(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5378603号
(P5378603)
(45)発行日　平成25年12月25日(2013.12.25)　(24)登録日　平成25年10月4日(2013.10.4)

(51)Int.Cl.　F I
H04W 12/06 (2009.01)　H04W 12/06
H04W 36/14 (2009.01)　H04W 36/14

請求項の数 10　(全 19 頁)

(21)出願番号　特願2012-526858 (P2012-526858)
(86)(22)出願日　平成22年8月20日 (2010.8.20)
(65)公表番号　特表2013-502879 (P2013-502879A)
(43)公表日　平成25年1月24日 (2013.1.24)
(86)国際出願番号　PCT/US2010/046118
(87)国際公開番号　WO2011/028442
(87)国際公開日　平成23年3月10日 (2011.3.10)
審査請求日　平成24年4月19日 (2012.4.19)
(31)優先権主張番号　61/275,008
(32)優先日　平成21年8月24日 (2009.8.24)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　12/652,315
(32)優先日　平成22年1月5日 (2010.1.5)
(33)優先権主張国　米国 (US)

(73)特許権者　391030332
アルカテル－ルーセント
フランス国、７５００７・パリ、　アブニュ・オクターブ・グレアール、　３
(74)代理人　110001173
特許業務法人川口國際特許事務所
(72)発明者　フエダー，ペレツ
アメリカ合衆国、ニユー・ジヤージー・０７６３１、エングルウツド、スターリング・ロード・３００
(72)発明者　ミジコフスキー，セミヨン
アメリカ合衆国、ニユー・ジヤージー・０７７５１、モルガンビル、イエローナイフ・ロード・２２７

最終頁に続く

(54)【発明の名称】複数技術インターワーキングでの事前登録セキュリティサポート

(57)【特許請求の範囲】
【請求項１】
通信システムのコンピューティングデバイスで使用するための方法であって、通信システムが、所与の通信デバイスが通信システムにアクセスすることを可能にするための２つ以上のアクセス技術をサポートし、所与の通信デバイスが第１アクセス技術を介して通信システムにアクセスすることを可能にする第１セキュリティコンテキストの少なくとも一部が所与の通信デバイスのためのコンピューティングデバイスで生成され、
第１セキュリティコンテキストを維持しながら所与の通信デバイスが少なくとも第２のアクセス技術を介して通信システムにアクセスするために事前登録されるように、そして所与の通信デバイスが第１アクセス技術を介して通信システムにアクセスすることを継続することができ、その後第２アクセス技術を介して通信システムにアクセスするために事前登録されるように、所与の通信システムのための少なくとも第２のセキュリティコンテキストのうちの少なくとも一部をコンピューティングデバイスで生成するステップを備え、
第２のセキュリティコンテキストが、第１アクセス技術から第２アクセス技術へのハンドオーバを行う決定がなされる前に生成される、方法。
【請求項２】
コンピューティングデバイスが、
所与の通信デバイスのための第１アクセス技術から、再認証手順の開始を求める要求を受信するステップと、

