイル、実行ファイルなど、Ｍ２ＭＥ１１０にダウンロードしようとするデータパッケージの生成または取得もサポートすることができる。ＤＲＦ１８０は、このデータを安全にＰＳに伝送するように構成することもできる。あるいは、ＤＰＦ１８０がこれらの機能を提供することもできる。

【００１８】

最後に、ＤＲＦ１８０は、Ｍ２ＭＥ１１０とＤＰＦ１８０との間のセキュリティアソシエーションの設定を容易にすることもできる。これは、セキュリティトークンを生成し、安全なチャネル上でＭ２ＭＥ１１０およびＤＰＦ１８０に伝送することを必要とし得る。

【００１９】

ＤＰＦ１８０は、Ｍ２ＭＥ１１０にＵＳＩＭ／ＩＳＩＭ資格証明を遠隔プロビジョニングすることを可能にする。ＤＰＦ１８０の機能には、Ｍ２ＭＥ１１０をプロビジョンするための許可をＤＲＦ１７０から受ける機能が含まれる。これは、Ｍ２ＭＥ１１０と通信するためのセキュリティトークンを提供することを含むことができる。ＤＰＦ１８０は、ダウンロードされるアプリケーションパッケージをＤＲＦ１７０から受け取る役割も果たす。あるいはＤＰＦ１８０は、記憶された規則からこのアプリケーションパッケージを生成し、Ｍ２ＭＥ１１０にダウンロードされている資格証明をＤＲＦ１７０に知らせることができる。

【００２０】

ＤＰＦ１８０は、以下に説明するように、ＵＳＩＭ／ＩＳＩＭアプリケーションまたはＵＳＩＭ／ＩＳＩＭパラメータを、Ｍ２ＭＥ１１０にプロビジョニングすることをサポートするようにも構成される。プロビジョニングに加え、ＤＰＦ１８０は、Ｍ２ＭＥ１１０にとってのＵＳＩＭ／ＩＳＩＭアプリケーションまたはＵＳＩＭ／ＩＳＩＭパラメータを将来更新し、新たなアプリケーションを将来プロビジョニングするように構成することもできる。これらの機能に含まれ、ＤＰＦ１８０は、成功したまたは失敗したプロビジョニングイベントをＤＲＦ１７０に知らせるように構成することもできる。

【００２１】

ＳＨＯ１４０は、顧客またはＭ２ＭＥ１１０のエンドユーザと商業的関係を有するネットワークオペレータであり、顧客に課金する役割を担う。ＳＨＯ１４０は、他の役割、特にＤＲＦ１７０およびＤＰＦ１８０の一部もしくはすべてを運営することができ、またはそれらの他の役割はすべて、ＳＨＯ１４０と運営上の関係を有し、互いに運営上の関係を有する別個の商業エンティティとすることができる。

【００２２】

Ｍ２ＭＥ１１０は、サービスプロバイダを用いて動作する権限を最初は与えられておらず、そのためＶＮＯ１１５と通信し、ＲＯ１３０へのチャネルを確立する。サービスをプロビジョンするために、各Ｍ２ＭＥ１１０はＰＣＩＤなどの独自の一時的プライベート識別を有し、その独自の一時的プライベート識別は、任意のＶＮＯ１１５がＭ２ＭＥ１１０を認識し、そのＶＮＯ１１５が提供するサービスへの一時アクセスを許可し、オペレータとのサービスをダウンロードしてプロビジョンするために、初期接続性メッセージを適切なネットワーク構成要素に宛てることを可能にする。

【００２３】

ＰＶＡ１５０は、ダウンロードしたＵＳＩＭ／ＩＳＩＭアプリケーションを記憶し、実行するために使用する、Ｍ２ＭＥ１１０内のセキュアデバイスの真正性を立証する資格証明に関与する機関である。この機能は、証明書や鍵の対などの資格証明を発行し、証明書

検証サービスを提供する１つまたは複数の商業組織が行うことができる。このセキュアデバイスは、ＵＩＣＣ、ＴＲＥ、またはＭ２ＭＥ１１０に埋め込まれる他の何らかの形のセキュアモジュールとすることができる。この機能は、ＵＳＩＭ／ＩＳＩＭアプリケーションをプロビジョニングするために、セキュアデバイスの厳密認証が必須である場合に必要とされる。ＰＶＡ１５０は、Ｍ２ＭＥ１１０内のセキュアデバイスのセキュリティを立証するための資格証明の作成および発行などの機能も提供することができる。ただし、この機能は別のエンティティが実行し得る可能性もある。ＰＶＡ１５０は、必要なプロトコルを使用して依拠当事者が要求するとき、上述した資格証明を検証することなどの機能も提供することができる。これは認証ベクトルおよび／または他の関連データを、依拠当事者に安全に伝送することを含むことができる。ＰＶＡ１５０は、デバイスの発行された資格証明の有効性に関係するデータの保守などの機能も提供することができる。

【００２４】

機器製造業者／サプライヤ（Ｅ／Ｓ）（不図示）も、図１の通信システム１００内で役割を果たす。具体的には、Ｍ２ＭＥ１１０は、一時的な初期ネットワークアクセスのための認証用の資格証明を、ＩＣＦ１６０から安全に取得する。このＥ／Ｓも、一時的な初期ネットワークアクセスを可能にするために、それらの予備ネットワークアクセス資格証明を用いて、顧客に届ける前にＭ２ＭＥ１１０を再構成することをサポートできる。さらに、このＥ／Ｓは、ＩＣＦ１６０を介してＤＲＦ１７０に提供する際に使用するための、Ｍ２ＭＥ１１０が１組の標準化されたセキュリティ要件に従う、資格証明を、ＰＶＡ１５０から安全に得ることができる。この活動は、所要のセキュア基盤を備える承認された組織に外注することができる。

【００２５】

このＥ／Ｓは、顧客に届ける前に、Ｍ２ＭＥ１１０を資格証明で事前構成する役割を果たすこともできる。この事前構成活動は、所要のセキュア基盤を備える承認された組織に外注することができる。このＥ／Ｓは、端末の所有者が所望のＤＲＦ１７０およびＳＨＯ１４０を選択し、または端末をアクセスネットワーク（ＡＮ）に接続するときに、この選択を自動的に行わせるための手段も提供することができる。

【００２６】

図２は、図１のＭ２ＭＥ１１０の図の一例を示す。Ｍ２ＭＥ１１０は、送信機２１５、受信機２２０、プロセッサ２２５、高信頼環境（ＴＲＥ）２３０を含む。オプションで、Ｍ２ＭＥ１１０は、ＧＰＳ（全地球測位システム）ユニット２３５、ＳＩＭ（加入者識別モジュール）２４０、およびセキュアタイムユニットを含むことができる。

【００２７】

Ｍ２ＭＥ１１０は、ＴＲＥ２３０などの多くの異なる信頼機構、またはＳＩＭ２４０やＩＳＩＭなど、他の任意の高信頼処理機構もしくは記憶機構をサポートするように構成することができる。これらの信頼機構は、Ｍ２ＭＥ１１０内のＴＲＥ２３０が保護する「信頼状態」情報および／または任意の鍵を含めるために、共通ＡＫＡプロトコルに、より完全に統合し、完全なＡＫＡを行うことができる前かつ認証を確立した後の、Ｍ２ＭＥ１１０とネットワーク要素との間の（ＰＣＩＤの伝送だけでない）任意の通信を保護することもできる。

【００２８】

オプションで、ＳＩＭ２４０は、拡張して高信頼処理モジュール（ＴＰＭ：Ｔｒｕｓｔｅｄ　Ｐｒｏｃｅｓｓｉｎｇ　Ｍｏｄｕｌｅ）またはモバイル高信頼モジュール（ＭＴＭ：Ｍｏｂｉｌｅ　Ｔｒｕｓｔｅｄ　Ｍｏｄｕｌｅ）の機能を含め、上述した操作をサポートすることもできる。あるいは、ＳＩＭ２４０は、Ｍ２ＭＥ１１０内でＴＰＭまたはＭＴＭと密接に動作して所望の機能を実現することができる。このＳＩＭの機能は、ＴＲＥ２３０内でも実現できることにも留意すべきである。このことは、識別管理において、より一層の柔軟性をもたらす。

【００２９】

オプションで、Ｍ２ＭＥ１１０は、Ｅ／Ｓがインストールする少なくとも１つのＡＫＡ

ルート秘密（ＡＫＡ　ｒｏｏｔ　ｓｅｃｒｅｔ）で事前にプロビジョンすることができ、そのうちの１つは任意の所与の時間においてアクティブである。この１つまたは複数のＡＫＡルート秘密は、ＳＩＭ２４０によって保護することができ、決して変えられるべきでない。ＳＩＭ２４０は、アクティブなＡＫＡルート秘密からセッション鍵を取り出すように構成することができる。

【００３０】

Ｍ２ＭＥ１１０は、信頼状態情報をＩＣＦ１６０に提供するように構成することもできる。次いで、その信頼状態情報は、Ｍ２ＭＥ１１０がＶＮＯ１１５にアタッチするときの予備認証に使用することができる。この信頼状態情報は、セッション鍵（ＣＫおよびＩＫ）を取り出すために使用することもできる。

【００３１】

ＴＲＥ２３０の機能は、１つの構成要素に排他的に実装し、またはＭ２ＭＥ１１０内の埋め込み高信頼構成要素間に分散させることができることに留意すべきである。あるいは、ＴＲＥ２３０の機能は、リムーバブルＳＩＭモジュールに実装することができる。

【００３２】

ＰＣＲレジスタの値を、セッション鍵ＣＫｎおよびＩＫｎに結合するための公式の一例であって、ｎはCK_nおよびIK_nの最新の更新に関する指数を指す、公式の一例は次のものとすることができる。

【００３３】

【数１】

$$CK_n = f3_K(RAND||PCR0_n)$$
$$IK_n = f4_K(RAND||PCR0_n)$$

等式１

【００３４】

ただし、$f3_K()$および$f4_K()$は、共有マスタ秘密Ｋによる、暗号鍵および完全性鍵それぞれのＡＫＡ鍵導出関数を指し、ＲＡＮＤは、ＡＫＡプロセスにおいてＣＡＴＮＡが生成し、Ｍ２ＭＥ１１０に送信され、したがってＭ２ＭＥ１１０が共有する、認証ベクトル（ＡＶ）内のランダムノンスであり、$PCR0_n$は、Ｍ２ＭＥ１１０のＭＴＭＥ内のＰＣＲ０レジスタの最新値を指す。ＰＣＲ０レジスタの現在値は、Ｍ２ＭＥ１１０の直近のブート後の信頼状態についての記述を示すことに留意されたい。

【００３５】

等式１によれば、CK_nおよびIK_nの値は、２つのブート間でＭ２ＭＥ１１０のＰＣＲ０の値が変わるとき／場合に変わることに留意されたい。このような方式が機能するために、ＩＣＦ１６０もＰＣＲ０の値の変化（またはより具体的には、Ｍ２ＭＥ１１０のブート後の信頼状態に変化がある場合のＭ２ＭＥ１１０の「信頼状態」を知る必要がある。これは、Ｍ２ＭＥ１１０のブート後の信頼状態に影響を与える、Ｍ２ＭＥのＯＳ、ファームウェア、もしくはアプリケーションの任意の正当な更新／許可された更新についてのスケジュールおよび内容をＩＣＦ１６０に知らせる場合に可能にすることができる。この知らせることは、ＰＶＡ１５０および／またはＩＣＦ１６０を以下に説明する手順に関与させることによって行うことができる。その後、適切な手順に従い、セッション鍵がＭ２ＭＥ１１０の最新の「信頼状態」値を反映し、それにより、このＡＫＡ鍵導出プロセスの新鮮さおよびセキュリティを向上させる方法で、Ｍ２ＭＥ１１０とＩＣＦ１６０との間で共有されるＡＫＡ暗号鍵および完全性鍵が更新され、Ｍ２ＭＥ１１０の認証に関して有用にされることを確実にすることができる。

【００３６】

Ｍ２ＭＥ１１０とＩＣＦ１６０との間でセッション鍵を同じ方法で更新することができ、Ｍ２ＭＥ１１０における更新手順自体を、高信頼コンピューティング技術を使用することによって提供されるような高信頼実行環境で実行する限り、等式１の結合公式以外の結

合公式を考慮できることに留意すべきである。

【００３７】

ＴＲＥ２３０は、分離に対するハードウェアサポートを伴う、Ｍ２ＭＥ１１０内の論理的分離領域である。このＴＲＥ２３０は、必ずしもリムーバブルモジュールとは限らず、すなわちＴＲＥ２３０は、１つのＩＣ内で、またはＩＣの集まりにわたって分散される機能内で機能することができる。ＴＲＥ２３０は、ＴＲＥ２３０と直接通信することを許可されたエンティティの制御下でのみ使用可能な、外部への論理インターフェイスおよび物理インターフェイスを定義する。

【００３８】

ＴＲＥ２３０は、ＭＩＤ（複数の管理可能識別）のためのセキュア記憶域およびセキュア実行環境、ならびにＭＩＤのプロビジョニングおよび管理に関係する特定の機能に信頼のルートを提供する。このＭＩＤは、完全なセキュアアプリケーションおよびその関連するパラメータ、資格証明等の総称である。このＭＩＤは、標準ＵＳＩＭのアプリケーションおよび鍵や、ＩＳＩＭアプリケーションまたはセキュアペイメントアプリケーションなどの他のセキュアアプリケーションなど、任意の加入管理機能を含むことができる。本明細書では以下、ＭＩＤは、管理可能識別、加入管理識別、ＵＳＩＭアプリケーション、ＩＳＩＭアプリケーション、仮想ＳＩＭ（ｖＳＩＭ）、または他の任意の動的セキュア識別解決策を指すために使用することができる。

【００３９】

ＴＲＥ２３０は、任意の所要の暗号化鍵および他の資格証明とともに、セキュアな帯域外機能実装内に事前にプロビジョンすることもできる。ＴＲＥ２３０の他のセキュリティ上重要な機能も、同じ方法でＭ２ＭＥ１１０に事前にプロビジョンされる。Ｍ２ＭＥ１１０が発行された後、典型的にはダウンロードすることにより、さらなる機能をプロビジョンすることができる。

【００４０】

ＴＲＥ２３０はさらに、物理的攻撃および論理的攻撃からの一定の保護を提供し、自らのセキュリティポリシをサポート／実施し、現在はＵＩＣＣまたは他のスマートカードプラットフォームにしか実装されていないＭＩＤの記憶および実行を可能にすることに関し、十分にセキュアである。ＴＲＥ２３０は、ＴＲＥ２３０外部の、Ｍ２ＭＥ１１０の各部へのインターフェイスも備える。

【００４１】

ＴＲＥ２３０は、Ｍ２ＭＥ１１０の識別に典型的に関連する独自の埋め込まれた一意の識別を有し、Ｍ２ＭＥ１１０の識別は、使用する場合、同様にＴＲＥ２３０に埋め込まれる。そのようなものとして、ＴＲＥ２３０は、標準化されたプロトコルを使用し、それらの識別を発行機関に対して安全に認証するように構成することができる。次いでその発行機関は、そのＴＲＥの識別が、有効な、発行済みのＴＲＥ２３０およびＭ２ＭＥ１１０の識別であるとして検証することができる。それらの識別のそれぞれは、Ｍ２ＭＥ１１０が発行される前に行われる、物理的にセキュアな帯域外プロセスの一部として埋め込まれる。

【００４２】

ＴＲＥ２３０は、特定の強化機能を備える埋め込み型ＵＩＣＣ内に実装し、またあるいは、Ｍ２ＭＥ１１０が提供するハードウェア構成要素およびソフトウェア構成要素を利用する、Ｍ２ＭＥ１１０上の統合的解決策として実装することができる。ＴＲＥ２３０を強化型ＵＩＣＣ内に実装する場合、ＴＲＥ２３０は、ＭＩＤのダウンロード、遠隔プロビジョニングおよび管理、ならびにＴＲＥ２３０内の管理可能識別エンジン（ＭＩＤＥ：Ｍａｎａｇｅａｂｌｅ　Ｉｄｅｎｔｉｔｙ　Ｅｎｇｉｎｅ）の機能を依然としてサポートする。

【００４３】

ＴＲＥ２３０を、Ｍ２ＭＥ１１０内の統合的解決策として実装する場合、Ｍ２ＭＥ１１０は、ＴＲＥコードベースを構成するソフトウェアコードおよびデータの完全性検査をサ

ポートする。ＴＲＥコードは、Ｍ２ＭＥ１１０の電源投入／ブート時に少なくとも１度検査すべきである。オプションのコード検査は、定義済みの間隔でまたは特定のトリガ／イベント時に、バックグラウンドプロセスとして、Ｍ２ＭＥ１１０の動作的使用の間に行うことができる。さらに、Ｍ２ＭＥ１１０の完全検査または部分的検査を範囲に含むように、コード検査の適用範囲を拡張することができる。

【００４４】

代替的拡張策では、ＴＲＥ２３０は、ＴＲＥ２３０内に、利害関係のある所有者がそれぞれ所有する複数の分離された信頼済みドメインに対するサポートを含むことができる。そのようなドメインは、互いに分離され、不正変更および不正アクセスを防ぎ、認証機能および／または立証機能などのドメイン間サービスを提供することができる。

【００４５】

一部の使用事例では、Ｍ２ＭＥ１１０は、その導入サイクルのほとんどの期間休止状態で動作し、散発的にまたはたまにしか３Ｇネットワークに接続しない。そのような場合、ＴＲＥのソフトウェアコードの実行時完全性検査は、休止状態の期間中に行わせることができる。このようにして、このコード検査はＴＲＥ２３０またはＭ２ＭＥ１１０内の他のプロセスを妨げることはなく、コード検査の結果は、Ｍ２ＭＥ１１０がＳＨＯ１４０に再接続するときに準備ができているようにすることができる。

【００４６】

各Ｍ２ＭＥ１１０に、Ｍ２ＭＥ１１０にとって固有の一時的プライベート識別、仮接続識別（ＰＣＩＤ）を割り当てる必要がある。ＰＣＩＤとは、各Ｍ２ＭＥを一意に識別する一時的プライベート識別である。状況によっては、このＭ２ＭＥがＳＨＯ１４０などの任意の特定のＳＨＯに関連付けられる前に、３ＧＰＰネットワークに登録することを可能にするために、ＥＳがＭ２ＭＥ１１０にこのＰＣＩＤをインストールする必要がある。このＰＣＩＤは、ＩＣＦ１６０が最初に発行し、ＩＣＦ１６０はそのＰＣＩＤを、自らが提供関係を有するＥＳに送信する。次いで、そのＥＳは、そのＰＣＩＤをＭ２ＭＥ１１０のＴＲＥ２３０内にプロビジョンする。Ｍ２ＭＥ１１０からＶＮＯ１１５にＰＣＩＤが提示される場合、ＶＮＯ１１５は、標準のＩＭＳＩの形式を有するものとしてそのＰＣＩＤを認識し、その後、Ｍ２ＭＥ１１０をＲＯ１３０に導き、プロビジョニングのための初期接続性を確立することができる。