成功した再認証手順に応答して、第１アクセス技術のための所与の通信デバイスのために新しいセキュリティコンテキストの少なくとも一部を生成するステップと、
第１セキュリティコンテキストを新しいセキュリティコンテキストと置換するステップとをさらに備える、請求項１に記載の方法。
【請求項３】
コンピューティングデバイスが、第２セキュリティコンテキストを生成する前に、所与の通信デバイスが第２アクセス技術からのアクセスのために認可されているかどうかを検証するステップをさらに備える、請求項１に記載の方法。
【請求項４】
コンピューティングデバイスが、（ｉ）１つまたは複数のセキュリティコンテキストが失効する場合、および（ｉｉ）１つまたは複数のセキュリティコンテキストが１つまたは複数のアクセス技術で登録抹消される場合のうちの少なくとも１つの場合に、１つまたは複数のセキュリティコンテキストを削除するステップをさらに備える、請求項１に記載の方法。
【請求項５】
コンピューティングデバイスが、通信デバイスが通信システムにアクセスしているセッションが終了する場合に、任意の対応するセキュリティコンテキストを削除するステップをさらに備える、請求項１に記載の方法。
【請求項６】
通信デバイスが、第１アクセス技術を介して通信システムにアクセスしたものと同じ通信セッションの中で、第２アクセス技術を介して通信システムにアクセスする、請求項１に記載の方法。
【請求項７】
コンピューティングデバイスが、通信システムの中でネットワークサービスプロバイダによって管理される認証サーバを備える、請求項１に記載の方法。
【請求項８】
通信システムのコンピューティングデバイスで使用するための装置であって、通信システムが、所与の通信デバイスが通信システムにアクセスすることを可能にするための２つ以上のアクセス技術をサポートし、所与の通信デバイスが第１アクセス技術を介して通信システムにアクセスすることを可能にする第１セキュリティコンテキストの少なくとも一部が所与の通信デバイスのためのコンピューティングデバイスで生成され、
メモリと、
メモリに結合され、第１セキュリティコンテキストを維持しながら所与の通信デバイスが少なくとも第２のアクセス技術を介して通信システムにアクセスするために事前登録されるように、そして所与の通信デバイスが第１アクセス技術を介して通信システムにアクセスすることを継続することができ、その後第２アクセス技術を介して通信システムにアクセスするために事前登録されるように、所与の通信デバイスのための少なくとも第２のセキュリティコンテキストのうちの少なくとも一部をコンピューティングデバイスで生成するために構成されたプロセッサとを備え、
第２のセキュリティコンテキストが、第１アクセス技術から第２アクセス技術へのハンドオーバを行う決定がなされる前に生成される、装置。
【請求項９】
通信システムの通信デバイスで使用するための方法であって、通信システムが、通信デバイスが通信システムにアクセスすることを可能にするための２つ以上のアクセス技術をサポートし、通信デバイスが第１アクセス技術を介して通信システムにアクセスすることを可能にする第１セキュリティコンテキストの少なくとも一部が通信デバイスで生成され、
第１セキュリティコンテキストを維持しながら通信デバイスが少なくとも第２のアクセス技術を介して通信システムにアクセスするために事前登録されるように、そして通信デバイスが第１アクセス技術を介して通信システムにアクセスすることを継続することがで

き、その後第２アクセス技術を介して通信システムにアクセスするために事前登録されるように、通信デバイスのための少なくとも第２のセキュリティコンテキストのうちの少なくとも一部を通信デバイスで生成するステップを備え、
第２のセキュリティコンテキストが、第１アクセス技術から第２アクセス技術へのハンドオーバを行う決定がなされる前に生成される、方法。
【請求項１０】
通信システムの通信デバイスで使用するための装置であって、通信システムが、通信デバイスが通信システムにアクセスすることを可能にするための２つ以上のアクセス技術をサポートし、通信デバイスが第１アクセス技術を介して通信システムにアクセスすることを可能にする第１セキュリティコンテキストの少なくとも一部が通信デバイスで生成され、
メモリと、
メモリに結合され、第１セキュリティコンテキストを維持しながら通信デバイスが少なくとも第２のアクセス技術を介して通信システムにアクセスするために事前登録されるように、そして通信デバイスが第１アクセス技術を介して通信システムにアクセスすることを継続することができ、その後第２アクセス技術を介して通信システムにアクセスするために事前登録されるように、通信デバイスのための少なくとも第２のセキュリティコンテキストのうちの少なくとも一部を通信デバイスで生成するために構成されたプロセッサとを備え、
第２のセキュリティコンテキストが、第１アクセス技術から第２アクセス技術へのハンドオーバを行う決定がなされる前に生成される、装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本出願は、その開示が参照により本明細書に組み込まれている、２００９年８月２４日に出願した米国仮特許出願第６１／２７５，００８号「Ｍｅｔｈｏｄ ｆｏｒ Ｐｒｅ－Ｒｅｇｉｓｔｒａｔｉｏｎ Ｓｅｃｕｒｉｔｙ Ｓｕｐｐｏｒｔ ｉｎ Ｍｕｌｔｉ－Ｔｅｃｈｎｏｌｏｇｙ Ｉｎｔｅｒｗｏｒｋｉｎｇ」の優先権を主張するものである。
【０００２】
本発明は一般に通信システムでのセキュリティに関し、より詳細には複数アクセス技術環境での事前登録セキュリティサポートに関する。
【背景技術】
【０００３】
近年では、同等の性能で提供される通信システムアクセス技術の数が大幅に増加し、複数モードのワイヤレスアクセス端末を製造することを慎重にさせている。すなわち、３ＧＰＰ２－第３世代パートナーシッププロジェクト２によって定義されるＣＤＭＡ（符号分割多重アクセス）および１ｘＥＶ－ＤＯ（エボリューションデータ最適化）、ＧＳＭ（登録商標）（モバイル用グローバルシステム）、ＷＣＤＭＡとしても知られるＵＭＴＳ（ユニバーサルモバイルテレコミュニケーションシステム）、ＵＭＴＳのためのＧＰＲＳ（汎用パケット無線サービス）、３ＧＰＰ－第３世代パートナーシッププロジェクトによって定義されるＥＤＧＥ（ＧＳＭエボリューションのための進化型データレート）、ＷｉＦｉ（Ｗｉｒｅｌｅｓｓ Ｆｉｄｅｌｉｔｙ－ＩＥＥＥ８０２．１１規格に基づくワイヤレスローカルエリアネットワーク（ＷＬＡＮ）デバイスのクラス）、ＷｉＭＡＸ Ｆｏｒｕｍによって定義されるＷｉＭＡＸ（マイクロ波のための世界相互運用性）等で動作することが可能なモバイル端末に出会うことは珍しくない。２つ以上のアクセス技術間のインターワーキングは、ワイヤレスコアネットワーク事業者が共通のコアネットワークサービスを、複数モード端末を所有するユーザに提供することができることから、それらの事業者にとって重要なものとなる。
【０００４】
ワイヤレス端末がネットワークにアクセスすると、正当性が認証される。この認証は所