【００４７】

一実施形態では、Ｍ２ＭＥ１１０が実施する限られた期間（本明細書では以下「有効期間」）にわたり、単一のＰＣＩＤを有効とすることができる。この有効期間は、Ｍ２ＭＥ１１０のＴＲＥ２３０により、とりわけ制御することができる。各Ｍ２ＭＥデバイスは、ＰＣＩＤおよび有効期間を受け取ることができる。この期間が切れた後、Ｍ２ＭＥ１１０はそのＰＣＩＤを除去することができる。次いで、そのＰＣＩＤは、同じＰＣＩＤでプロビジョンされた別のＭ２ＭＥ（不図示）がコアネットワークにアタッチしようと試みるときに再利用することができる。ただし、第２のＭ２ＭＥのＰＣＩＤの有効期間は、概して前のＭ２ＭＥのＰＣＩＤの有効期間と重複すべきでない。

【００４８】

第１のＭ２ＭＥ１１０が、ＰＣＩＤを再び必要とすることがなくなった後、Ｍ２ＭＥ１１０にとっての適切な有効期間が切れるまで、典型的にはそのＰＣＩＤを新たなＭ２ＭＥに再発行しなくてよい。

【００４９】

別の実施形態では、ＰＣＩＤを、（ＰＣＩＤの同時使用なしに）系統的に再割当することができる。この系統的再割当は、Ｍ２ＭＥ１１０のライフサイクルに及ぶことができる。限られた数のＰＣＩＤを、Ｍ２ＭＥ１１０に系統的に事前にプロビジョンすることができる。この系統的再割当は、ＴＲＥ２３０の能力を活用しながら、初期ネットワーク接続性の自律管理を可能にすることができる。Ｍ２ＭＥは、サイズＮのグループでリリースされると想定される。ｊ番目のロットのＭ２ＭＥは、Ｍ＿ｉ，ｊと称し、ただし、ｊ＝１，．．．，Ｍである。ＰＣＩＤの割当は、サイズＮｘＭの行列（Ｐ）＿｛ｉ，ｊ｝を用いて

初期化することができる。Ｍ２ＭＥ１１０　Ｍ＿ｉ，１は、製造中に列Ｐ＿ｉ，*がＴＲＥ２３０にロードされる。このＭ２ＭＥがリリースされるとき、セキュアタイマまたは単調カウンタが初期化され、アクティブにされ、ＴＲＥ２３０の制御下に置かれる。ロット１のＭ２ＭＥ１１０、すなわちＭ＿ｉ，１は、初期化された時間またはカウンタに基づいて、確定した期間Ｔまたは所定回数にわたり、Ｐ＿ｉ，１を使用する。その所与の時間（有効期間）の後、これらＭ＿ｉ，１のＴＲＥは、Ｐ＿ｉ，１を破棄し、Ｐ＿ｉ，２を使用する。この期間または使用回数は、第２のロットがまだリリースされていないようになされるべきであることに留意すべきである。リリースされると、第２のロットＭ＿ｉ，２もＰ＿ｉ，１を使用し始め、そのＰ＿ｉ，１はこの時点ではＭ＿ｉ，１によって解放されている。理想的には、ＭｘＴが、ネットワークによってサポートされる必要があるすべてのＭ２ＭＥの全動作時間に及ぶ。

【００５０】

この実施形態は、デバイスが寿命サイクルのどこにあるのかを、ネットワークが判断できるようにすることができる。前のＰＣＩＤは、新たなデバイスに安全に再割当することができる。この方式は、Ｍ２ＭＥ製造業者のＴＲＥ２３０との本質的信頼関係を活用する。ＴＲＥ２３０が、ＴＲＥ２３０内のＰＣＩＤ列ベクトルを処理し、時間制限を実施することは、ＰＣＩＤの同時使用を防ぎ、Ｍ２ＭＥ１１０が、その動作時間の間中使用するための有効なＰＣＩＤを有するという確信をＰＬＭＮオペレータに対して与える。

【００５１】

ただし、ネットワークオペレータは、製造プロセスの特定の時点においてこのＰＣＩＤの組を製造業者に送り、またはこのＰＣＩＤの組をリリース前にセキュアな機能実装にインストールすることができるので、この実施形態はネットワークオペレータに影響を与える場合がある。さらに、これらのＭ２ＭＥは、複数のＰＣＩＤで事前にプロビジョンすることができる。これらのＭ２ＭＥは、後のロットのＰＣＩＤを再プロビジョニングすることをサポートできる。任意の所与の時点において同じロットのＰＣＩＤを共有する複数のＭ２ＭＥには、２つ以上のＭ２ＭＥが同じロットから同じＰＣＩＤを選択し、同時に接続しようと試み、結果的に「ＰＣＩＤの衝突」をもたらすことがある、「偶然の」衝突があり得る。ＰＣＩＤが衝突する可能性は、ロットのサイズ（行のサイズＮ）を、同じロットのＰＣＩＤを使用するＭ２ＭＥの数よりもはるかに大きくし、使用するＰＣＩＤをＭ２ＭＥがランダムに選択する場合、より小さくなる可能性がある。

【００５２】

時間制限付きのＰＣＩＤを管理するには、Ｍ２ＭＥの内部クロックを所与の精度限界の範囲内で同期する必要がある。この同期は、例えば単一のＭ２ＭＥ１１０の電源切断イベントであって、その後再同期が必要となり得る、電源切断イベントに及ぶ必要がある。したがって、ＴＲＥ２３０は時間基準を保持／管理し、ネットワーク内の信頼できる時間源との同期をサポートすべきである。オプションで、ＴＲＥ２３０は、図２に示すようにＭ２ＭＥ１１０内に位置する信頼できる時間源に依拠することができる。

【００５３】

Ｍ２ＭＥ１１０は、ＧＰＳ２３５などの自律型地理測位機器を備えることができる。Ｍ２ＭＥ１１０のＴＲＥ２３０は、その地理測位機器に安全にアクセスできる。

【００５４】

Ｍ２ＭＥ１１０は、様々な領域に分散し、２つのＭ２ＭＥが、同じアクセスネットワーク（ＡＮ）セルまたは基地局に対して同時に無線接続を物理的に確立できないように構成することができる。したがって複数のＭ２ＭＥは、同じＰＣＩＤだけでなく、目的地理位置（Ｄ）および許容差範囲（ｒ）でも事前にプロビジョンすることができ、目的地理位置（Ｄ）は各Ｍ２ＭＥにとって固有のものである。このデータは、ＴＲＥ２３０の中に安全に記憶し、またはＴＲＥ２３０しかこのデータにアクセスできないように、暗号を使用して保護することができる。

【００５５】

Ｍ２ＭＥ１１０が初期ネットワークアクセスを試みる前に、ＴＲＥ２３０が現在の地理

位置を求め、その地理位置が許容差範囲ｒの範囲内で位置Ｄに一致するかどうかを検査する。一致する場合、ＴＲＥ２３０は、初期ネットワークアクセスのためのＰＣＩＤをリリースする。このようにしてＡＮは、２つのＭ２ＭＥが同じＰＣＩＤを使用し、同じセルを介してアクセスしようと試みないと確信することができる。

【００５６】

それでもなお、一部の事例では、同じＰＣＩＤを使用した互いに異なるセルからの同時アクセスの試みを、ＡＮが見分ける必要があり得る。したがってこのＡＮは、初期ネットワーク接続性サービス内の（ＰＣＩＤ、セルＩＤの）対の記録を取らなければならない場合がある。したがってこの場合、コアネットワークに対していくらかの影響があり得る。

【００５７】

代替的実施形態では、Ｍ２ＭＥ１１０によるネットワークへのアクセスは、所定のネットワークセルを介してのみ許可される。所定のネットワークセルは、Ｍ２ＭＥのＴＲＥ内にロードされる、それらのセルのネットワークセル識別子によって識別される。それらのネットワークセル識別子は、対（Ｄ、ｒ）に取って代わる。

【００５８】

さらに別の代替的実施形態では、Ｍ２ＭＥを地理的に移動させることができる。Ｍ２ＭＥ１１０を移動させるとき、ネットワークアクセスは無効にされる。Ｍ２ＭＥの移動性を有効にするために、特定のＰＣＩＤを使用することができる様々な場所を示す１組の三つ組（ＰＣＩＤ、Ｄ、ｒ）で、Ｍ２ＭＥ１１０を事前にプロビジョンすることができる。Ｍ２ＭＥ１１０が初期ネットワーク接続を試みる前に、ＴＲＥ２３０は、現在の地理位置が目的Ｄのうちの１つの、範囲ｒのうちの１つの範囲内にあるかどうかを検査し、成功の場合は対応するＰＣＩＤをリリースする。

【００５９】

さらに、（ＰＣＩＤ、Ｄ、ｒ）の三つ組に、寿命、すなわち上記のように使用し実施する、許容使用期間を割り当てることができる。資格証明は、五つ組（ＰＣＩＤ、Ｄ、ｒ、ｔ１、ｔ２）をなし、ただしｔ１およびｔ２は、有効期間の開始時間および終了時間を指定する。この五つ組は、Ｍ２ＭＥ１１０の許容された移動についての経路を示す。例えば、Ｍ２ＭＥ１１０の移動は、車両内などの移動導入シナリオにおいて制御することができる。Ｍ２ＭＥのＴＲＥ２３０が頻繁に再接続することを強いられ、またさもなければＰＣＩＤを使用することを強いられる場合、ネットワークサービスが（時間切れの形で）障害を検出し、そのＭ２ＭＥ１１０が確定経路から離れているとして解釈し、したがってアラームを引き起こす可能性がある。

【００６０】

上記の方法および機器は、Ｍ２ＭＥ１１０の寿命全体にわたり、Ｍ２ＭＥ１１０の移動性および／またはＰＣＩＤ管理要件に対応するのに不十分な場合がある。したがって、五つ組（ＰＣＩＤ、Ｄ、ｒ、ｔ１、ｔ２）を管理する、すなわち再プロビジョン／削除するための方法が望ましい。

【００６１】

そのような五つ組は、ＰＣＩＤ更新サービス（ＰＵＳ）を使用して再プロビジョンすることができる。ＰＵＳは、自らが更新する、（Ｍ２ＭＥ１１０に一意に対応する）ＴＲＥ２３０を識別することができる。このＰＵＳは、ネットワーク内のＣＣＩＦサービスの一部、または別個の構成要素とすることができる。その更新は、１つまたは複数の五つ組（ＰＣＩＤ、Ｄ、ｒ、ｔ１、ｔ２）への変更を含むことができる。ＴＲＥ２３０の識別（ＩＤ）は、ＴＲＥのＩＤを現在のネットワーク（ＩＰ）アドレスに関連させることができるネットワークサービスに送信することができる。例えば、ネットワークエンティティは、完全なネットワーク接続性を得る過程でＴＲＥ２３０およびＭ２ＭＥ１１０の完全性を検証したＰＶＡ１５０、またはＰＶＡ１５０と連携してＭ２ＭＥ１１０の有効性を確認し、新たな１つまたは複数のＰＣＩＤを発行し、その新たな１つまたは複数のＰＣＩＤをＭ２ＭＥ１１０に遠隔的にプロビジョンする接続資格証明発行機能（ＣＣＩＦ）とすることができる。この遠隔プロビジョニングは、ネットワーク内のＤＰＦ１７０に委ねることもで

きる。

【００６２】

この再配置手順は、ＰＵＳが目標のＭ２ＭＥ１１０およびＴＲＥ２３０に接続し、例えば以下に説明し、図３～図５に示すプラットフォーム検証手順により、その状態の検証を要求するときに開始する。この手順は、ＴＲＥ２３０が以前の五つ組（ＰＣＩＤ、Ｄ、ｒ、ｔ１、ｔ２）（の組）を安全に破棄し、所望の新たな五つ組をインストールすることをＰＵＳに知らせることができる。検証が成功し次第、ＰＵＳは新たな五つ組（ＰＣＩＤ、Ｄ、ｒ、ｔ１、ｔ２）、および破棄すべき以前の五つ組のリストを送ることができる。ＴＲＥ２３０は、その新たな五つ組を自律的にインストールし、（継続的接続性を確保するため）以前の五つ組を破棄する。

【００６３】

別の実施形態では、ＴＲＥ２３０は、ＰＣＩＤに付加して衝突を軽減できる、（擬似）乱数を作成することができる場合がある。これらの追加情報を追跡し、見分ける能力をＡＮに与えることができる。

【００６４】

通信エンティティは、Ｍ２ＭＥ１１０、ＴＲＥ２３０、およびネットワークアクセスポイント（ＮＡＰ）（不図示）である。このＮＡＰは、例えばＶＮＯ１１５に関連するｅＮｏｄｅＢ（ｅＮＢ）とすることができる。ＴＲＥ２３０は、単一の初期ネットワーク接続試行で使用する乱数（ＲＡＮＤ）を生成する。ＴＲＥ２３０は、ＲＡＮＤが例えば第２のパラメータ、必要に応じて追加データ（Ｄ１）、およびＰＣＩＤに入る、鍵付きハッシュ関数などの完全性保護方法を適用する。ＴＲＥ２３０は、このデータを次のように送信する：ＴＲＥ→ｅＮＢ：ＲＡＮＤ｜｜ＰＣＩＤ｜｜Ｄ１｜｜Ｍ１：＝ＭＡＣ（ＰＣＩＤ｜｜Ｄ１，ＲＡＮＤ）。

【００６５】

このｅＮＢは、ＭＡＣ（メッセージ認証コード）を検証し、ペイロードデータ（Ｄ２）および受信データから返信パッケージを次のように構築し、ＴＲＥに送信する：ｅＮＢ→ＴＲＥ：Ｄ２｜｜Ｍ２：＝ＭＡＣ（ＰＣＩＤ｜｜Ｄ２，Ｍ１。

【００６６】

この方法は、初期ネットワーク接続において交換されるすべての後続のメッセージに及ぶ。後続のメッセージ交換は、任意の新たなメッセージ要素を含むデータ要素のＭＡＣ、および直前の交換のＭＡＣを含む。このｅＮＢおよびＴＲＥ２３０は、新たなM_nを構築するための最終値M_{n-1}を使用してこの通信中にメッセージを区別することができる。

【００６７】

この通信に対する中間者型攻撃を回避する目的で、通信当事者を認証するために、あらかじめ決められた秘密または取り決められた／共有された秘密をメッセージに含めることができる。

【００６８】

ＰＣＩＤ本体（ｐｒｏｐｅｒ）をＭＡＣ値に含めることはオプションだが、ハッシュ表を構築し、異なるＰＣＩＤおよび／または共通のＰＣＩＤを備える複数のＭ２ＭＥの、同時にアクティブなネットワーク接続試行を効率的に見分けるために有利であり得る。これは、セキュリティ問題となり得る、初期ネットワーク接続通信のすべてのメッセージ内で（おそらく平文の）ＰＣＩＤを送信することを防ぐことができる。

【００６９】

このｅＮＢは、ＰＣＩＤを使用する、すべての同時にアクティブなネットワークアクセス試行（本明細書では以下、チャネルと呼ぶ）の状態を表す表を保つことができる。各チャネルごとに、このｅＮＢは表１の情報を含む。

【００７０】

【表１】
表１

ＰＣＩＤの索引	アクティブハッシュ値	データ履歴
Ｉ	M_2	ＲＡＮＤ，D_1，D_2

【００７１】
１列目は、すべてのチャネルにわたり現在アクティブなすべてのＰＣＩＤのリスト内の一項目を指し示す、この特定のチャネルに属するＰＣＩＤの索引を含み、ＰＬ：＝［ＰＣＩＤ１，．．．ＰＣＩＤＮ］である。この索引は上記の表についてメモリを節約するが、メモリが問題にならない場合、この列は完全なＰＣＩＤを含むことができる。
【００７２】
このｅＮＢは、次のようにチャネル上で第３のメッセージを受信する。
【００７３】
ＴＲＥ→ｅＮＢ：　Ｄ３｜｜Ｍ３：＝ＭＡＣ（ＰＣＩＤ｜｜Ｄ３，Ｍ２）
【００７４】
ｉ＝１，．．．，Ｎにわたり、ｅＮＢは、次の手順が成功するまで、$PCID_i$をＰＬから選択する。最初のセルにＰＣＩＤの索引Ｉが含まれるすべての表の行に対し、ｅＮＢはM：＝ＭＡＣ（$PCID_i$｜｜D_3，M_2）を計算し、M_2はその行の２番目のセルから取る。$M=M_3$の場合、成功状態に達し、この検索手順は終了する。最後に受信した第３のメッセージに対応するチャネルの行番号を返す。データ履歴にD_3が追加され、選択された表の行のアクティブハッシュ値のセル内で、M_3がM_2に取って代わる。このプロセスは、後続のすべての通信ステップに関して繰り返す。
【００７５】
あるいは、第１のメッセージの後のメッセージは、ＰＣＩＤの代わりにチャネルの索引Ｉを含んで、後続メッセージの関連チャネルをより一層効率的に見つけることができる。
【００７６】
Ｍ２ＭＥ１１０および／またはｅＮＢの資源、特にメモリが限られている場合、アクティブなＰＣＩＤをロックすることができる。これは、Ｍ２ＭＥ１１０がロック済みのＰＣＩＤを使用するのを防ぐことにより、有利であり得る。
【００７７】
例えば、Ｍ２ＭＥ１１０が、あるＰＣＩＤに関してｅＮＢとのチャネルを開いた。その第１のチャネルが依然として開いている間、第２のＴＲＥ（不図示）を備える第２のＭ２ＭＥ（不図示）が、同じＰＣＩＤを使用してそのｅＮＢへのチャネルを開こうと試みる。このｅＮＢは、M_1を伝送することにより、第２のＭ２ＭＥのＴＲＥの第１のメッセージに応答することができる。したがって第２のＴＲＥには、このＰＣＩＤが現在占有されていることが知らされる。この第２のＴＲＥは、チャネルを開設する別の試みに関し、インストール済みＰＣＩＤのプールからの別のＰＣＩＤを使用することができ、または所定の期間待機してから同じＰＣＩＤを再び使用することができる。
【００７８】
あるいは、関与するエンティティが、ＰＣＩＤをアクティブに割当解除することができる。このＭ２ＭＥのＴＲＥ２３０は、完全なネットワーク接続性を得るためにあるＰＣＩＤが使用されている場合（すなわち永久資格証明がダウンロードされた後）、その使用済みＰＣＩＤを破棄することができる。このＰＣＩＤの破棄は、様々なイベントが引き起こすことができる。例えばこのＰＣＩＤの破棄は、完全なネットワーク接続性を保証するためのプロトコルを成功裏に実行することなどにより、ＴＲＥ２３０が完全なネットワーク接続性が保証された状態に達する場合にトリガすることができる。このＰＣＩＤの破棄は、有効期間が切れた場合、ｅＮＢ、セキュリティゲートウェイ、もしくは専用ＰＣＩＤ管理エンティティなどのネットワークエンティティが破棄を強制する場合、または、ＶＮＯ１１５を介したＭ２ＭＥ１１０へのセキュアな接続を確立し得る、Ｍ２ＭＥ１１０の製造