与のアクセス技術に固有であってもよいが、カプセル化認証プロトコル（ＥＡＰ）の急増とともに、アクセス技術に対してトランスペアレントな共通の認証フレームワークが普及するようになった。ＥＡＰは、その開示が参照により本明細書に組み込まれているＩＥＴＦ　ＲＦＣ５２４７、「Ｅｘｔｅｎｓｉｂｌｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ（ＥＡＰ）　Ｋｅｙ　Ｍａｎａｇｅｍｅｎｔ　Ｆｒａｍｅｗｏｒｋ」、２００８年８月の中で詳細に開示されている。

【０００５】

しかしながら、既存のＥＡＰ認証オペレーションは、多数のセキュリティコンテキストが、複数アクセス技術のための所与の通信デバイスに関して効果的に維持されるようにすることができない。したがって、このこと、および既存の認証方式の他の制限を克服する必要がある。

【先行技術文献】

【非特許文献】

【０００６】

【非特許文献１】ＩＥＴＦ　ＲＦＣ５２４７、「Ｅｘｔｅｎｓｉｂｌｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ（ＥＡＰ）　Ｋｅｙ　Ｍａｎａｇｅｍｅｎｔ　Ｆｒａｍｅｗｏｒｋ」、２００８年８月
【非特許文献２】ＷｉＭＡＸ　ＮＷＧステージ３仕様書、ＷＭＦ－Ｔ３３－００１－Ｒ０１５ｖ０１＿Ｎｅｔｗｏｒｋ－Ｓｔａｇｅ３－Ｂａｓｅ
【非特許文献３】ＩＥＴＦ　ＲＦＣ３３４４、ＩＰ　Ｍｏｂｉｌｉｔｙ　Ｓｕｐｐｏｒｔ　ｆｏｒ　ＩＰｖ４（ＭＩＰｖ４）、２００２年８月
【非特許文献４】ＲＦＣ３７７５、ＩＰ　Ｍｏｂｉｌｉｔｙ　Ｓｕｐｐｏｒｔ　ｆｏｒ　ＩＰｖ６（ＭＩＰｖ６）、２００４年６月
【非特許文献５】ＷｉＭＡＸフォーラムネットワークアーキテクチャ仕様書、１．５版
【非特許文献６】ＲＦＣ５２１３
【非特許文献７】ＷｉＭＡＸフォーラムネットワークアーキテクチャ、１．５版、ＰＭＩＰｖ６ステージ３仕様書
【非特許文献８】ＲＦＣ２１３１
【非特許文献９】ＩＥＴＦ　ＲＦＣ２８６５、「Ｒｅｍｏｔｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｄｉａｌ　Ｉｎ　Ｕｓｅｒ　Ｓｅｒｖｉｃｅ」、２０００年６月
【非特許文献１０】ＩＥＴＦ　ＲＦＣ４００５、「Ｄｉａｍｅｔｅｒ　Ｎｅｔｗｏｒｋ　Ａｃｃｅｓｓ　Ｓｅｒｖｅｒ　Ａｐｐｌｉｃａｔｉｏｎ」、２００５年８月
【非特許文献１１】ＷＭＦ－Ｔ３３－００ｘ－Ｒ０１５ｖ０１－Ｊ＿Ｎｅｔｗｏｒｋ－Ｓｔａｇｅ３＿Ｖ＆Ｖ
【非特許文献１２】ＩＥＥＥ８０２．１１ｉ仕様書