業者などのネットワーク外エンティティが破棄を強制する場合にトリガすることができる。

【００７９】

どのイベントが破棄をトリガするのかに関係なく、そのイベントに関する情報を使用してそのＰＣＩＤを適切に割当解除する、つまり、そのＰＣＩＤを他のＭ２ＭＥが再利用するために解放することができる。この割当解除イベントを信号で伝えるため、ＴＲＥ２３０からＭ２ＭＥの製造業者への接続を確立することができる。その製造業者は、解放されたＰＣＩＤの現行リストを更新することができ、それらのＰＣＩＤを再利用し、リリース時に新たなＭ２ＭＥ上にＰＣＩＤを付与することができる。

【００８０】

あるいは、例えばあるＳＨＯから別のＳＨＯへの加入変更の開始時の、将来の接続性操作を容易にするために、ＥＳ、既存のＳＨＯ１４０、不図示の新たなＳＨＯ、またはＩＣＦ１６０などのネットワーク内のエンティティを、ＰＣＩＤを更新するように構成することができる。Ｍ２ＭＥ１１０がプロビジョンされると、新たなＳＨＯとのサービスをプロビジョニングすることを助ける際に将来使用するために、初期ネットワークアクセス資格証明、ＰＣＩＤの更新された値をＭＩＤとしてＭ２ＭＥ１１０に送ることができる。この資格証明は、Ｍ２ＭＥ１１０のＴＲＥ２３０において抽出され、記憶され、排他的に使用される。

【００８１】

ＳＨＯを変更することに起因する資格証明の再プロビジョニングプロセスの前に、Ｍ２ＭＥ１１０の既存の初期ネットワークアクセス資格証明、ＰＣＩＤが失効したか、または失効しそうであることを、Ｍ２ＭＥ１１０に知らせることができる。Ｍ２ＭＥ１１０は、Ｅ／Ｓ、既存のＳＨＯ１４０、新たなＳＨＯ、またはＩＣＦ１６０に新たな初期ネットワークアクセス資格証明を要求し、受け取ることができる。あるいは、Ｍ２ＭＥ１１０が初期状態から新たな初期ネットワークアクセス試行を行うときに、新たなＰＣＩＤがＭ２ＭＥ１１０を新たなＳＨＯまで経路指定できるように、Ｍ２ＭＥ１１０は、Ｅ／Ｓまたはその新たなＳＨＯから供給されるこれらのネットワーク要素の１つから新たなＰＣＩＤを受け取ることができる。

【００８２】

一実施形態では、Ｍ２ＭＥ１１０は、Ｕ（Ｉ）ＳＩＭアプリケーション、ＰＣＩＤ、および１度に１つのアクティブな組を使用すべき、複数組のＡＫＡルート秘密で事前構成することができる。ＰＣＩＤの変更時に、Ｍ２ＭＥ１１０は、次の組のＡＫＡ資格証明を使用するように指示され、そのためこれらのＡＫＡ資格証明を使用してＭ２ＭＥ１１０に３ＧＰＰ接続性を提供し、そうしてオペレータの変更および新たなＳＨＯへの加入の再プロビジョニングを容易にすることができる。

【００８３】

上記の内容は、初期ネットワークアクセス資格証明を置換し、サービスを再プロビジョニングするための可能な方法のごく一部を説明したに過ぎない。すべての割当解除プロセスにおけるセキュリティ上の配慮は、割当解除プロセスにおいてＰＣＩＤを平文で転送しないことを要求することに留意すべきである。さらに、すべての割当解除プロセスに関し、割当解除プロセスにおいて通信相手を認証すべきである。

【００８４】

ＴＲＥ２３０またはＭ２ＭＥ１１０の信頼状態、ならびに関連するデータおよび資格証明の検証または認証を行うことに関し、３つの本質的に異なる可能性がある。その可能性には、次のものが含まれ、それはつまり：（１）自律的検証、（２）半自律的検証、および（３）遠隔的検証である。そのそれぞれを、図１に示すアーキテクチャを参照して以下により詳細に論じる。

【００８５】

自律的検証とは、Ｍ２ＭＥ１１０が自らをネットワークにアタッチできるようにする前に、Ｍ２ＭＥ１１０の内部検証が生じているとみなされる手順である。

【００８６】
半自律的検証とは、Ｍ２ＭＥ１１０の有効性が、外部ネットワークエンティティに依拠せず、Ｍ２ＭＥ１１０自体の内部で評価される手順である。そのような検証の結果、およびＴＲＥ２３０の認証をＭ２ＭＥ１１０の有効性に結合する所要の根拠は、ＰＶＡ１５０などの遠隔エンティティに信号で伝えられ、そのエンティティは、Ｍ２ＭＥ１１０からのメッセージの内容に基づいて判断を行う。Ｍ２ＭＥ１１０からＰＶＡ１５０へのこの信号伝達は保護すべきである。
【００８７】
遠隔的検証は、外部ネットワークエンティティ（例えばＰＶＡ１５０）が、Ｍ２ＭＥのＴＲＥ２３０が生成した検証用の根拠、ならびにＴＲＥ２３０とＭ２ＭＥ１１０との間の結合の根拠を受け取った後、Ｍ２ＭＥ１１０の有効性／完全性を直接評価する手順で構成される。遠隔的検証のために、Ｍ２ＭＥ１１０とＰＶＡ１５０との間で行われるこの通信は保護すべきである。
【００８８】
ＴＲＥ２３０が、Ｍ２ＭＥ１１０の完全性についての自律的検証を行う場合、この検証の直接的根拠は外部に提供されない。外部は、Ｍ２ＭＥおよびＴＲＥが指定され、実装される方法が原因で、その内部完全性検査に失敗するＭ２ＭＥ１１０は、自らをネットワークにアタッチし、または遠隔エンティティへの認証済み接続を得ることを、自らのＴＲＥ２３０によって妨げられるとみなす。例えば、セキュアブートプロセスは、Ｍ２ＭＥ１１０内のコードを安全に持ち出すことを容易にするが、この目的を果たす機器に依拠する場合以外、対外的な信号伝達はない。
【００８９】
図３は、Ｍ２ＭＥ１１０の完全性を検証するために、ＴＲＥ２３０が行う自律的検証手順３００の一例を示す。
【００９０】
まず３１０で、ＴＲＥ２３０は、自らがセキュア始動（ｓｅｃｕｒｅ　ｓｔａｒｔ－ｕｐ）の定義済み状態に達しているかどうかを検査する。次に３２０で、ＴＲＥ２３０は、セキュア始動を必要とするＭ２ＭＥ１１０の残りの定義済み部分が、セキュア始動の定義済み状態に達しているかどうかを検査する。
【００９１】
次いで３３０で、ＴＲＥ２３０自体により、またはＴＲＥ２３０にとって外部にあるが、ＴＲＥ２３０が完全性を保護する、Ｍ２ＭＥ１１０内の測定構成要素により、さらなる検査を行うことができる。そのような後期検査では、Ｍ２ＭＥ１１０の残りの他の構成要素、構成、またはパラメータの完全性が、ロードされるとき、または開始されるとき、または他の定義済み実行時イベント時に、それらのイベントをこの測定構成要素が利用できる場合はいつでも、検査される。
【００９２】
最後に３４０で、ＴＲＥ２３０は、要求された認証手順にＭ２ＭＥ１１０が関与することを許可する。
【００９３】
自律的検証は、必要とされる対外的通信の観点から最も経済的な方法である。しかし、自律的検証は、ネットワークアクセス中または連続的接続段階の間、任意の外部エンティティが、ＴＲＥ２３０もしくはＭ２ＭＥ１１０の完全性を独立に評価することを認めない。つまり、ネットワークまたは他の通信相手によって捉えられるものとしてのＭ２ＭＥ１１０の信頼性は、単純なスマートカードベースの認証の場合のように、Ｍ２ＭＥのＴＲＥ２３０のセキュリティ特性の技術仕様のみに基づく。
【００９４】
したがって、ＴＲＥ２３０は、（例えばネットワークアクセス試行前の）自律的検証のすべてのイベントに応答し、検証プロセスおよびその結果のログを記憶することもできる。例えば、その記憶した測定ログおよびプラットフォーム構成レジスタ（ＰＣＲ）の値は

記憶し、Ｔｒｕｓｔｅｄ　Ｃｏｍｐｕｔｉｎｇ　Ｇｒｏｕｐ（ＴＣＧ）の原理を使用し、Ｍ２ＭＥ１１０の完全性を保護するために使用することができる。

【００９５】

この記憶したデータは、データが監査記録を構成するので、外部監査にも使用することができる。この監査データは、ＴＲＥ２３０内のまたはＴＲＥ２３０が保護する、安全な内部アーカイブに記憶されるため、そのような不正変更を検出可能でなしに、変更することはできない。その結果、データの完全性保護が実現される。

【００９６】

さらに、この監査データは、自律的検証が引き起こされた特定の目的（例えばネットワークアクセスプロトコルの実行の、特定のインスタンス）に結合される。この結合は、検証目的を一意に識別するデータを、監査データに含めることによって達成することができる。

【００９７】

例えば、アクセスプロトコル内に確立される、共有された秘密または資格証明を監査データに添付することができ、ＴＲＥ２３０は、その作成した１組のデータにデジタル署名を施してその１組のデータの完全性を保護することができる。その後、Ｍ２ＭＥ１１０から独立したエンティティが、その監査データを後の任意の時点において要求することができる。例えば、そのエンティティは監査データを周期的に要求して、前のネットワークアクセスイベントごとに、問題のＭ２ＭＥ１１０が信頼できるかどうかを確認することができる。次いで、ＴＲＥ２３０およびＭ２ＭＥ１１０の識別資格証明とともに、この根拠をネットワークアクセス試行に関するネットワーク側プロトコルに再照合し、ＴＲＥ２３０の識別および信頼性をさらに検証し、Ｍ２ＭＥ１１０の不正変更を検出することができる。

【００９８】

図４は、ＴＲＥ２３０が、Ｍ２ＭＥ１１０の完全性の半自律的検証を行うための手順４００を示す。この手順４００が開始すると、４１０で、ＴＲＥ２３０は、自らがセキュア始動の定義済み状態に達しているかどうかを検査する。次に４２０で、ＴＲＥ２３０は、セキュア始動を必要とするＭ２ＭＥ１１０の残りの定義済み部分が、セキュア始動の定義済み状態に達しているかどうかを検査する。次いで４３０で、ＴＲＥ２３０自体により、またはＴＲＥ２３０にとって外部にあるが、ＴＲＥ２３０が完全性を保護する、Ｍ２ＭＥ１１０内の測定構成要素により、さらなる検査を行うことができる。そのような後期検査では、Ｍ２ＭＥ１１０の残りの他の構成要素、構成、またはパラメータの完全性が、ロードされるとき、開始されるとき、またはこの測定構成要素が利用できる他の任意の定義済み実行時時間イベント時に検査される。

【００９９】

ＰＶＡ１５０などの遠隔エンティティは、Ｍ２ＭＥ１１０が半自律的検証テストを通過したことを間接的に知ることができる。ネットワークに対し、この検証の成果について明確な信号伝達がある。４４０で、この信号伝達はＴＲＥ２３０内から生じるべきであり、暗号を使用して保護されるべきである。さらにこの信号伝達は、ＭＩＤをダウンロードするのに必要な、Ｍ２ＭＥ１１０の認証より前に起こり、Ｍ２ＭＥ１１０のダウンロード目標である構成要素の完全性を確実にする。この信号伝達は、ＴＲＥの認証と実際の有効性検査に使用されるＭ２ＭＥ１１０内の資源との間の結合の根拠を含むこともできる。そのような根拠には、ＴＲＥ２３０およびＭ２ＭＥ１１０の証明を確立するためのさらなる情報を提供する、Ｍ２ＭＥ１１０からネットワークに送信されるトークンが含まれ得る。

【０１００】

図５は、ＴＲＥ２３０の完全性の半自律的検証に関する代替的手順５００を示す。この手順５００は、５１０で、ＰＶＡ１５０またはＳＨＯ１４０が、検証を周期的に行うようにＴＲＥ２３０に要求するときに開始する。この要求は、Ｍ２ＭＥ１１０が最初に登録された後に送信することができ、またはこの要求は、Ｍ２ＭＥ１１０がＳＨＯを相手に一番初めに認証された時点で送信することができる。

【０１０１】
あるいはこの要求は、ＰＶＡ１５０またはＳＨＯ１４０から、保護された運用保守（ＯＡＭ：Ｏｐｅｒａｔｉｏｎ　Ａｎｄ　Ｍａｉｎｔｅｎａｎｃｅ）メッセージとして周期的に送信することができる。「周期的再検証」の期間は相対的に長いが、それでもなお、ＳＨＯ１４０が検証の「新鮮さ」に関して安心できるようにするのに十分な短さのものとすることができる。
【０１０２】
次に５２０で、ＴＲＥ２３０が、その要求に基づいて検証手順を実行する。検証が成功すると、５３０で、ＴＲＥ２３０は、ＴＲＥ２３０が作成する、最後の検証がいつ行われたのかを示すタイムスタンプを含み得る検証応答メッセージをＰＶＡに送信する。あるいは、ＴＲＥ２３０は、周期的検証サイクルの現在のラウンドが失効する前に、最後の検証が行われたことを述べるメッセージを送信することができる。
【０１０３】
この検証の「成果」に関する明確な信号伝達はなく、規定された周期的検証が実際に行われたことを示す、認証要求の一部としての一定の間接的な指示のみがあることに留意すべきである。この指示は、この周期的検証が行われた日付または時間を含むことができる。
【０１０４】
図６は、Ｍ２ＭＥの完全性を遠隔的に検証するための手順６００の一例である。この手順６００を開始するために、６１０で、Ｍ２ＭＥ１１０は定義済みセキュア状態に向けて始動することができる。セキュア状態に達すると、６２０で、Ｍ２ＭＥ１１０は、プラットフォームの有効性の根拠をＴＲＥ２３０が生成することを要求することができる。次に６３０で、ＴＲＥ２３０は、Ｍ２ＭＥ１１０の残りから、そのような根拠を作成するために使用する材料を集める。例えばこの材料には、Ｍ２ＭＥ１１０内のセキュリティ上重要な実行可能コード、Ｍ２ＭＥのオペレーティングシステム（ＯＳ）の資格証明、機器ＩＤ等が含まれ得る。次いで６４０で、ＴＲＥ２３０は、Ｍ２ＭＥ１１０の検証用の根拠を生成し、完全性および／または機密性を得るために、それを暗号を使用して保護する。次に６５０で、ＴＲＥ２３０はその保護された根拠をＭ２ＭＥ１１０に渡す。６６０で、Ｍ２ＭＥ１１０はその保護された根拠をＰＶＡ１５０に転送する。
【０１０５】
その保護された根拠を受信すると、６７０で、ＰＶＡ１５０はその根拠を評価して、引き続きデバイス認証を実行させ、ＭＩＤをダウンロードさせるのに、そのＭ２ＭＥ１１０が十分信頼できるかどうかを判定する。
【０１０６】
オプションで、上述した手順の要素の一部を、ＭＩＤをダウンロードするのに必須のＭ２ＭＥ認証に使用するプロセスに、統合することができる。ＴＲＥ２３０とＰＶＡ１５０との間のこの通信は、保護すべきであることに留意すべきである。
【０１０７】
上述した３つの検証手順のうちのいずれかを実行した後、Ｍ２ＭＥの検証と認証との間の結合が多くのシナリオにおいて望ましい。自律的検証の場合、検証はＭ２ＭＥ１１０のセキュア状態を立証する、Ｍ２ＭＥ１１０の何らかの証明書または資格証明とすることができる。他の検証手順の場合、検証はＭ２ＭＥ１１０のセキュア状態についての、より安全な証明手段を含むことができる。Ｍ２ＭＥのＴＲＥ２３０は、Ｍ２ＭＥ１１０の検証を行うために使用する、Ｍ２ＭＥの内部資源のセキュリティ特性を保証する高信頼環境なので、認証に使用される資格証明への検証の資格証明および／または成果の結合があるべきである。
【０１０８】
Ｍ２ＭＥ１１０を認証するための手順が３つある。第１に、初期ネットワーク接続性の必須条件として、ＩＣＦ１６０が初期状態のＭ２ＭＥ１１０を認証することができる。第２に、ＭＩＤ（例えばその資格証明を伴うＵＳＩＭアプリケーション）をダウンロードす

る必須条件として、認証されたＴＲＥ２３０をＭ２ＭＥ１１０が含むことを証明するために、ＤＰＦ１８０などのエンティティがＭ２ＭＥ１１０を認証することができる。第３に、（例えばダウンロードしたＭＩＤを使用する）操作上のネットワークアクセスのために、ＳＨＯ１４０がＭ２ＭＥ１１０を認証することができる。

【０１０９】

自律的検証は、上述の初期ネットワーク接続性に関して使用する認証手順に結合することができる唯一のタイプの検証である。上述した残りの２つの検証方法はＰＶＡ１５０が関与することを必要とするが、初期接続性はなく、Ｍ２ＭＥ１１０が検証にＰＶＡ１５０を関与させることはできない。