【発明の概要】

【発明が解決しようとする課題】

【０００７】

本発明の原理は、複数アクセス技術環境での事前登録セキュリティサポートを提供する。

【課題を解決するための手段】

【０００８】

例えば、１つの態様では、通信システムのコンピューティングデバイスで使用するための方法であって、通信システムが、通信デバイスが通信システムにアクセスすることを可能にするための２つ以上のアクセス技術をサポートし、所与の通信デバイスが第１アクセス技術を介して通信システムにアクセスすることを可能にする第１セキュリティコンテキストのうちの少なくとも一部が所与の通信デバイスのためのコンピューティングデバイスで生成される方法が提供される。この方法は、所与の通信デバイスが第１アクセス技術を介して通信システムにアクセスすることを継続することができ、その後第２アクセス技術を介して通信システムにアクセスするために事前登録されるように第１セキュリティコン

テキストを維持しながら、所与の通信デバイスが少なくとも第２のアクセス技術を介して通信システムにアクセスするために事前登録されるように、所与の通信デバイスのための少なくとも第２のセキュリティコンテキストのうちの少なくとも一部をコンピューティングデバイスで生成することを備える。このコンピューティングデバイスは、通信システムの中でネットワークサービスプロバイダによって管理される認証サーバを備えてもよい。

【０００９】

さらに他の態様では、通信システムの通信デバイスで使用するための方法であって、通信システムが、通信デバイスが通信システムにアクセスすることを可能にするための２つ以上のアクセス技術をサポートし、通信デバイスが第１アクセス技術を介して通信システムにアクセスすることを可能にする第１セキュリティコンテキストのうちの少なくとも一部が通信デバイスで生成される方法が提供される。この方法は、所与の通信デバイスが第１アクセス技術を介して通信システムにアクセスすることを継続することができ、その後第２アクセス技術を介して通信システムにアクセスするために事前登録されるように第１セキュリティコンテキストを維持しながら、所与の通信デバイスが少なくとも第２のアクセス技術を介して通信システムにアクセスするために事前登録されるように、所与の通信デバイスのための少なくとも第２のセキュリティコンテキストのうちの少なくとも一部を通信デバイスで生成することを備える。

【００１０】

有利にも、本発明の例示的原理は、複数アクセス技術での同時モバイル登録を可能にするために、複数アクティブの明確に識別可能なセキュリティアソシエーションを維持する技術を提供する。

【００１１】

本発明のこれら、およびその他の目的、特徴ならびに利点は、添付の図面と併せて読まれるべき以下の本発明の例示的実施形態の詳細な説明から、明らかになるであろう。

【図面の簡単な説明】

【００１２】

【図１】本発明の１つまたは複数の実施形態による、複数アクセス技術環境の中の事前登録セキュリティサポートを組み込んだネットワーク参照モデルを示す図である。

【図２Ａ】本発明の１つの実施形態による第１アクセス技術のためのネットワークエントリー手順を示す図である。

【図２Ｂ】本発明の１つの実施形態による第２アクセス技術のためのネットワークエントリー手順を示す図である。

【図２Ｃ－１】本発明の１つの実施形態による複数アクセス技術環境の中の事前登録セキュリティサポートのための手順を示す図である。

【図２Ｃ－２】本発明の１つの実施形態による複数アクセス技術環境の中の事前登録セキュリティサポートのための手順を示す図である。

【図２Ｄ－１】本発明の他の実施形態による複数アクセス技術環境の中の事前登録セキュリティサポートのための手順を示す図である。

【図２Ｄ－２】本発明の他の実施形態による複数アクセス技術環境の中の事前登録セキュリティサポートのための手順を示す図である。

【図３】本発明の１つまたは複数の実施形態による、複数アクセス技術環境の中で事前登録セキュリティサポートを実施するために適した通信システムの一部分の汎用ハードウェアアーキテクチャを示す図である。