【０１１０】

初期ネットワーク接続性に関し、自律的検証では、ネットワークアタッチメントが生じる後まで、完全性／有効性についてのネットワークベースの検査は行われないので、ネットワークアクセス認証への完全性／有効性の結合は単に暗示的に過ぎないことがある。残りの２つの形態の検証に関しては、Ｍ２ＭＥ１１０内のＴＲＥ２３０識別、したがってＴＲＥ２３０のセキュリティ機能およびＭ２ＭＥ１１０の完全性についてのさらなる情報を提供するトークン（ＴＲＥ２３０の資格証明および証明を立証するデジタル証明書など）を、初期アタッチメントメッセージ内で渡すことができる。

【０１１１】

操作上の接続性では、半自律的検証ならびに遠隔的検証があり得る。さらに、後続の認証ステップへのそのような検証方法の結合があり得る。プラットフォーム検証と認証との結合を果たすための２つの方法を以下に説明する。

【０１１２】

第１に、Ｍ２ＭＥ１１０への、認証資格証明を保持するＴＲＥ２３０の論理的結合があり得る。認証の間、デバイスプラットフォームの完全性が検証される。論理的結合についての以前の解決策（例えばＳＩＭロック）はすぐに回避されていることに留意すべきである。しかしＴＣＧなど、成功裏に適用し得る他のより新しい方法体系がある。

【０１１３】

第２に、Ｍ２ＭＥ１１０への、ＴＲＥ２３０の物理的結合があり得る。ＴＲＥ２３０の認証の間、デバイスプラットフォームの完全性が検証される。

【０１１４】

上記のいずれの場合にも、プラットフォーム資源の実際の検証は、Ｍ２ＭＥ１１０に安全に埋め込まれたハードウェアセキュリティ構成要素（すなわち埋め込まれたＴＲＥ）の機能を使用することにより、またはＴＲＥ２３０の外側にあるが、ＴＲＥ２３０がそのセキュリティ特性を保証することができ、ＴＲＥ２３０に安全に接続することができる、そのようなハードウェアセキュリティ構成要素を使用することによって実行されるべきである。３ＧＰＰ　ＡＫＡ認証に使用する資格証明およびアプリケーションは、ホスティングデバイス内のセキュアハードウェア構成要素の結合を検証する目的で設計されていないことに留意すべきである。

【０１１５】

検証および認証のステップは、共通プロトコルのセッション内で組み合わせることができる。例えば３ＧＰＰは、デバイスおよびホスティング当事者の認証ステップを組み合わせるための方法としてＩＫＥｖ２を使用する。同じプロトコルを、組み合わせられた検証／認証手順で使用するために考慮することもできる。

【０１１６】

図７は、アクセスが認証された場合の、ＭＩＤをＭ２ＭＥ１１０にプロビジョニング／再プロビジョニングするための、第１の手順７００の例を示す。この手順は例証目的で提供するが、同様の結果を伴う、ネットワークエンティティ間の他の対話も可能である。図７では、矢印が、各機能、サービスプロバイダ、および検証局間の接続を示す。実線の矢印は、Ｍ２ＭＥ１１０からＶＮＯ１１５への初期ネットワークアクセスのためのエアインターフェイスを示し、破線矢印は、ＶＮＯのネットワークが提供するエアインターフェイ

スを介した、Ｍ２ＭＥ１１０とＩＣＦ１６０との間の接続を示し、点線矢印は、ＶＮＯのネットワークのエアインターフェイスならびにＩＣＦ１６０が提供するＩＰ接続性を介した、Ｍ２ＭＥ１１０とＤＰＦ１８０、ＤＰＦ１７０およびＰＶＡ１５０との間の接続を示す。ＩＣＦ１６０、ＤＲＦ１７０、およびＤＰＦ１８０をすべて個別のエンティティとして示すが、図１に示すようにそれらを単一のエンティティ内に、または本質的に同じ機能を果たす他の何らかの仕組みの中に配置できることも当業者なら理解されよう。

【０１１７】

図７の手順７００では、Ｍ２ＭＥ１１０へのＭＩＤのダウンロードおよびプロビジョニングは、Ｍ２ＭＥ１１０がその初期ネットワークアクセスにおいて３Ｇ　ＶＮＯのネットワークにアクセスするときに生じることができる。ＶＮＯ１１５は以下の手順により、Ｍ２ＭＥ１１０にエアインターフェイスを提供する。

【０１１８】

Ｍ２ＭＥ１１０は、例えば標準ＧＳＭ／ＵＭＴＳ原理（ＧＰＲＳ／ＰＳ）を使用してネットワーク情報を復号し、アタッチメッセージを使用してＶＮＯ１１５のネットワークにアタッチすることができる。７０１で、Ｍ２ＭＥ１１０は、アタッチメッセージ内で仮のＭ２ＭＥ　ＩＤまたはＰＣＩＤをＶＮＯ１１５に送信し、ＶＮＯ１１５が、標準ＵＭＴＳ　ＡＫＡ手順によりＭ２ＭＥ１１０を認証する。そのＰＣＩＤの内容および構造は、ＶＮＯ１１５がそのＰＣＩＤをＩＭＳＩとして認識するようなものである。

【０１１９】

ＶＮＯのネットワークに初期アタッチメントするためのクライアント認証を実行できるためには、Ｍ２ＭＥ１１０が、すべてのＭ２ＭＥおよびＶＮＯ１１５によって共有される、Ｍｉｌｅｎａｇｅアルゴリズムなどの認証アルゴリズムをサポートする必要があることに留意すべきである。

【０１２０】

７０２で、そのＰＣＩＤをＭ２ＭＥ１１０のＩＤとして認識するＶＮＯ１１５は、そのＰＣＩＤを正当な予備資格証明として承認するＩＣＦ１６０に接触する。次いで７０３で、ＩＣＦ１６０は、Ｍ２ＭＥ１１０とのさらなる通信を保護するための１組の予備認証ベクトル（ＡＶ）を発行し、保護されたＩＰ接続性をＭ２ＭＥ１１０に提供し始める。この通信は、ＶＮＯのネットワークが提供するエアインターフェイスを使用して実行される。

【０１２１】

次に７０４で、Ｍ２ＭＥ１１０とＩＣＦ１６０とが標準ＡＫＡプロセスを実行し、予備ＡＫＡ鍵を作成してＭ２ＭＥ１１０からの／Ｍ２ＭＥ１１０への通信を保護する。その後、Ｍ２ＭＥ１１０がＳＨＯのＭＩＤ資格証明をダウンロードし、プロビジョニングした後にそれらを使用してネットワークに接続するまで、様々なネットワークエンティティへのＭ２ＭＥ１１０間のすべての通信は、ＶＮＯのネットワークが提供するエアインターフェイス、ならびにＩＣＦ１６０が提供するＩＰ接続性および暗号化保護を介して行われる。

【０１２２】

次いで、ＩＣＦ１６０が、Ｍ２ＭＥ１１０をＤＰＦ１８０に転送する。その際７０５で、ＩＣＦ１６０は、ＰＣＩＤをＤＲＦ１７０に送信することができる。次いで７０６で、ＤＲＦ１７０は、Ｍ２ＭＥ１１０がＳＨＯ１４０を探すのを支援する。次に７０７で、ＤＲＦ１７０が、ＳＨＯ１４０に接続し、ＳＨＯのネットワークへの接続に関してＭ２ＭＥ１１０を登録する。それに応答して７０８で、ＳＨＯ１４０が、Ｍ２ＭＥ１１０のＴＲＥ２３０の真正性および完全性を検証するようにＰＶＡ１５０に要求する。次いで７０９で、ＰＶＡ１５０が、Ｍ２ＭＥ１１０のＴＲＥ２３０の真正性および完全性を検証する。この検証手順は、図３～図５に関して上述した検証手順と同様の方法で実行することができる。

【０１２３】

検証完了時に、７１０で、ＰＶＡ１５０が検証結果をＳＨＯ１４０に送り返す。７１１で、ＳＨＯ１４０がＤＰＦ１８０に接触し、ＭＩＤ（ＵＳＩＭ／ＩＳＩＭアプリケーション）をＭ２ＭＥ１１０にプロビジョニングすることを許可する。

【０１２４】
次に７１２で、ＤＰＦ１８０が、ＭＩＤオブジェクトをＭ２ＭＥ１１０にダウンロードする。次いで７１３で、Ｍ２ＭＥ１１０が、ダウンロード済みＭＩＤをＴＲＥ２３０内にプロビジョンし、そのプロビジョニングの成功／失敗状態をＤＰＦ１８０に報告する。Ｍ２ＭＥ１１０は、そのようなメッセージを検証するために使用できるトークンを送信する必要があり得る。そのようなトークンは、不正変更およびリプレイ攻撃に耐性がある形式をなす必要がある。最後に７１４で、ＤＰＦ１５０が、プロビジョニングの成功／失敗状態をＳＨＯ１４０に折り返し報告する。
【０１２５】
図８は、アクセスが認証された場合の、ＭＩＤをＭ２ＭＥ１１０にプロビジョニング／再プロビジョニングするための、もう１つの手順８００を示す。この手順８００では、Ｍ２ＭＥ１１０へのＭＩＤのダウンロードおよびプロビジョニングは、Ｍ２ＭＥ１１０がその初期ネットワークアクセスにおいて３Ｇ　ＶＮＯのネットワークにアクセスするときに生じることができる。ＳＨＯ１４０が、自らのＭＩＤをダウンロードし、プロビジョニングすることを許可する前にＴＲＥ２３０の検証を行わせる代わりに、ＩＣＦ１６０は、仮認証ベクトルをＭ２ＭＥ１１０にリリースする前に、さらにＩＰ接続性をＭ２ＭＥ１１０に与える前に、Ｍ２ＭＥ１１０のＴＲＥ２３０を検証するよう、ＰＶＡ１５０に要求する。
【０１２６】
手順８００は、８０１で、Ｍ２ＭＥ１１０が、例えば標準ＧＳＭ／ＵＭＴＳ原理（ＧＰＲＳ／ＰＳ）を使用してネットワーク情報を復号し、ＶＮＯ１１５のネットワークにアタッチするときに開始する。Ｍ２ＭＥ１１０は、アタッチメッセージ内でＰＣＩＤをＶＮＯ１１５に送信する。ＶＮＯ１１５が、標準ＵＭＴＳ　ＡＫＡ手順によりＭ２ＭＥ１１０を認証する。
【０１２７】
８０２で、Ｍ２ＭＥ１１０のＰＣＩＤを認識するＶＮＯ１１５は、そのＰＣＩＤを正当な予備資格証明として承認するＩＣＦ１６０に接触する。次に８０３で、ＩＣＦ１６０が、Ｍ２ＭＥ１１０のＴＲＥ２３０の真正性および完全性を検証するようにＰＶＡ１５０に要求する。次いで８０４で、ＰＶＡ１５０が、Ｍ２ＭＥ１１０のＴＲＥ２３０の真正性および完全性を検証する。この検証は、前に述べた検証手順のうちの１つを使用して実行することができる。
【０１２８】
８０５で、ＰＶＡ１５０が検証結果をＩＣＦ１６０に送り返すと、８０６で、そのＩＣＦは、Ｍ２ＭＥ１１０とのさらなる通信を保護するための１組の予備認証ベクトル（ＡＶ）を発行し、保護されたＩＰ接続性をＭ２ＭＥ１１０に提供し始める。この通信は、ＶＮＯのネットワークが提供するエアインターフェイスを介して行われる。
【０１２９】
次に８０７で、Ｍ２ＭＥ１１０とＩＣＦ１６０とが標準ＡＫＡプロセスを実行し、予備ＡＫＡ鍵を作成してＭ２ＭＥ１１０からの／Ｍ２ＭＥ１１０への通信を保護する。その後、Ｍ２ＭＥ１１０がＳＨＯのＵ（Ｉ）ＳＩＭ資格証明をダウンロードし、プロビジョニングした後にそれらを使用してネットワークに接続するまで、様々なネットワークエンティティへのＭ２ＭＥ１１０間のすべての通信は、ＶＮＯのネットワークが提供するエアインターフェイス、ならびにＩＣＦ１６０が提供するＩＰ接続性および暗号化保護を介して行われる。
【０１３０】
８０８で、ＩＣＦ１６０が、Ｍ２ＭＥ１１０をＤＲＦ１７０に導く。その際、ＩＣＦ１６０は、ＰＣＩＤならびにＴＲＥの検証状態に関する情報をＤＲＦ１７０に送信する。８０９で、ＤＲＦ１７０は、Ｍ２ＭＥ１１０がそのＳＨＯ１４０を探すのを支援し、Ｍ２ＭＥ１１０をＳＨＯ１４０に転送する。次いで８１０で、ＤＲＦ１７０が、ＳＨＯ１４０に接続し、ＳＨＯ１４０への接続に関してＭ２ＭＥ１１０を登録する。その際、ＤＲＦ１７

０は、ＴＲＥの検証状態に関する情報もＳＨＯ１４０に伝える。
【０１３１】
ＤＲＦ１７０から受信したＴＲＥの検証状態情報を検討した後、８１１で、ＳＨＯ１４０がＤＰＦ１８０に接触し、ＭＩＤ（ＵＳＩＭ／ＩＳＩＭアプリケーション）をＭ２ＭＥ１１０内にプロビジョニングすることを許可する。それに応答して８１２で、ＤＰＦ１８０が、ＭＩＤ（Ｕ（Ｉ）ＳＩＭアプリケーションおよび資格証明）オブジェクトをＭ２ＭＥ１１０にダウンロードする。
【０１３２】
８１３で、Ｍ２ＭＥ１１０が、ダウンロード済みＭＩＤをＴＲＥ２３０内にプロビジョンし、そのプロビジョニングの成功／失敗状態をＤＰＦ１８０に報告する。Ｍ２ＭＥ１１０は、そのようなメッセージを検証するために使用できるトークンを送信することができる。そのようなトークンは、不正変更およびリプレイ攻撃に耐性がある形式をなすべきである。最後に、ＤＰＦ１８０が、プロビジョニングの成功／失敗状態をＳＨＯ１４０に折り返し報告する。
【０１３３】
図９は、新たなＳＨＯ（不図示）に対してＭ２ＭＥ１１０を再プロビジョニングするための、手順９００の流れ図の一例である。この手順９００は、９１０で、Ｍ２ＭＥの所有者が、新たなＳＨＯに接触してＭ２ＭＥのパラメータを転送するときに開始する。次いで９２０で、Ｍ２ＭＥの所有者が、Ｍ２ＭＥに接触して再プロビジョニング手順を開始する。
【０１３４】
９３０で、その新たなＳＨＯが、Ｍ２ＭＥ１１０を検証するように検証エンティティに要求する。次いで９４０で、ＰＶＡ１５０がＭ２ＭＥ１１０を検証し、成功／失敗メッセージをその新たなＳＨＯに送信する。９５０で、成功通知の受信時に、その新たなＳＨＯが、新たなＭＩＤ（すなわちＵＳＩＭアプリケーションおよび資格証明）をＭ２ＭＥ１１０にダウンロード／プロビジョンするよう、ＤＰＦに要求する。
【０１３５】
次いで９６０で、ＤＰＦ１８０が、新たなＭＩＤパッケージをＭ２ＭＥ１１０に安全にダウンロードする。９７０で、Ｍ２ＭＥ１１０が、以前のＭＩＤを破棄したというメッセージを以前のＳＨＯに送信する。次いで９８０で、以前のＳＨＯがＭ２ＭＥ１１０にＡＣＫを送信し、次いでＭ２ＭＥ１１０は、そのＡＣＫをＤＰＦ１８０に転送し、その後新たなＳＨＯに転送する。
【０１３６】
９９０で、Ｍ２ＭＥ１１０が、ＤＰＦ１８０の助けで自らのシステムを更新し、ＭＩＤをインストールし、ＤＰＦ１８０に成功／失敗メッセージを送り返す。９９２で、ＤＰＦ１８０が、その成功／失敗メッセージを新たなＳＨＯに報告する。９９８で、成功時に、このプロビジョニングプロセスは完了する。
【０１３７】
別の再プロビジョニング手順では、Ｍ２ＭＥ１１０を初期状態に置き、図７および図８に示す初期プロビジョニング手順と同じタイプのプロセスを再び開始することができる。
【０１３８】
別の実施形態では、ＰＶＡ１５０は、Ｍ２ＭＥ１１０が依然として同じＳＨＯ１４０に加入している間に実行される、任意のソフトウェア（ＳＷ）またはファームウェア（ＦＷ）の更新が、安全な方法で行われることを保証する役割を果たす。この保証することは、資格証明を更新しまたは再構成することを含む。
【０１３９】
これは、ＰＶＡ１５０またはＤＰＦ１８０が、ＳＷ／ＦＷの安全な無線（さらに有線）ダウンロードや、Ｍ２ＭＥ１１０および／またはＴＲＥ２３０の再プロビジョニングなどの手順を監督すべきであることを意味する。したがって、ＰＶＡ１５０またはＤＰＦ１８０は、安全なダウンロード、ＦＬＡＳＨ更新、および／またはＭ２ＭＥ１１０のデバイス

再構成に関し、ＯＭＡ　ＤＭおよびＯＭＡ　ＦＯＴＡ規格において提供される方法などの、利用可能な方法を使用することができる。

【０１４０】

さらに、このＭ２ＭＥの信頼状態情報は、遠隔ＳＷ／ＦＷ更新または再構成が原因で変わる可能性があるので、ＳＷ／ＦＷ更新または再構成の完了時に、ＰＶＡ１５０またはＤＰＦ１８０は、Ｍ２ＭＥ１１０またはＴＲＥ２３０の新たな検証可能ブートもしくは実行時信頼状態情報検査を開始し、その結果を得ることができるべきである。ＰＶＡ１５０またはＤＰＦ１８０はさらに、Ｍ２ＭＥ１１０に関する信頼状態情報についての自らのデータベースを更新すべきである。この遠隔ＳＷ／ＦＷ更新または遠隔資格証明再構成にＤＰＦ１８０が関与する場合、ＰＶＡ１５０がＭ２ＭＥ１１０の「信頼状態」情報についての自らのデータベースを更新することができるように、Ｍ２ＭＥ１１０に関する「信頼状態」情報に対するその更新／再構成の任意の予想効果を、ＤＰＦ１８０からＰＶＡ１５０に送信する必要がある。

【０１４１】

さらに、Ｍ２ＭＥ１１０の不正変更の検出、および不正変更に対する検出後の救済反応に関する解決策を開示する。Ｍ２ＭＥ１１０を不正変更攻撃に強くするため、いくつかの解決策を提案する。

【０１４２】

まず、Ｍ２ＭＥ１１０は、自らに、または自らの内部の１つまたは複数の任意のサブシステムに対して行われる特定のタイプの「不正変更」を、（定期的にスケジュールされた検出試行の場合は）十分に頻繁にかつ／または（イベント駆動型の検出試行の場合は）適時ベースで検出することができる機能を備えるように構成することができる。そのような検出可能な不正変更イベントの例には、（１）マルウェアまたはウイルスが、ＯＳを救済可能なおよび／または救済不可能な危険にさらすこと、（２）バッファオーバフローイベント、（３）無線もしくは上位層接続特性、および／または環境測定値の突然の予期せぬもしくは未承認の変化、（３）Ｍ２ＭＥの予備認証、登録、またはＭＩＤプロビジョニング要求に対し、信頼できるネットワーク要素がアクセスまたはサービスの失敗および／もしくは拒否を過度に繰り返すこと、または（４）Ｍ２ＭＥ１１０または遠隔ＭＩＤ管理機能に関係するＭ２ＭＥサブシステムの「信頼状態」の、ブート後または実行時読取り値の任意の予期せぬ／未承認の変化が含まれ得るが、これだけに限定されない。ＰＶＡ１５０、ＩＣＦ１６０などのネットワーク要素、または図１に示す他の任意のネットワーク要素も、不正変更を検出するように構成することができる。例えば、これらのネットワーク要素は、自らの機能および／またはＭ２ＭＥ１１０の機能を使用して、Ｍ２ＭＥ１１０に対して行われる特定のタイプの「不正変更」を遠隔的に検出するように構成することができる。さらに、これらのネットワーク要素は、任意の不正変更検出イベントについて報告するよう、Ｍ２ＭＥ１１０に要求するように構成することができる。

【０１４３】

自らに対する任意の不正変更を自己検出するとき、Ｍ２ＭＥ１１０は、自らに対する、または他のネットワーク要素に対するさらなる被害を抑えるための措置を講じるべきである。例えば、不正変更の検出時に、遠隔ＭＩＤ管理に関係する機能を無効にするようにＭ２ＭＥ１１０を構成することができる。Ｍ２ＭＥ１１０は、自らの内部資源（ＳＷや、ＯＳの特定の部分など）による、ＴＲＥ２３０など、Ｍ２ＭＥ１１０のあらかじめ指定された極めてデリケートな領域へのアクセス、またはＳＩＭおよび／もしくはＴＰＭ／ＭＴＭなど、遠隔ＭＩＤ管理に関係するデータ、コードまたは資格証明を保持する、Ｍ２ＭＥ１１０の他の部分へのアクセスを無効にするように構成することもできる。

【０１４４】

不正変更を自己検出するとき、Ｍ２ＭＥ１１０は、疑わしいまたは検出した不正変更イベント、ならびにＭ２ＭＥ１１０が取った検出後の自己救済アクションまたは反応アクションのイベントについての報告を、指定されたネットワーク要素（ＰＶＡなど）に送信するように構成することもできる。そのようなイベント報告はさらに、それらのイベントの

タイムスタンプ、または、Ｍ２ＭＥ１１０の最新のＧＰＳ読取り値や隣接セルのリストなど、それらのイベントの位置情報スタンプさえも含むことができることに留意すべきである。

【０１４５】

さらに、不正変更を検出するとき、Ｍ２ＭＥ１１０は、最近のＳＷ更新、または疑わしいウイルスもしくはマルウェアコードもしくはデータの削除、隔離、アンインストールなどの救済アクションを実行するように構成することができる。Ｍ２ＭＥ１１０は、一時記憶域（例えばＲＡＭ）および／または永続記憶域（例えばＮＶＲＡＭ、フラッシュ、ハードディスク、ＳＩＭ、ＴＰＭ／ＭＴＭ内部記憶領域または暗号化された記憶領域等）からの、ＵＳＩＭに関係する鍵や資格証明など、遠隔ＭＩＤ管理機能に関係する、任意のあらかじめ指定された１組のデータを削除するように構成することもできる。

【０１４６】

最後に、不正変更を検出するとき、Ｍ２ＭＥ１１０は、自らの、または遠隔ＭＩＤ管理機能を取り扱う端末の部分／サブシステムの電源を切るように構成することもできる。

【０１４７】

ＰＶＡ１５０などの特定のネットワーク要素も、Ｍ２ＭＥ１１０であって、（１）疑わしいまたは検出した不正変更イベントを報告しまたは（２）対話相手であったＰＶＡ１５０自体または他のネットワーク要素により不正変更イベントにあったと疑われている、Ｍ２ＭＥ１１０のために、遠隔「検出後」反応アクションを開始／実行する役割を果たし、それらを開始／実行する能力を有することができる。

【０１４８】

上述した機能および実施形態は、３Ｇ　ＵＭＴＳネットワークアクセスの認証に必要な認証プロトコル以外の認証プロトコルに適用可能である。そのようなプロトコルの例には、アプリケーション層認証に使用される汎用ブートストラッピングアーキテクチャ（ＧＢＡ）に準拠するプロトコル、およびＧＳＭ／ＵＭＴＳ端末の非３Ｇアクセスネットワークに対する認証のための、ＳＩＭ（ＥＡＰ－ＳＩＭ）に基づく拡張可能認証プロトコルが含まれ得るが、これだけに限定されない。例えば、図１に示すネットワーク要素は、識別の認証および遠隔管理ならびにサービス、アプリケーションもしくは（非３Ｇ）ネットワークアクセスについてのＭ２ＭＥデバイスの認証を可能にするために、存在し、同様のまたは同じ機能を実行することができる。

【０１４９】

諸特徴および要素を特定の組合せにより上記に記載したが、各特徴または要素を、他の特徴および要素なしに単独で、または他の特徴および要素を伴うもしくは伴わない様々な組合せで使用することができる。本発明で提供する方法または流れ図は、汎用コンピュータまたはプロセッサによって実行するためにコンピュータ可読記憶媒体中に実施されるコンピュータプログラム、ソフトウェアまたはファームウェアで実施することができる。コンピュータ可読記憶媒体の例には、ＲＯＭ（読出し専用メモリ）、ＲＡＭ（ランダムアクセスメモリ）、レジスタ、キャッシュメモリ、半導体記憶装置、内蔵ハードディスクやリムーバブルディスクなどの磁気媒体、光磁気媒体、およびＣＤ‐ＲＯＭディスクやＤＶＤ（デジタル多機能ディスク）などの光学媒体が含まれる。

【０１５０】

適切なプロセッサには、例えば汎用プロセッサ、専用プロセッサ、従来型プロセッサ、ＤＳＰ（デジタル信号プロセッサ）、複数のマイクロプロセッサ、ＤＳＰコアに関連する１個または複数個のマイクロプロセッサ、コントローラ、マイクロコントローラ、特定用途向け集積回路（ＡＳＩＣ）、書替え可能ゲートアレイ（ＦＰＧＡ）回路、他の任意のタイプの集積回路（ＩＣ）および／または状態機械が含まれる。

【０１５１】

ソフトウェアに関連するプロセッサを使用して、無線送受信ユニット（ＷＴＲＵ）、ユーザ機器（ＵＥ）、端末、基地局、無線ネットワークコントローラ（ＲＮＣ）、または任意のホストコンピュータで使用するための無線周波数トランシーバを実装することができ

る。ＷＴＲＵは、カメラ、ビデオカメラモジュール、テレビ電話、スピーカホン、振動デバイス、スピーカ、マイクロホン、テレビトランシーバ、ハンズフリーヘッドセット、キーボード、Ｂｌｕｅｔｏｏｔｈ（登録商標）モジュール、ＦＭ（周波数変調）無線ユニット、ＬＣＤ（液晶ディスプレイ）ディスプレイユニット、ＯＬＥＤ（有機発光ダイオード）ディスプレイユニット、デジタル音楽プレイヤ、メディアプレイヤ、ビデオゲーム機モジュール、インターネットブラウザ、および／または任意のＷＬＡＮ（無線ローカルエリアネットワーク）もしくはＵＷＢ（超広帯域）モジュールなど、ハードウェアおよび／またはソフトウェアによって実装されるモジュールと組み合わせて使用することができる。

【０１５２】

実施形態

１．機械対機械（Ｍ２Ｍ）通信を実行するための方法。

【０１５３】

２．通信には、認証、プロビジョニング、または再プロビジョニングのうちの１つもしくは複数が含まれることを特徴とする上記の実施形態に記載の方法。

【０１５４】

３．Ｍ２Ｍ対応機器（Ｍ２ＭＥ）において、訪問先ネットワークオペレータの（ＶＮＯの）ネットワークに接続するステップ

をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１５５】

４．選択ホームオペレータの（ＳＨＯの）ネットワークに接続するための許可を受けるステップ

をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１５６】

５．そのＳＨＯのネットワークに接続するステップ

をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１５７】

６．ＶＮＯは、単一のネットワークエンティティであることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１５８】

７．ＶＮＯには、複数のネットワークエンティティが含まれることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１５９】

８．ＶＮＯは、初期登録およびプロビジョニングのためにアクセスされる、任意のアクセスネットワークであることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１６０】

９．登録およびプロビジョニングには、ＵＳＩＭ／ＩＳＩＭアプリケーションの登録およびプロビジョニングが含まれることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１６１】

１０．Ｍ２ＭＥが、ＶＮＯではないＳＨＯに登録するステップと、

ＶＮＯがＶＮＯのままであるステップと

をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１６２】

１１．Ｍ２ＭＥが、ＶＮＯであるＳＨＯに登録するステップと、

ＶＮＯがＳＨＯになるステップと

をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１６３】

１２．ＶＮＯは、Ｍ２ＭＥに一時的なネットワークアクセスを提供する役割を果たすことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１６４】

１３．一時的なネットワークアクセスは、一時的ネットワークアクセス資格証明に基づくことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１６５】

１４．一時的ネットワークアクセス資格証明には、ＰＣＩＤまたは他の任意の一時的プライベートＩＤが含まれることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１６６】

１５．ＶＮＯは、発見および登録機能（ＤＲＦ）へのオープンネットワークアクセスを提供するステップ

をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１６７】

１６．少なくともＤＲＦのサービスへのアクセスに関しては、資格証明または認証は不要であることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１６８】

１７．ＶＮＯがＳＨＯになる場合、ＶＮＯはＤＲＦへのオープンネットワークアクセスを提供することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１６９】

１８．ＶＮＯは、プロビジョンしたＵＳＩＭ／ＩＳＭアプリケーションを使用して完全なネットワークアクセスを提供するステップ

をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１７０】

１９．完全なネットワークアクセスには、ＩＭＳが含まれることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１７１】

２０．ＲＯは、ＩＣＦ、ＤＲＦ、ならびにダウンロードおよびプロビジョニング機能（ＤＰＦ）のうちの１つまたは複数を含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１７２】

２１．ＩＣＦ、ＤＲＦ、およびＤＰＦは、個別のエンティティにそれぞれ位置することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１７３】

２２．ＩＣＦは、操作上のネットワークアクセスの登録およびプロビジョニングのために、通信ネットワークへの一時アクセスを許可する資格証明を検証する役割を果たすことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１７４】

２３．ＩＣＦが、一時的ネットワークアクセス資格証明を発行するステップ

をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１７５】

２４．ＩＣＦが、Ｍ２ＭＥに対して一時的プライベート識別子を発行するステップ

をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１７６】

２５．一時的ネットワークアクセス資格証明または一時的プライベート識別子は、認証済み初期一時的ネットワークアクセスに使用されることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１７７】

２６．ＩＣＦは、Ｍ２Ｍの鍵、構成、およびアプリケーションのうちの１つまたは複数でＭ２ＭＥをプロビジョニングするステップ

をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０１７８】

２７．プロビジョニングには、無線によるプロビジョニングが含まれることを特徴とす

る上記の実施形態のいずれか１つに記載の方法。
【０１７９】
２８．Ｍ２ＭＥを事前構成するために、ＩＣＦが機器サプライヤ（Ｅ／Ｓ）に資格証明を提供するステップ
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０１８０】
２９．資格証明をＭ２ＭＥに埋め込む役割を果たす組織に対し、それらの資格証明を安全に伝送するようにＩＣＦを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０１８１】
３０．ＩＣＦが、資格証明をデータベースに登録するステップ
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０１８２】
３１．ＩＣＦが、資格証明検証要求をサードパーティから受け取るステップと、
ＩＣＦが、資格証明の検証を実行するステップと
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０１８３】
３２．資格証明の検証には、サードパーティに認証ベクトルを安全に伝送することが含まれることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０１８４】
３３．認証ベクトルは、関連データを含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０１８５】
３４．Ｍ２ＭＥをＳＨＯに成功裏に登録する前、すべてのアクセスネットワークは訪問先ネットワークとみなされることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０１８６】
３５．Ｍ２ＭＥは、ネットワークを変更することなく、従来のネットワークを介してＳＨＯにトランスペアレントに接続することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０１８７】
３６．ＤＲＦは、特定のＳＨＯを購入後に選択すること、およびその選択したＳＨＯにＭ２ＭＥを登録することを可能にすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０１８８】
３７．ＤＲＦは、独立したサービスであることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０１８９】
３８．ＤＲＦは、ＳＨＯが運営することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０１９０】
３９．ＳＨＯのＲＯには、ＳＨＯの３ＧＰＰネットワークを介して接触することができることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０１９１】
４０．ＳＨＯのＲＯには、インターネットを介して接触することができることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０１９２】
４１．ＳＨＯのＲＯは、発見可能であることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０１９３】

４２．ＳＨＯのＲＯは、Ｍ２ＭＥ内の機能を使用して発見可能であることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０１９４】
４３．ＤＲＦは、Ｍ２ＭＥが届けられた後、顧客がＳＨＯを選択できるようにすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０１９５】
４４．ＤＲＦは、一時的に認証されたネットワークアクセスまたは限定されたオープンネットワークアクセスを使用し、Ｍ２ＭＥがＲＯにＩＰ接続できるようにすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０１９６】
４５．ＤＲＦは、ＶＮＯを介し、ＵＳＩＭ／ＩＳＭアプリケーションのプロビジョニングを、Ｍ２ＭＥが要求できるようにすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０１９７】
４６．ＤＲＦが、プロビジョニング要求を承認するステップと、
Ｍ２ＭＥをＤＰＦがプロビジョンすることを許可するステップと
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０１９８】
４７．ＤＲＦは、Ｍ２ＭＥの所有者が、そのＭ２ＭＥを登録することをサポートすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０１９９】
４８．ＤＲＦは、Ｍ２ＭＥとＳＨＯとの関連付けをサポートすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２００】
４９．Ｍ２ＭＥの資格証明を使用して、ＴＲＥの真正性を、ＰＶＡを介して検証するステップ
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２０１】
５０．ＤＲＦが、Ｍ２ＭＥに伝送しようとするデータパッケージを生成するステップ
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２０２】
５１．ＤＲＦが、Ｍ２ＭＥに伝送しようとするデータパッケージを取得するステップ
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２０３】
５２．ＤＲＦが、データを安全にＰＳに伝送するステップ
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２０４】
５３．ＤＰＦが、Ｍ２ＭＥに伝送しようとするデータパッケージを生成するステップ
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２０５】
５４．ＤＰＦが、Ｍ２ＭＥに伝送しようとするデータパッケージを取得するステップ
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２０６】
５５．ＤＰＦが、データを安全にＰＳに伝送するステップ
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２０７】
５６．ＤＲＦが、Ｍ２ＭＥとＤＰＦとの間のセキュリティアソシエーションの設定を容易にするステップ
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２０８】

５７．ＤＲＦが、セキュリティトークンを生成し、安全なチャネル上でＭ２ＭＥおよびＤＰＦに伝送するステップ
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２０９】
５８．ＤＰＦは、Ｍ２ＭＥにＵＳＩＭ／ＩＳＭ資格証明を遠隔プロビジョニングすることを可能にすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２１０】
５９．ＤＰＦが、Ｍ２ＭＥをプロビジョンするための許可をＤＲＦから受けるステップ
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２１１】
６０．許可を受けるステップは、ＤＰＦが、Ｍ２ＭＥと通信するためのセキュリティトークンを受け取るステップを含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２１２】
６１．ＤＰＦが、アプリケーションパッケージをＤＲＦから受け取るステップ
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２１３】
６２．ＤＰＦが、記憶された規則からアプリケーションパッケージを生成するステップと、
ＤＲＦにダウンロードされている資格証明をＤＲＦに知らせるステップと
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２１４】
６３．ＵＳＩＭ／ＩＳＭアプリケーションまたはＵＳＭＩ／ＩＳＩＭパラメータを、Ｍ２ＭＥにプロビジョニングすることをサポートするように、ＤＰＦを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２１５】
６４．Ｍ２ＭＥにとってのＵＳＩＭ／ＩＳＩＭアプリケーションまたはＵＳＩＭ／ＩＳＩＭパラメータを将来更新するように、ＤＰＦを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２１６】
６５．新たなアプリケーションを将来プロビジョニングするように、ＤＰＦを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２１７】
６６．成功したまたは失敗したプロビジョニングイベントをＤＲＦに知らせるように、ＤＰＦを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２１８】
６７．ＳＨＯは、Ｍ２ＭＥのユーザと商業的関係を有するネットワークオペレータであることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２１９】
６８．ＳＨＯは、顧客に課金する役割を担うことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２２０】
６９．ＳＨＯは、ＤＲＦの役割を果たすことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２２１】
７０．ＳＨＯは、ＤＰＦの役割を果たすことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２２２】
７１．ＳＨＯは、他の役割を果たすことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２２３】
７２．ＳＨＯは、ＤＲＦおよびＤＰＦと運営上の関係を有することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２２４】
７３．ＤＲＦとＤＰＦとは、互いに運営関係を有することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２２５】
７４．Ｍ２ＭＥは、サービスプロバイダを用いて動作する権限を最初は与えられていないことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２２６】
７５．Ｍ２ＭＥは、ＶＮＯと通信し、ＲＯへのチャネルを確立することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２２７】
７６．Ｍ２ＭＥは、プライベート識別を有することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２２８】
７７．ＰＣＩＤは、プライベート識別であることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２２９】
７８．プライベート識別は、任意のＶＮＯがＭ２ＭＥを認識し、そのＶＮＯのサービスへの一時アクセスを許可し、オペレータとのサービスをダウンロードしてプロビジョンするために、初期接続性メッセージを適切なネットワーク構成要素に宛てることを可能にすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２３０】
７９．ＰＶＡは、ダウンロードしたＵＳＩＭ／ＩＳＩＭアプリケーションを記憶し、実行するために使用する、Ｍ２ＭＥ内のセキュアデバイスの真正性を立証する資格証明に関与することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２３１】
８０．ＰＶＡには、資格証明を発行し、資格証明検証サービスを提供する１つまたは複数の商業組織が含まれることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２３２】
８１．資格証明には、証明書および鍵の対が含まれることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２３３】
８２．Ｍ２ＭＥ内のセキュアデバイスは、ＵＩＣＣ、ＴＲＥ、または他の何らかのセキュアモジュールのうちの１つもしくは複数であることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２３４】
８３．ＰＶＡの機能は、ＵＳＩＭ／ＩＳＩＭアプリケーションをプロビジョニングするために、セキュアデバイスの厳密認証が必須である場合に必要であることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２３５】
８４．Ｍ２ＭＥ内のセキュアデバイスのセキュリティを立証するための資格証明を作成し、発行するステップ
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２３６】
８５．Ｍ２ＭＥ内のセキュアデバイスのセキュリティを立証するための資格証明を作成し、発行するステップは、ＰＶＡによって実行されることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２３７】