【発明を実施するための形態】

【００１３】

「通信システム」という語句は一般に、通信デバイスおよび／またはネットワークノードが他の通信デバイスおよび／またはネットワークノードと通信／対話することを可能にし、それらを通して１つまたは複数の種類の媒体が輸送されることが可能な、１つまたは複数の通信ネットワークを含むように定義される。そのような１つまたは複数の種類の媒体（すなわちマルチメディア）は、限定されないが、テキストベースデータ、グラフィッ

クベースデータ、音声ベースデータ（より一般的にはオーディオ型データ）およびビデオベースデータを含んでもよい。

【００１４】

さらに以下では、複数アクセス技術のために事前登録サポートを提供する本発明の例示的実施形態が２つの例示的アクセス技術であるＷｉＭＡＸおよびＷｉＦｉに関して説明されているが、本発明はこれらの２つのアクセス技術に限定されず、また２つのアクセス技術とだけ使用することに限定されないということを理解されたい。すなわち本発明の原理は、限定されないがＣＤＭＡ、ＧＳＭ、ＵＭＴＳ、１ｘＥＶ－ＤＯ、ＧＰＲＳおよびＥＤＧＥなどの多くの異なるその他のアクセス技術に適用されてもよい。また、本発明の原理はＥＡＰフレームワークで使用することに限定されないということも理解されたい。

【００１５】

さらに「セキュリティコンテキスト」および「セキュリティアソシエーション」という語句は本明細書ではほとんど同じ意味で使用され、一般に、通信システムに対してエンティティを認証する目的で生成される（例えば１つまたは複数のキーなどの）暗号化およびセキュアデータを指すものとして定義される。

【００１６】

また「サーバ」は本明細書で使用する際、一般に１つまたは複数のコンピューティングデバイスとして定義される。さらに「ノード」は、通信システムの中の専用コンピューティングデバイスのことを指すか、または１つまたは複数の他の機能を実行するコンピューティングデバイスの機能部分のことを指してもよいということを理解されたい。

【００１７】

例示的実施形態によって、（例えばモバイル端末などの）通信デバイスは、現在アクセスしているネットワークに対して認証を行うためにＥＡＰを使用することができ、また他の利用可能なサポートされる技術への起こりうるハンドオフを見越して、そのアクセス技術に予め事前登録および事前認証することができる。このようにして、１つのアクセス技術から他のアクセス技術への通信セッションのハンドオフを決定するときには、対象とする技術の資源はすでに認可されており、ハンドオフプロセスの待ち時間は大幅に削減される。

【００１８】

ここで、論点となっている複数アクセス技術がＷｉＦｉとＷｉＭＡＸを含む例示的実施形態について説明する。前述の例示的実施形態によって、２つの異種のアクセスネットワーク（アクセス技術）で重複する期間の同じＨｏＡ（ホームアドレス）セッションのために、同じＥＡＰ認証方式を同時に実行することが可能である。継ぎ目のないＨＯ（ハンドオフ）を維持するために、この方式には両方のネットワークのために３つの共通のエンティティ、すなわちＭＳ（移動局）およびそのサプリカント、ＡＡＡ（認証、認可および課金）サーバならびにＨＡ（ホームエージェント）サーバが伴う。

【００１９】

「サプリカント」は本明細書で使用する際、安全なアクセスサポート機能を実行するＭＳ（通信デバイス）の一部、すなわち通信システムへアクセスするためのセキュリティコンテキストの作成に関与するＭＳの中の機能エンティティのことを指すということを理解されたい。以下に示すように、本発明の原理によって、通信デバイスは複数のサプリカントのインスタンスを作成し、それによって各サプリカントは別個のセキュリティコンテキストを作成して維持する。例えば、１つのサプリカントは第１アクセス技術に関連した第１セキュリティコンテキストを作成し、第２サプリカントは第２アクセス技術に関連した第２セキュリティコンテキストを作成してもよい。１つまたは複数のサプリカントは、実行可能命令符号、ハードウェア、またはそれらの組み合わせとしてＭＳの中で実装されてもよい。

【００２０】

図１は、ＷｉＭＡＸおよびＷｉＦｉネットワークの間のインターワーキングのためのネットワーク参照モデル（ＮＲＭ）１００の例を示す。「ネットワーク」または「通信ネッ

トワーク」という用語は、本明細書では特定のアクセス技術に関して使用されているが、複数アクセス技術は「通信システム」全体のうちの一部と見なされることを理解されたい。