８６．Ｍ２ＭＥ内のセキュアデバイスの資格証明の検証を行うように、ＰＶＡを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２３８】
８７．発行された資格証明の有効性に関係するデータの保守を行うように、ＰＶＡを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２３９】
８８．機器サプライヤ（Ｅ／Ｓ）は、一時的な初期ネットワークアクセスのための認証用の資格証明を、ＩＣＦから安全に取得することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２４０】
８９．Ｍ２ＭＥの再構成をサポートするようにＥ／Ｓを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２４１】
９０．再構成には、予備ネットワークアクセス資格証明を用いて、Ｍ２ＭＥをプロビジョニングすることが含まれることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２４２】
９１．Ｅ／Ｓは、ＩＣＦ１６０を介してＤＲＦ１７０に提供する際に使用するための、Ｍ２ＭＥが１組の標準化されたセキュリティ要件に従う、資格証明を、ＰＶＡ１５０から安全に得ることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２４３】
９２．Ｍ２ＭＥを資格証明で構成するようにＥ／Ｓを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２４４】
９３．所望のＤＲＦおよびＳＨＯをＭ２ＭＥの所有者が選択するための手段を提供するように、Ｅ／Ｓを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２４５】
９４．Ｍ２ＭＥがアクセスネットワークに接続するとき、ＤＲＦおよびＳＨＯの自動的選択が生じることが実現するようにＥ／Ｓを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２４６】
９５．Ｍ２ＭＥは、送信機、受信機、プロセッサ、高信頼環境（ＴＲＥ）、ＧＰＳ（全地球測位システム）、ＳＩＭ（加入者識別モジュール）、およびセキュアタイムユニットのうちの１つまたは複数を含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２４７】
９６．多くの異なる信頼機構をサポートするようにＭ２ＭＥを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２４８】
９７．ＴＲＥ、ＳＩＭ、またはＩＳＩＭのうちの１つもしくは複数をサポートするようにＭ２ＭＥを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２４９】
９８．共通ＡＫＡプロトコルに信頼機構を完全に統合することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２５０】
９９．共通ＡＫＡプロトコルは、ＴＲＥが保護する信頼状態情報または鍵のうちの１つもしくは複数を含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２５１】
１００．ＡＫＡプロトコルは、完全なＡＫＡを行うことができる前かつ認証を確立した

後の、Ｍ２ＭＥとネットワーク要素との間の任意の通信を保護することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２５２】

１０１．ＳＩＭは、拡張されて高信頼処理モジュール（ＴＰＭ）またはモバイル高信頼モジュール（ＭＴＭ）の機能を含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２５３】

１０２．ＴＰＭまたはＭＴＭと密接に動作するようにＳＩＭを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２５４】

１０３．ＳＩＭの機能を実行するようにＴＲＥを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２５５】

１０４．Ｍ２ＭＥは、ＡＫＡルート秘密でプロビジョンされることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２５６】

１０５．ルート秘密は、Ｅ／Ｓによってプロビジョンされることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２５７】

１０６．ルート秘密は、ＵＳＩＭによって保護されることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２５８】

１０７．ルート秘密は、決して変わらないことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２５９】

１０８．ＡＫＡルート秘密からセッション鍵を取り出すようにプロセッサを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２６０】

１０９．信頼状態情報をＩＣＦに提供するようにＭ２ＭＥを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２６１】

１１０．信頼状態情報は、Ｍ２ＭＥがＶＮＯにアタッチするときの予備認証に使用することができることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２６２】

１１１．信頼状態情報は、セッション鍵を取り出すために使用することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２６３】

１１２．ｎはセッション鍵CK_nおよびIK_nの最新の更新に関する指数を指し、ＣＫｎ＝ｆ３Ｋ（ＲＡＮＤ｜｜ＰＣＲ０ｎ）、ＩＫｎ＝ｆ４Ｋ（ＲＡＮＤ｜｜ＰＣＲ０　ｎ）が成立し、ただし、$f3_K()$および$f4_K()$は、共有マスタ秘密Ｋによる、暗号鍵および完全性鍵それぞれのＡＫＡ鍵導出関数を指し、ＲＡＮＤは、ＡＫＡプロセスにおいてＣＡＴＮＡが生成し、Ｍ２ＭＥ１１０に送信され、したがってＭ２ＭＥ１１０が共有する、認証ベクトル（ＡＶ）内のランダムノンスであり、$PCR0_n$は、Ｍ２ＭＥ１１０のＭＴＭＥ内のＰＣＲ０レジスタの最新値を指すことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２６４】

１１３．ＰＣＲ０レジスタの現在値は、Ｍ２ＭＥの直近のブート後の信頼状態についての記述を示すことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２６５】

１１４．CK_nおよびIK_nの値は、ブート間でＰＣＲ０の値が変わるときに変わること

を特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２６６】
１１５．ＩＣＦは、Ｍ２ＭＥの信頼状態の変化を知ることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２６７】
１１６．Ｍ２ＭＥの信頼状態の変化には、ＰＣＲ０の値の変化が含まれることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２６８】
１１７．ＩＣＦは、Ｍ２ＭＥのＯＳ、ファームウェア、またはアプリケーションの更新についてのスケジュールおよび内容を知らされることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２６９】
１１８．ＩＣＦは、Ｍ２ＭＥの信頼状態に影響を与える、Ｍ２ＭＥの任意の変化を知らされることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２７０】
１１９．Ｍ２ＭＥとＩＣＦとの間で共有されるＡＫＡ暗号鍵および完全性鍵を更新し、Ｍ２ＭＥの認証に関して有用にすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２７１】
１２０．セッション鍵は、Ｍ２ＭＥの最新の信頼状態値を反映することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２７２】
１２１．セッション鍵は、ＡＫＡ鍵導出プロセスのセキュリティを向上させることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２７３】
１２２．ＴＲＥは、Ｍ２ＭＥ内の論理的分離領域であることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２７４】
１２３．ＴＲＥの論理的分離に対するハードウェアサポートがあることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２７５】
１２４．ＴＲＥは、リムーバブルモジュールであることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２７６】
１２５．ＴＲＥは、固定型モジュールであることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２７７】
１２６．ＴＲＥは、集積回路（ＩＣ）を用いて機能することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２７８】
１２７．ＴＲＥの機能は、複数のＩＣにわたって分散されることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２７９】
１２８．ＴＲＥは、外部への論理インターフェイスおよび物理インターフェイスを定義することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２８０】
１２９．ＴＲＥによってさらされるインターフェイスは、許可されたエンティティの制御下で使用できることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２８１】
１３０．ＴＲＥは、ＭＩＤ（複数の管理識別）のためのセキュア記憶域およびセキュア

実行環境に信頼のルートを提供することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２８２】

１３１．ＴＲＥは、ＭＩＤのプロビジョニングおよび管理を提供することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２８３】

１３２．ＭＩＤは、セキュアアプリケーションであることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２８４】

１３３．ＭＩＤには、加入管理機能、セキュアペイメントアプリケーション、加入管理識別、ＵＳＩＭアプリケーション、ＩＳＩＭアプリケーション、仮想ＳＩＭ（ｖＳＩＭ）、または動的セキュリティ識別解決策のうちの１つもしくは複数が含まれることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２８５】

１３４．ＴＲＥは、任意の所要の暗号化鍵および他の資格証明とともに、セキュアな帯域外機能実装内にプロビジョンすることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２８６】

１３５．ＴＲＥは、物理的攻撃および論理的攻撃からの保護を提供することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２８７】

１３６．ＴＲＥは、自らのセキュリティポリシを実施することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２８８】

１３７．ＴＲＥは、ＭＩＤの記憶および実行を可能にすることについて、十分にセキュアであることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２８９】

１３８．ＴＲＥは、ＴＲＥ外部の、Ｍ２ＭＥの各部へのインターフェイスを備えることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２９０】

１３９．ＴＲＥは、埋め込まれた一意の識別を有することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２９１】

１４０．ＴＲＥの識別は、Ｍ２ＭＥの識別に関連することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２９２】

１４１．ＴＲＥは、標準プロトコルを使用し、自らの識別を発行機関に対して安全に認証するように構成されることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２９３】

１４２．ＴＲＥは、ＵＩＣＣ内に実装することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２９４】

１４３．ＴＲＥは、Ｍ２ＭＥが提供するハードウェア構成要素およびソフトウェア構成要素を使用する、Ｍ２ＭＥ上の統合的解決策として実装することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２９５】

１４４．ＴＲＥは、ＭＩＤのダウンロード、遠隔プロビジョニング、および管理をサポートすることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０２９６】

１４５．ＴＲＥは、管理識別実行ファイル（ＭＩＤＥ）の機能をサポートすることを特

徴とする上記の実施形態のいずれか１つに記載の方法。
【０２９７】
１４６．Ｍ２ＭＥは、ＴＲＥコードベースを構成するソフトウェアコードおよびデータの完全性検査をサポートすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２９８】
１４７．ＴＲＥは、Ｍ２ＭＥの電源投入／ブート時に検査されることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０２９９】
１４８．コード検査は、Ｍ２ＭＥの動作使用の間に行うことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３００】
１４９．コード検査は、定義済みの間隔でまたは特定のトリガ時に、バックグラウンドプロセスとして行うことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３０１】
１５０．コード検査は、Ｍ２ＭＥの部分的検査または完全検査を範囲に含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３０２】
１５１．ＴＲＥは、複数の分離された信頼済みドメインに対するサポートを含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３０３】
１５２．各ドメインは、利害関係のある所有者が所有することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３０４】
１５３．各ドメインは、他のドメインから分離されることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３０５】
１５４．各ドメインは、不正変更および不正アクセスから保護されることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３０６】
１５５．ＴＲＥは、ドメイン間サービスを提供することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３０７】
１５６．ドメイン間サービスには、認証機能および立証機能のうちの１つまたは複数が含まれることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３０８】
１５７．Ｍ２ＭＥは、散発的にまたはたまにネットワークに接続することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３０９】
１５８．Ｍ２ＭＥは、休止状態で動作することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３１０】
１５９．ＴＲＥのソフトウェアコードの実行時完全性検査は、Ｍ２ＭＥが休止状態で動作する間に行うように構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３１１】
１６０．完全性検査は、他のＭ２ＭＥプロセスまたはＴＲＥプロセスを妨げないことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３１２】
１６１．完全性検査の状態は、Ｍ２ＭＥがＳＨＯに接続するときに準備ができているこ

とを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３１３】
１６２．Ｍ２ＭＥには、Ｍ２ＭＥにとって固有の一時的プライベート識別が割り当てられることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３１４】
１６３．ＰＣＩＤは、時限有効期間にわたって有効であることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３１５】
１６４．有効期間は、Ｍ２ＭＥが実施することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３１６】
１６５．有効期間は、ＴＲＥが制御することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３１７】
１６６．ＰＣＩＤを除去するステップ
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３１８】
１６７．ＰＣＩＤは、複数のＭ２ＭＥが使用できるが、同時には使用できないことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３１９】
１６８．ＰＣＩＤを系統的に再割当することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３２０】
１６９．複数のＰＣＩＤをＭ２ＭＥにプロビジョンすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３２１】
１７０．Ｍ２ＭＥは、サイズＮのグループでリリースされることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３２２】
１７１．ｊ番目のロットのＭ２ＭＥは、Ｍ＿ｉ，ｊと称し、ただし、ｊ＝１，．．．，Ｍであることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３２３】
１７２．ＰＣＩＤの割当は、サイズＮｘＭの行列（Ｐ）＿｛ｉ，ｊ｝を用いて初期化することができることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３２４】
１７３．Ｍ２ＭＥ　Ｍ＿ｉ，１は、製造中に列Ｐ＿ｉ，*がＴＲＥにロードされることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３２５】
１７４．セキュアタイマまたは単調カウンタを初期化し、アクティブにし、ＴＲＥの制御下に置くことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３２６】
１７５．Ｍ２ＭＥ　Ｍ＿ｉ，１は、初期化された時間またはカウンタに基づいて、確定した期間Ｔまたは所定回数にわたり、Ｐ＿ｉ，１を使用することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３２７】
１７６．ＴＲＥは、Ｐ＿ｉ，１を破棄し、Ｐ＿ｉ，２を使用することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３２８】
１７７．デバイスが寿命サイクルのどこにあるのかを判断するように、ネットワークを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０３２９】
１７８．ＴＲＥを用いてＰＣＩＤ列ベクトルを処理し、ＴＲＥが時間制限を実施することは、ＰＣＩＤの同時使用を防ぎ、Ｍ２ＭＥが、その動作時間の間中有効なＰＣＩＤを有することを確実にすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３３０】
１７９．ＰＣＩＤを再プロビジョンするようにＭ２ＭＥを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３３１】
１８０．少なくとも２つのＭ２ＭＥが、同じＰＣＩＤを同時に使おうとすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３３２】
１８１．ＰＣＩＤの数は、１つのロット内のＭ２ＭＥの数よりもはるかに多いことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３３３】
１８２．ＰＣＩＤを、ランダムに選択することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３３４】
１８３．複数のＭ２ＭＥのクロックを同期することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３３５】
１８４．Ｍ２ＭＥのクロックを、複数のＭ２ＭＥに再同期することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３３６】
１８５．時間基準を保持／管理するようにＴＲＥを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３３７】
１８６．信頼できる時間源との同期をサポートするようにＴＲＥを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３３８】
１８７．ＴＲＥは、Ｍ２ＭＥ内に位置する信頼できるタイムユニットに依拠することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３３９】
１８８．Ｍ２ＭＥは、自律型地理位置機器を含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３４０】
１８９．ＴＲＥは、その地理測位機器に安全にアクセスできることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３４１】
１９０．２つのＭ２ＭＥが、同じアクセスネットワークセルに対して同時に無線接続を物理的に確立することはないことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３４２】
１９１．目的地理位置（Ｄ）および許容差範囲（Ｒ）でＭ２ＭＥをプロビジョンすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３４３】
１９２．ＤおよびＲの値をＴＲＥ内に記憶することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３４４】
１９３．ＴＲＥしかそのデータにアクセスできないように、暗号を使用してＤおよびＲの値を保護することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０３４５】
１９４．ＴＲＥが自らの現在の地理位置を求めるステップと、
その現在の地理位置を、Ｒの範囲内でＤと比較するステップと、
ネットワークアクセスのためのＰＣＩＤをリリースするステップと
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３４６】
１９５．アクセスネットワークは、ＰＣＩＤ、セルＩＤの対の記録を保持することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３４７】
１９６．Ｍ２ＭＥによるネットワークへのアクセスは、所定の複数のセルにおいて認められることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３４８】
１９７．複数のネットワークセル識別子でＭ２ＭＥを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３４９】
１９８．Ｍ２ＭＥを、地理的に移動させることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３５０】
１９９．Ｍ２ＭＥを移動させるとき、ネットワークアクセスを無効にすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３５１】
２００．ＰＣＩＤを使用することができる場所を示す複数の三つ組で、Ｍ２ＭＥをプロビジョンすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３５２】
２０１．三つ組は、ＰＣＩＤ、Ｄ、およびＲを含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３５３】
２０２．ＴＲＥの現在の地理位置を求めるステップと、
その現在の地理位置を、複数の三つ組と比較するステップと、
その現在の地理位置に関連するＰＣＩＤをリリースするステップと
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３５４】
２０３．複数の五つ組でＭ２ＭＥをプロビジョンすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３５５】
２０４．五つ組は、ＰＣＩＤ、Ｄ、Ｒ、ｔ１、およびｔ２を含み、ｔ１は有効期間の開始時間を指定し、ｔ２は有効期間の終了時間を指定することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３５６】
２０５．五つ組は、Ｍ２ＭＥの経路を示すことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３５７】
２０６．所定時間においてＭ２ＭＥがネットワークに接続できないことは、アラームをトリガすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３５８】
２０７．五つ組は、再プロビジョンすることができることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３５９】
２０８．五つ組は、ＰＣＩＤ更新サービス（ＰＵＳ）を使用して再プロビジョンすることができることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０３６０】
２０９．ＴＲＥを識別するようにＰＵＳを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３６１】
２１０．ＩＣＦは、ＰＵＳを含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３６２】
２１１．ＰＵＳは、別個のネットワーク構成要素であることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３６３】
２１２．五つ組の再プロビジョニングは、１つまたは複数の五つ組への変更を含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３６４】
２１３．ＴＲＥの識別は、ＴＲＥを現在のネットワークＩＰアドレスに関連させることができるネットワークサーバに送信することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３６５】
２１４．遠隔プロビジョニングをＤＰＦに委ねることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３６６】
２１５．ＰＵＳがＭ２ＭＥおよびＴＲＥに接続するステップと、
ＰＵＳがＴＲＥの検証を要求するステップと、
ＰＵＳが、新たな複数の五つ組、および破棄すべき以前の五つ組のリストを送るステップと、
ＴＲＥが、その新たな五つ組をインストールし、以前の五つ組を破棄するステップと
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３６７】
２１６．ＰＣＩＤに付加することができる擬似乱数を作成するように、ＴＲＥを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３６８】
２１７．擬似乱数を追跡し、見分けるようにアクセスネットワークを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３６９】
２１８．通信エンティティは、Ｍ２ＭＥ、ＴＲＥ、およびネットワークアクセスポイント（ＮＡＰ）であることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３７０】
２１９．ＮＡＰは、ＶＮＯに関連するｅｎｏｄｅＢであることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３７１】
２２０．単一の初期ネットワーク接続で使用する乱数（ＲＡＮＤ）を生成するようにＴＲＥを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３７２】
２２１．ＴＲＥが完全性保護方法を適用するステップ
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３７３】
２２２．完全性保護方法は、ＲＡＮＤが第２のパラメータ、必要に応じて追加データ（Ｄ１）、およびＰＣＩＤに入る、鍵付きｈａｓ関数であることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３７４】
２２３．ＴＲＥは、ＴＲＥ→ｅＮＢ：ＲＡＮＤ｜｜ＰＣＩＤ｜｜Ｄ１｜｜Ｍ１：＝ＭＡ