【００２１】

ＮＲＭ１００では、同一の複数モードワイヤレス端末（通信デバイス）ＭＳ１０２がＷｉＭＡＸ技術とＷｉＦｉ技術の両方へのアクセスをサポートし、ＷｉＭＡＸネットワークへのアクセスがＲ１無線インターフェースを通じて行われることが仮定されている。ネットワークアクセスプロバイダ（ＮＡＰ）１０６に属するアクセスサービングネットワーク（ＡＳＮ）１０４は、バックホールＩＰ（インターネットプロトコル）ベースのＲ３インターフェースを通じて、ネットワークサービスプロバイダ（ＮＳＰ）１１０に属するコアサービングネットワーク（ＣＳＮ）１０８に相互接続性を提供する。

【００２２】

ＩＰセッションは、ＣＳＮ１０８の中でＭＳ１０２とホームＡＡＡサーバ１１２の間の成功した認証を通じて認可される。この成功した認証の結果、ＡＡＡサーバ１１２およびＭＳ１０２は相互にセキュリティアソシエーション（セキュリティコンテキスト）のセット、すなわち秘密キーをアクセスおよび移動性のセキュリティのために生成する。１つの実施形態では、そのようなセキュリティアソシエーションは、その開示が参照により本明細書に組み込まれているＷｉＭＡＸ　ＮＷＧステージ３仕様書、ＷＭＦ－Ｔ３３－００１－Ｒ０１５ｖ０１＿Ｎｅｔｗｏｒｋ－Ｓｔａｇｅ３－Ｂａｓｅの中で定義されているように生成される。しかしながら、本発明はこれらの特定のセキュリティアソシエーションまたはコンテキストとともに使用することに限定されない。

【００２３】

アクセスセキュリティアソシエーションは、ＡＡＡサーバ１１２によってＡＳＮ－ＧＷ（アクセスサービスネットワークゲートウェイ）サーバ１１４のオーセンティケータ機能に届けられるマスターセッションキー（ＭＳＫ）に基づく。このオーセンティケータは、Ｒ１無線インターフェース上で暗号化および完全性保護のための特殊キーのセットを生成するためにＭＳＫを使用する。

【００２４】

ＭＳＫに加えて、ＭＳ１０２およびＡＡＡサーバ１１２もまた、ＡＡＡサーバを決して離れることのない拡張マスターセッションキー（ＥＭＳＫ）を生成する。このＥＭＳＫは、移動性を保護するための特殊ルートキー、ＭＩＰ－ＲＫ（モバイルＩＰルートキー）を生成するために使用される。ＭＩＰ－ＲＫは次いで、モバイルＩＰノード間でモバイルＩＰメッセージの安全な署名を生成する方法によって、（その開示が参照により本明細書に組み込まれているＩＥＴＦ　ＲＦＣ３３４４、ＩＰ　Ｍｏｂｉｌｉｔｙ　Ｓｕｐｐｏｒｔ　ｆｏｒ　ＩＰｖ４（ＭＩＰｖ４）、２００２年８月によって定義されるような）モバイルＩＰシグナリングを保護するために使用される。ＩＰｖ６のためのＩＰモバイルサポートは、その開示が参照により本明細書に組み込まれているＲＦＣ３７７５、ＩＰ　Ｍｏｂｉｌｉｔｙ　Ｓｕｐｐｏｒｔ　ｆｏｒ　ＩＰｖ６（ＭＩＰｖ６）、２００４年６月の中で定義されていることに留意されたい。

【００２５】

具体的には、ＭＳ１０２のモバイルノード（ＭＮ）とＣＳＮ１０８のホームエージェント（ＨＡ）１１６の間のメッセージは、ＭＩＰ－ＲＫから生成されたＭＮ－ＨＡキーを使用するＭＮ－ＨＡ認証拡張子によって保護される。ＭＮとＡＳＮ－ＧＷサーバ１１４のフォーリンエージェント（Ｆｏｒｅｉｇｎ　Ａｇｅｎｔ）（ＦＡ）の間のメッセージは、ＭＩＰ－ＲＫ等から作り出されたＭＮ－ＦＡキーを使用するＭＮ－ＦＡ認証拡張子によって保護される。