Ｃ（ＰＣＩＤ｜｜Ｄ１，ＲＡＮＤ）をｅＮＢに送信し、
ｅＮＢは、ＭＡＣ（メッセージ認証コード）を検証し、
ｅＮＢは、ペイロードデータＤ２、Ｍ１から返信パッケージを構築し、
ｅＮＢは、ｅＮＢ→ＴＲＥ：Ｄ２｜｜Ｍ２：＝ＭＡＣ（ＰＣＩＤ｜｜Ｄ２，Ｍ１としてその返信パッケージをＴＲＥに送信すること
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０３７５】
２２４．後続のメッセージ交換は、任意の新たなメッセージ要素を含むデータ要素のＭＡＣ、および直前の交換のＭＡＣを含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０３７６】
２２５．ｅＮＢおよびＴＲＥは、新たなM_nを構築するための最終値M_{n-1}を使用して、通信中にメッセージを区別することができることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０３７７】
２２６．中間者型攻撃を回避することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０３７８】
２２７．通信当事者を認証するために、共有された秘密をメッセージに含めることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０３７９】
２２８．共有された秘密は、取り決められた秘密であることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０３８０】
２２９．ＭＡＣ値は、ＰＣＩＤを含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０３８１】
２３０．ｅＮＢは、ＰＣＩＤを使用する、すべての同時にアクティブなネットワークアクセス試行（チャネルと）の状態を表す表を保持することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０３８２】
２３１．その表の１列目は、チャネルに属するＰＣＩＤの索引を含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０３８３】
２３２．その索引は、すべてのチャネルにわたり現在アクティブなすべてのＰＣＩＤのリストの中の一項目を指し示すことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０３８４】
２３３．その索引は、ＰＣＩＤの値であることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０３８５】
２３４．ｅＮＢが、チャネル上でメッセージを受信するステップであって、ＴＲＥ→ｅＮＢ：　Ｄ３｜｜Ｍ３：＝ＭＡＣ（ＰＣＩＤ｜｜Ｄ３，Ｍ２）が成立する、ステップ
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０３８６】
２３５．ｉ－１からＮにわたり、ｅＮＢは$PCID_i$をＰＬから選択するステップ
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０３８７】
２３６．最初のセルにＰＣＩＤの索引Ｉが含まれるすべての表の行に対し、ｅＮＢはＭ：＝ＭＡＣ（$PCID_i$｜｜D_3，M_2）を計算するステップであって、M_2はその行の２番

目のセルから取る、計算するステップ
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３８８】
２３７．成功状態に達し、検索手順は終了すること
をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３８９】
２３８．最後受信第３のメッセージに対応するチャネルの行番号を返すことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３９０】
２３９．データ履歴にD_3が追加され、選択された表の行のアクティブハッシュ値のセル内で、M_3がM_2に取って代わることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３９１】
２４０．メッセージは、チャネルの索引Ｉを含んで後続メッセージの関連チャネルを見つけることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３９２】
２４１．アクティブなＰＣＩＤをロックすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３９３】
２４２．ＰＣＩＤをアクティブに割当解除することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３９４】
２４３．ＴＲＥは、完全なネットワーク接続性を得るためにあるＰＣＩＤが使用されている場合、その使用済みＰＣＩＤを破棄することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３９５】
２４４．有効期間が切れた後にＰＣＩＤを破棄することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３９６】
２４５．要求に応答してＰＣＩＤを破棄することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３９７】
２４６．破棄されたＰＣＩＤを、別のＭ２ＭＥが使用することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３９８】
２４７．デロケーションイベントを信号で伝えるため、ＴＲＥからＥ／Ｓへの接続を確立することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０３９９】
２４８．Ｅ／Ｓは、割当解除されたＰＣＩＤのリストを保持することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４００】
２４９．割当解除プロセスの間、ＰＣＩＤを平文で転送しないことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４０１】
２５０．検証を自律的に実行することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４０２】
２５１．検証を半自律的に実行することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４０３】

２５２．検証を遠隔的に実行することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４０４】

２５３．自律的検証は、Ｍ２ＭＥが自らをネットワークにアタッチできるようにする前に実行されることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４０５】

２５４．半自律的検証は、Ｍ２ＭＥ１１０の有効性を、外部ネットワークエンティティに依拠せずに評価することを含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４０６】

２５５．半自律的検証の結果を、遠隔エンティティに報告することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４０７】

２５６．その結果は、ＴＲＥの認証をＭ２ＭＥに結合する根拠を含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４０８】

２５７．遠隔エンティティは、ＰＶＡであることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４０９】

２５８．Ｍ２ＭＥと遠隔エンティティとの間の信号伝達は保護されることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４１０】

２５９．遠隔的検証は、外部ネットワークエンティティが、ＴＲＥが生成した検証用の根拠、およびＴＲＥとＭ２ＭＥとの間の結合の根拠を受け取った後、Ｍ２ＭＥの有効性／完全性を直接評価することを含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４１１】

２６０．外部ネットワークエンティティは、ＰＶＡであることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４１２】

２６１．Ｍ２ＭＥと外部ネットワークエンティティとの間の通信は保護されることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４１３】

２６２．自律的検証が実行され、検証の直接的根拠は外部に提供されないことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４１４】

２６３．Ｍ２ＭＥは検証に失敗し、そのＭ２ＭＥがネットワークにアタッチし、または遠隔エンティティへの認証済み接続を得ることをＴＲＥが妨げることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４１５】

２６４．ＴＲＥが、自らがセキュア始動の定義済み状態に達しているかどうかを検査するステップ

をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４１６】

２６５．セキュア始動を必要とするＭ２ＭＥの残りの定義済み部分が、セキュア始動の定義済み状態に達しているかどうかを検査するステップ

をさらに含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４１７】

２６７．ＴＲＥがさらなる検査を行うことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４１８】
２６８．ＴＲＥにとって外部にあるが、ＴＲＥが完全性を保護する、Ｍ２ＭＥ内の測定構成要素がさらなる検査を行うことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４１９】
２６９．ＴＲＥは、要求された認証手順にＭ２ＭＥが関与することを許可することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４２０】
２７０．自律的検証は、必要とされる対外的通信の観点から最も経済的な方法であることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４２１】
２７１．自律的検証は、ネットワークアクセス中または連続的接続段階の間、任意の外部エンティティが、ＴＲＥの完全性を独立に評価することを認めないことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４２２】
２７２．ＴＲＥは、検証プロセスおよびその結果のログを記憶することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４２３】
２７３．そのログは、監査記録を構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４２４】
２７４．監査データは、安全な内部アーカイブに記憶することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４２５】
２７５．安全な内部アーカイブは、ＴＲＥ内にあることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４２６】
２７６．安全な内部アーカイブは、ＴＲＥが保護することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４２７】
２７７．安全な内部アーカイブの不正変更を検出することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４２８】
２７８．データの完全性保護を実現することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４２９】
２７９．監査データは、自律的検証が引き起こされる特定の目的に結合されることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４３０】
２８０．そのデータは、検証の目的を含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４３１】
２８１．アクセスプロトコル内に確立される、共有された秘密または資格証明を監査データに添付し、ＴＲＥは、その作成したデータにデジタル署名を施してそのデータの完全性を保護することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４３２】
２８２．Ｍ２ＭＥから独立したエンティティは監査データを周期的に要求して、前のネットワークアクセスイベントごとに、そのＭ２ＭＥが信頼できるかどうかを確認することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４３３】

２８３．そのデータを、ネットワークアクセス試行に関するネットワーク側プロトコルに再照合して不正変更を検出することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４３４】

２８４．Ｍ２ＭＥの残りの他の構成要素、構成、またはパラメータの完全性は、ロードされるとき、開始されるとき、または測定構成要素が利用できる他の任意の定義済み実行時時間イベント時に検査されることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４３５】

２８５．遠隔エンティティは、Ｍ２ＭＥが半自律的検証テストを通過したことを間接的に知ることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４３６】

２８６．ネットワークに対し、半自律的検証の成果について明確な信号伝達があることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４３７】

２８７．その信号伝達は、暗号を使用して保護されることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４３８】

２８８．その信号伝達は、ＭＩＤをダウンロードするのに必要な、Ｍ２ＭＥの認証より前に起こることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４３９】

２８９．その信号伝達は、ＴＲＥの認証と有効性検査に使用されるＭ２ＭＥ内の資源との間の結合の根拠を含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４４０】

２９０．根拠には、ＴＲＥおよびＭ２ＭＥの証明を確立するためのさらなる情報を提供する、Ｍ２ＭＥからネットワークに送信されるトークンが含まれることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４４１】

２９１．ＰＶＡまたはＳＨＯは、検証を周期的に行うようにＴＲＥに要求することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４４２】

２９２．セキュリティゲートウェイ（ＳｅＧＷ）が検証を要求することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４４３】

２９３．その要求は、Ｍ２ＭＥが登録された後に送信されることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４４４】

２９４．その要求は、ＳｅＧＷがホームｅＮｏｄｅＢ（Ｈ（ｅ）ＮＢ）を一番初めに認証した時点で送信されることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４４５】

２９５．その要求は、ＰＶＡ、ＳＨＯ、ＳｅＧＷのうちの１つまたは複数から、保護された運用保守（ＯＡＭ）メッセージとして周期的に送信されることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４４６】

２９６．周期的再検証の期間は、相対的に長いが、ＳＨＯが検証の新鮮さに関して安心できるようにするのに十分な短さのものであることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４４７】

２９７．ＴＲＥは、その要求に基づいて検証手順を実行することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４４８】
２９８．ＴＲＥは、最後の成功裏の検証を示すタイムスタンプを生成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４４９】
２９９．ＴＲＥは、周期的検証の現在のラウンドが失効する前に、最後の検証が行われたことを示すメッセージを送信することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４５０】
３００．検証の成果に関する明確な信号伝達はないことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４５１】
３０１．Ｍ２Ｍ１Ｅは、定義済みセキュア状態に向けて始動することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４５２】
３０２．Ｍ２ＭＥは、プラットフォームの有効性の根拠をＴＲＥが生成することを要求することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４５３】
３０３．ＴＲＥは、Ｍ２ＭＥの残りから、プラットフォームの有効性の根拠を作成するために使用する材料を集めることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４５４】
３０４．根拠には、セキュリティ上重要な実行可能コード、Ｍ２ＭＥのオペレーティングシステムの資格証明、および機器ｉｄが含まれることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４５５】
３０５．ＴＲＥは、Ｍ２ＭＥの検証用の根拠を生成し、完全性および機密性を得るために、それを暗号を使用して保護することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４５６】
３０６．Ｍ２ＭＥは、その保護された根拠をＰＶＡに転送することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４５７】
３０７．ＰＶＡはその保護された根拠を受信し、その根拠を評価して、引き続き認証を実行し、ＭＩＤをダウンロードするのに、そのＭ２ＭＥが十分信頼できるかどうかを判定することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４５８】
３０８．Ｍ２ＭＥの検証と認証との間の結合を実行することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４５９】
３０９．その結合は、Ｍ２ＭＥのセキュア状態を立証する、Ｍ２ＭＥの証明書または資格証明を含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４６０】
３１０．その結合は、より安全な証明手段を含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４６１】
３１１．初期ネットワーク接続性の必須条件として、ＩＣＦがＭ２ＭＥを認証することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４６２】
３１２．ＭＩＤをダウンロードする前に、認証されたＴＲＥをＭ２ＭＥが含むことを証明するために、ＤＰＦがＭ２ＭＥを認証することを特徴とする上記の実施形態のいずれか

１つに記載の方法。
【０４６３】
３１３．操作上のネットワークアクセスの前に、ＳＨＯがＭ２ＭＥを認証することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４６４】
３１４．ネットワークアクセス認証への有効性の結合は、自律的検証では暗示的であることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４６５】
３１５．ＴＲＥの識別についてのさらなる情報を提供するトークンを、初期アタッチメントメッセージ内で渡すことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４６６】
３１６．Ｍ２ＭＥへの、認証資格証明を保持するＴＲＥの論理的結合があることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４６７】
３１７．認証の間、デバイスプラットフォームの完全性が検証されることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４６８】
３１８．Ｍ２ＭＥへの、ＴＲＥの物理的結合があることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４６９】
３１９．ＴＲＥの認証の間、デバイスプラットフォームの完全性が検証されることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４７０】
３２０．プラットフォーム資源の実際の検証は、Ｍ２ＭＥに安全に埋め込まれたハードウェアセキュリティ構成要素の機能を使用することによって実行されることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４７１】
３２１．プラットフォーム資源の実際の検証は、ＴＲＥの外側にあるが、ＴＲＥがそのセキュリティ特性を保証し、ＴＲＥに安全に接続することができるハードウェアセキュリティ構成要素を使用することによって実行されることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４７２】
３２２．検証および認証を、共通プロトコルのセッション内で組み合わせることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４７３】
３２３．ＩＫＥｖ２を、組み合わせられた検証／認証手順で使用することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４７４】
３２４．ＩＣＦ、ＤＲＦ、およびＤＰＦは、個別のエンティティであることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４７５】
３２５．ＩＣＦ、ＤＲＦ、およびＤＰＦは、組み合わせられることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４７６】
３２６．Ｍ２ＭＥへのＭＩＤのダウンロードおよびプロビジョニングは、Ｍ２ＭＥが初期ネットワークアクセスのために３Ｇ　ＶＮＯのネットワークにアクセスするときに生じることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４７７】
３２７．ＶＮＯは、Ｍ２ＭＥにエアインターフェイスを提供することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０４７８】
３２８．Ｍ２ＭＥは、標準ＧＳＭ／ＵＭＴＳ原理を使用してネットワーク情報を復号し、アタッチメッセージを使用してＶＮＯのネットワークにアタッチすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４７９】
３２９．アタッチメッセージは、仮のＭ２ＭＥ　ＩＤ（ＰＣＩＤ）を含むことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４８０】
３３０．ＶＮＯは、標準ＵＭＴＳ　ＡＫＡ手順を使用してＭ２ＭＥを認証することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４８１】
３３１．ＶＮＯは、ＰＣＩＤの内容および構造に基づいて、そのＰＣＩＤをＩＭＳＩとして認識することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４８２】
３３２．Ｍ２ＭＥおよびＶＮＯは、共通認証アルゴリズムをサポートすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４８３】
３３３．共通認証アルゴリズムは、Ｍｉｌｅｎａｇｅであることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４８４】
３３４．ＰＣＩＤをＭ２ＭＥのＩＤとして認識するＶＮＯは、そのＰＣＩＤを正当な予備資格証明として承認するＩＣＦに接触することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４８５】
３３５．ＩＣＦは、Ｍ２ＭＥとのさらなる通信を保護するための１組の予備ＡＶを発行し、保護されたＩＰ接続性をＭ２ＭＥに提供し始めることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４８６】
３３６．Ｍ２ＭＥとＩＣＦとが標準ＡＫＡプロセスを実行し、予備ＡＫＡ鍵を作成してＭ２ＭＥとの通信を保護することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４８７】
３３７．ＩＣＦは、Ｍ２ＭＥをＤＰＦに転送することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４８８】
３３８．ＩＣＦは、ＰＣＩＤをＤＲＦに送信することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４８９】
３３９．ＤＲＦは、Ｍ２ＭＥがＳＨＯを探すのを助けることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４９０】
３４０．ＤＲＦは、ＳＨＯに接続し、ＳＨＯのネットワークへの接続に関してＭ２ＭＥを登録することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４９１】
３４１．ＳＨＯは、ＴＲＥの真正性および完全性を検証するようにＰＶＡに要求することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４９２】
３４２．ＰＶＡは、ＴＲＥの真正性および完全性を検証することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４９３】

３４３．ＰＶＡは、検証結果をＳＨＯに送信することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４９４】
３４４．ＳＨＯは、ＤＰＦに接触し、ＭＩＤをＭ２ＭＥにプロビジョニングすることを許可することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４９５】
３４５．ＤＰＦは、ＭＩＤをＭ２ＭＥにダウンロードすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４９６】
３４６．Ｍ２ＭＥは、ダウンロード済みＭＩＤをＴＲＥ内にプロビジョンし、そのプロビジョニングの状態をＤＰＦに報告することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４９７】
３４７．Ｍ２ＭＥは、その状態メッセージを検証するためのトークンを送信することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４９８】
３４８．そのトークンは、不正変更およびリプレイ攻撃に耐性があることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０４９９】
３４９．ＤＰＦは、プロビジョニングの状態をＳＨＯに報告することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５００】
３５０．Ｍ２ＭＥへのＭＩＤのダウンロードおよびプロビジョニングは、Ｍ２ＭＥが初期ネットワークアクセスのために３Ｇ　ＶＮＯのネットワークにアクセスするときに生じることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５０１】
３５１．ＩＣＦは、仮認証ベクトルをＭ２ＭＥにリリースする前に、さらにＩＰ接続性をＭ２ＭＥに与える前に、ＴＲＥを検証するよう、ＰＶＡに要求することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５０２】
３５２．Ｍ２ＭＥの所有者は、新たなＳＨＯに接触してＭ２ＭＥのパラメータを転送することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５０３】
３５３．Ｍ２ＭＥの所有者は、Ｍ２ＭＥに接触して再プロビジョニングを開始することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５０４】
３５４．新たなＳＨＯは、Ｍ２ＭＥを検証するように検証エンティティに要求することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５０５】
３５５．検証エンティティはＭ２ＭＥを検証し、結果を新たなＳＨＯに送信することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５０６】
３５６．新たなＳＨＯは、新たなＭＩＤをＭ２ＭＥにダウンロードし、プロビジョンするよう、ＤＰＦに要求することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５０７】
３５７．ＤＰＦは、新たなＭＩＤパッケージをＭ２ＭＥに安全にダウンロードすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５０８】
３５８．Ｍ２ＭＥは、以前のＭＩＤを破棄したというメッセージを以前のＳＨＯに送信

することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５０９】
３５９．以前のＳＨＯは、Ｍ２ＭＥにＡＣＫを送信することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５１０】
３６０．Ｍ２ＭＥは、そのＡＣＫをＤＰＦおよび新たなＳＨＯに転送することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５１１】
３６１．Ｍ２ＭＥは、ＤＰＦの助けで自らのシステムを更新し、ＭＩＤをインストールすることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５１２】
３６２．Ｍ２ＭＥは、状態をＤＰＦに送信することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５１３】
３６３．ＤＰＦは、その状態を新たなＳＨＯに報告することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５１４】
３６４．Ｍ２ＭＥを初期状態に置き、初期プロビジョニング手順を実行することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５１５】
３６５．ＰＶＡは、Ｍ２ＭＥが依然として同じＳＨｏに加入している間に実行される、任意のソフトウェアまたはファームウェア（ＳＷ／ＦＷ）の更新が、安全な方法で行われることを保証する役割を果たすことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５１６】
３６６．ＰＶＡまたはＤＰＦは、ＳＷ／ＦＷの安全な無線または有線ダウンロードや、Ｍ２ＭＥまたはＴＲＥの再プロビジョニングなどの手順を監督することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５１７】
３６７．ＰＶＡまたはＤＰＦは、ＯＭＡ　ＤＭおよびＯＭＡ　ＦＯＴＡの手順を使用することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５１８】
３６８．Ｍ２ＭＥの信頼状態情報は、遠隔ＳＷ／ＦＷ更新または再構成が原因で変わることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５１９】
３６９．Ｍ２ＭＥまたはＴＲＥの、新たな検証可能ブートもしくは実行時信頼状態情報検査を開始し、その結果を得るようにＰＶＡまたはＤＰＦを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５２０】
３７０．不正変更を検出するようにＭ２ＭＥを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５２１】
３７１．不正変更を検出することには、任意のサブシステムへの不正変更が含まれることを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５２２】
３７２．不正変更の検出は、頻繁に行うことを特徴とする上記の実施形態のいずれか１つに記載の方法。
【０５２３】
３７３．不正変更イベントには、マルウェアまたはウイルスが、ＯＳを救済可能なおよび／または救済不可能な危険にさらすこと、バッファオーバフローイベント、無線もしく

は上位層接続特性、および／または環境測定値の突然の予期せぬもしくは未承認の変化、Ｍ２ＭＥの予備認証、登録、またはＭＩＤプロビジョニング要求に対し、信頼できるネットワーク要素がアクセスまたはサービスの失敗および／もしくは拒否を過度に繰り返すこと、またはＭ２ＭＥもしくは遠隔ＭＩＤ管理機能に関係するＭ２ＭＥサブシステムの信頼状態の、ブート後または実行時読取り値の任意の予期せぬ／未承認の変化のうちの１つもしくは複数が含まれることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０５２４】

３７４．不正変更を検出するように他のネットワーク要素を構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０５２５】

３７５．Ｍ２ＭＥは、不正変更を検出することに応答して、被害を抑えるための措置を講じることを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０５２６】

３７６．遠隔ＭＩＤ管理を無効にするようにＭ２ＭＥを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０５２７】

３７８．指定されたネットワーク要素への、性質イベントの報告についてＭ２ＭＥを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０５２８】

３７９．最近のソフトウェア更新、または疑わしいウイルスもしくはマルウェアコードもしくはデータの削除、隔離、アンインストールなどの救済アクションを実行するように、Ｍ２ＭＥを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０５２９】

３８０．遠隔ＭＩＤ管理機能に関係する、任意のあらかじめ指定された１組のデータを削除するように、Ｍ２ＭＥを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０５３０】

３８１．Ｍ２ＭＥ、またはＭ２ＭＥの部分もしくはサブシステムの電源を切るようにＭ２ＭＥを構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０５３１】

３８２．不正変更後の救済手段を実行するように、ネットワーク要素を構成することを特徴とする上記の実施形態のいずれか１つに記載の方法。

【０５３２】

３８３．上記の実施形態のいずれか１つの少なくとも一部を実行するように構成される、無線送受信ユニット（ＷＴＲＵ）。

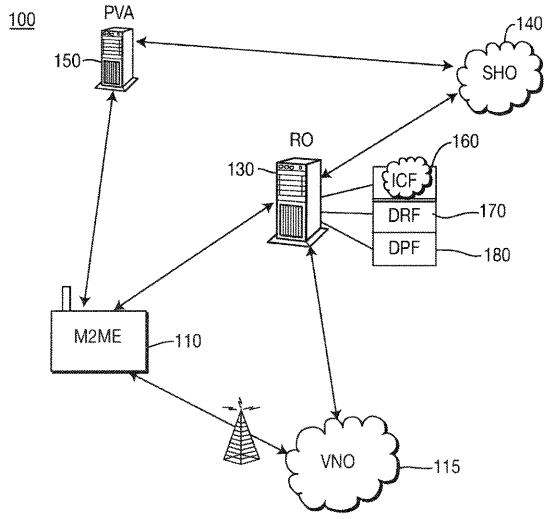
【０５３３】

３８４．上記の実施形態のいずれか１つの少なくとも一部を実行するように構成される、機械対機械（Ｍ２Ｍ）機器。

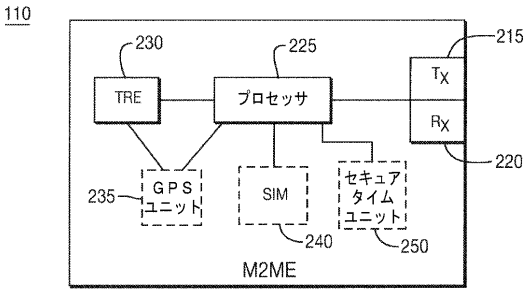
【０５３４】

３８５．上記の実施形態のいずれか１つの少なくとも一部を実行するように構成される、ネットワークエンティティ。

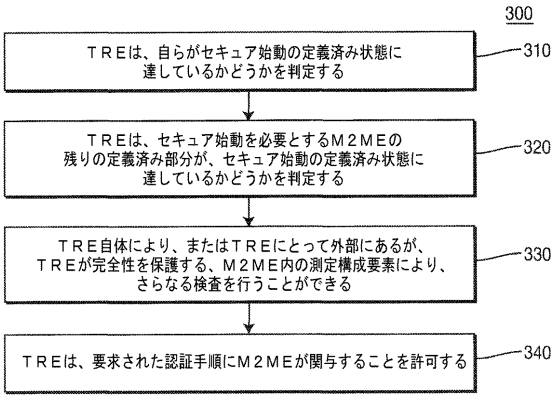
【図１】



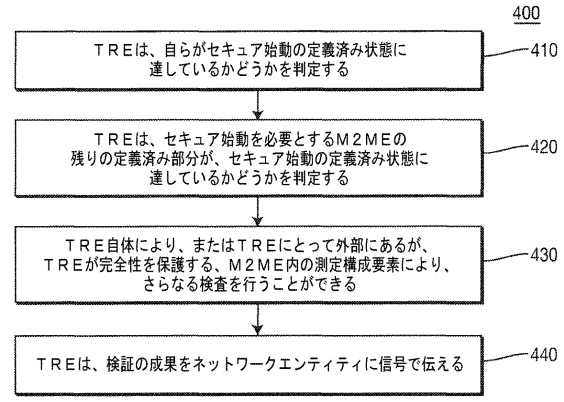
【図２】



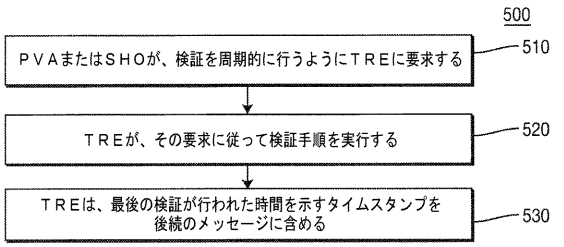
【図３】



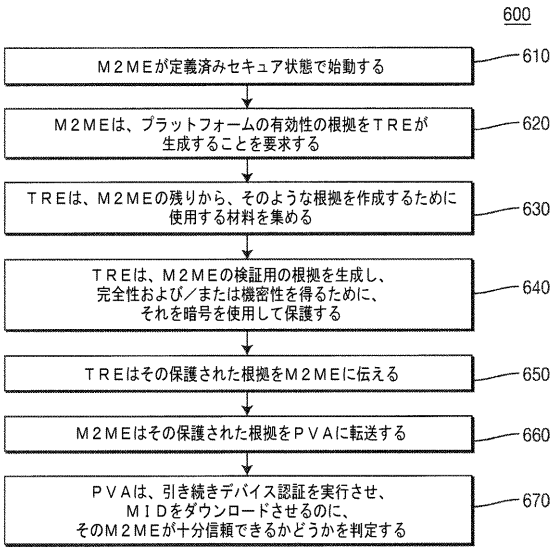
【図４】



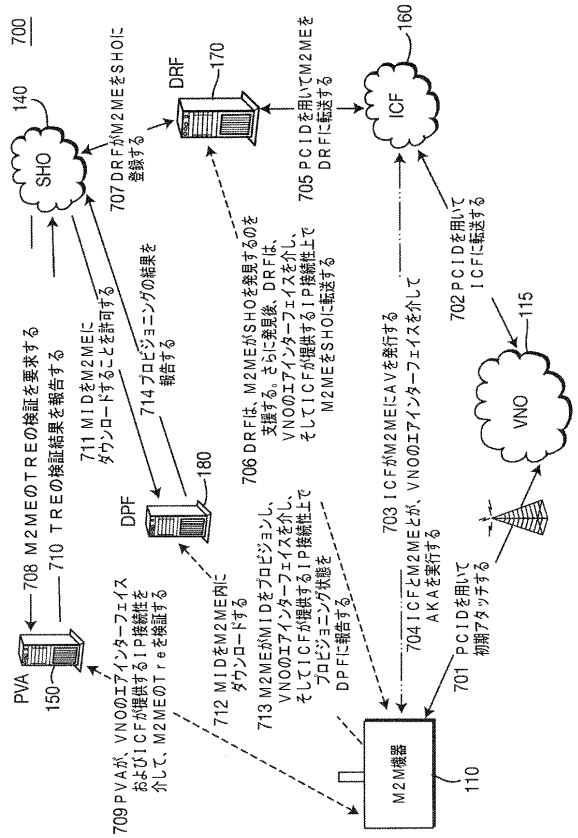
【図５】



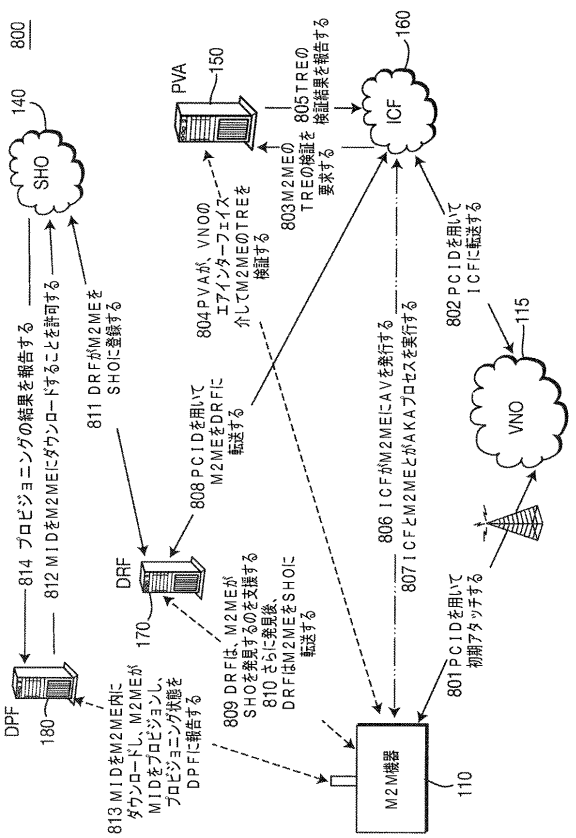
【図６】



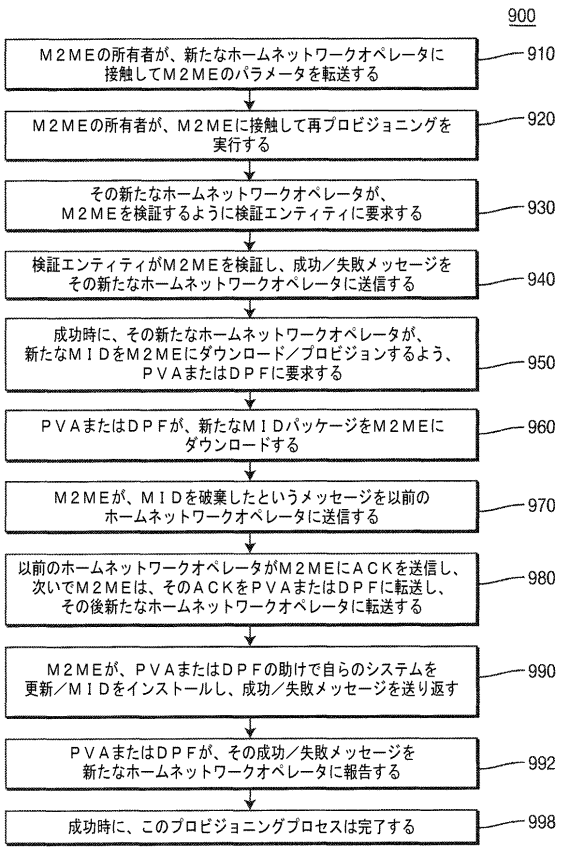
【図７】


700
140
SHO
DRF
170
160
ICF
PVA
150
DPF
180
VNO
115
M2M機器
110
708 M2MEのTREの検証を要求する
710 TREの検証結果を報告する
711 MIDをM2MEにダウンロードすることを許可する
707 DRFがM2MEをSHOに登録する
714 プロビジョニングの結果を報告する
706 DRFは、M2MEがSHOを発見するのを支援する。さらに発見後、DRFは、VNOのエアインターフェイスを介し、そしてICFが提供するIP接続性上でM2MEをSHOに転送する
705 PCIDを用いてM2MEをDRFに転送する
702 PCIDを用いてICFに転送する
703 ICFがM2MEにAVを発行する
704 ICFとM2MEとが、VNOのエアインターフェイスを介してAKAを実行する
701 PCIDを用いて初期アタッチする
709 PVAが、VNOのエアインターフェイスおよびICFが提供するIP接続性を介して、M2MEのTreを検証する
712 MIDをM2ME内にダウンロードする
713 M2MEがMIDをプロビジョンし、VNOのエアインターフェイスを介し、そしてICFが提供するIP接続性上でプロビジョニング状態をDPFに報告する

【図８】


800
140
SHO
PVA
150
ICF
160
DRF
170
DPF
180
VNO
115
M2M機器
110
814 プロビジョニングの結果を報告する
812 MIDをM2MEにダウンロードすることを許可する
811 DRFがM2MEをSHOに登録する
804 PVAが、VNOのエアインターフェイスを介してM2MEのTREを検証する
805 TREの検証結果を報告する
803 M2MEのTREの検証を要求する
808 PCIDを用いてM2MEをDRFに転送する
809 DRFは、M2MEがSHOを発見するのを支援する
810 さらに発見後、DRFはM2MEをSHOに転送する
806 ICFがM2MにAVを発行する
807 ICFとM2MEとがAKAプロセスを実行する
802 PCIDを用いてICFに転送する
801 PCIDを用いて初期アタッチする
813 MIDをM2ME内にダウンロードし、M2MEがMIDをプロビジョン、プロビジョニング状態をDPFに報告する

【図９】


900
M2MEの所有者が、新たなホームネットワークオペレータに接触してM2MEのパラメータを転送する
910
M2MEの所有者が、M2MEに接触して再プロビジョニングを実行する
920
その新たなホームネットワークオペレータが、M2MEを検証するように検証エンティティに要求する
930
検証エンティティがM2MEを検証し、成功／失敗メッセージをその新たなホームネットワークオペレータに送信する
940
成功時に、その新たなホームネットワークオペレータが、新たなMIDをM2MEにダウンロード／プロビジョンするよう、PVAまたはDPFに要求する
950
PVAまたはDPFが、新たなMIDパッケージをM2MEにダウンロードする
960
M2MEが、MIDを破棄したというメッセージを以前のホームネットワークオペレータに送信する
970
以前のホームネットワークオペレータがM2MEにACKを送信し、次いでM2MEは、そのACKをPVAまたはDPFに転送し、その後新たなホームネットワークオペレータに転送する
980
M2MEが、PVAまたはDPFの助けで自らのシステムを更新／MIDをインストールし、成功／失敗メッセージを送り返す
990
PVAまたはDPFが、その成功／失敗メッセージを新たなホームネットワークオペレータに報告する
992
成功時に、このプロビジョニングプロセスは完了する
998

フロントページの続き

(31)優先権主張番号 61/031,630
(32)優先日 平成20年2月26日(2008.2.26)
(33)優先権主張国 米国(US)
(31)優先権主張番号 61/127,792
(32)優先日 平成20年5月14日(2008.5.14)
(33)優先権主張国 米国(US)
(31)優先権主張番号 61/060,725
(32)優先日 平成20年6月11日(2008.6.11)
(33)優先権主張国 米国(US)
(31)優先権主張番号 61/141,569
(32)優先日 平成20年12月30日(2008.12.30)
(33)優先権主張国 米国(US)
(31)優先権主張番号 61/141,586
(32)優先日 平成20年12月30日(2008.12.30)
(33)優先権主張国 米国(US)

(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
(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 チュートンウェグ ３７
(72)発明者 マイケル ブイ. マイヤーステイン
イギリス １ピー５ ３ティーユー マートルシャム ヒース イプスウィッチ メイフィールズ ２７

審査官 重田 尚郎

(56)参考文献 米国特許出願公開第２００７／０１５７０２２（ＵＳ，Ａ１）
米国特許出願公開第２００６／００７５２１６（ＵＳ，Ａ１）
特表２００７－５２２６９５（ＪＰ，Ａ）
3GPP TSG Service and System Aspects; Security of H(e)NB (Release 8), 3GPP TR 33.820 V1.2.0 (2008-12), ２００８年１２月１１日, ＵＲＬ, http://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_42/Docs/SP-080758.zip

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｗ ４／００－９９／００