【００２６】

「単純な」ＩＰモバイル端末をサポートするために、アクセスネットワークのノードにＭＮ機能が配置されることも可能である。このいわゆるプロキシモバイルＩＰ機能（ＰＭＩＰ）は、モバイルが１つのＡＳＮから他のものへ移動するときにモバイルを追尾し、モ

バイルをＨＡに再登録し、したがってＨＡ上でのＩＰセッションの連続性を維持する。ＰＭＩＰ　ＭＮのためのＭＮ－ＨＡキーは通常、ＥＡＰアクセス認証の成功した結果を示すＡＡＡシグナリングとともにＡＳＮのＰＭＩＰ　ＭＮに届けられる。

【００２７】

図２Ａは、アクセス技術がＷｉＭＡＸである場合のための初期ネットワークエントリー手順２００の１つの実施形態を示す。示されているように、列挙された手順２００のステップを参照すると：

１．ＷｉＭＡＸ　ＭＳ（通信デバイス）２０１は、例えば、その開示が参照により本明細書に組み込まれているＷｉＭＡＸフォーラムネットワークアーキテクチャ仕様書、１．５版によって、ＷｉＭＡＸ　ＢＳ（基地局）２０２に接続し、ＷｉＭＡＸ接続を確立する。

２．ＭＳ２０１はＰＫＭｖ２および、以下のもの：ＥＡＰ－ＴＬＳ／ＴＴＬＳ／ＣＨＡＰｖ２／ＡＫＡのうちの任意のものを含むことが可能なＥＡＰ方法を使用してＷｉＭＡＸ　ＡＳＮ２０３に対して認証を行う。ＭＳ２０１は自身を、アクセス認証の間にＮＡＩを用いて識別する。ＷｉＭＡＸ　ＡＳＮ２０３は、アクセス技術を識別するためのＡＡＡ要求の中にＮＡＳ型を含む。このＥＡＰ認証および認可ステップの終わりに、ＭＳ２０１でＭＳＫが生成され、ＡＡＡ２０５からＷｉＭＡＸ　ＡＳＮ２０３（ＡＳＮ－ＧＷオーセンティケータ）へ届けられる。

３．次いでＭＳ２０１は、８０２．１６（ＷｉＭＡＸ）ネットワークに登録する。

４．次いでＭＳ２０１は、ＤＳＡ（動的サービス追加）要求／応答を使用してサービスフローを確立し、またＡＳＮ２０３へのデータ経路登録を完了する。

５．ＭＳは、ホストＩＰ構成のためのＤＨＣＰ（動的ホスト構成プロトコル）サーバを発見するために、ＤＨＣＰＤＩＳＣＯＶＥＲメッセージを送信する。

６．ＡＳＮ２０３の中のモビリティアクセスゲートウェイ（ＭＡＧ）のＰＭＩＰｖ４クライアントまたはＰＭＩＰｖ６クライアントは、登録手順を開始するように起動される。ＥＡＰ認証手順の間に使用されたものと同じＮＡＩは、ＭＩＰ　ＲＲＱまたはＢｉｎｄｉｎｇ　Ｕｐｄａｔｅメッセージの中で使用される。オプションの同時結合がサポートされ、起動されない限り、ＰＭＩＰｖ４　ＲＲＱメッセージでは、「Ｓ」ビットが「０」に設定される。ＰＭＩＰｖ６　ＰＢＵメッセージについては、ハンドオフインジケータオプションは値「１」（新しいインターフェースを介した添付）に設定されてもよく、アクセス技術型オプションは、その開示が参照により本明細書に組み込まれているＲＦＣ５２１３の中に明記されているように、値「５」（ＩＥＥＥ８０２．１６ｅ）に設定されてもよい。フィールドの残りの部分は、その開示が参照により本明細書に組み込まれている、ＷｉＭＡＸフォーラムネットワークアーキテクチャ、１．５版、ＰＭＩＰｖ６ステージ３仕様書に従って初期化される。一般にＭＩＰｖ４用語に関して知られているように、ＭＩＰｖ４クライアント、フォーリンエージェント（ＦＡ）およびホームエージェント（ＨＡ）が存在する。ＭＩＰｖ６用語では、ＭＩＰｖ６クライアントとホームエージェント（ＨＡ）は存在するが、ＦＡは存在しない。プロキシＭＩＰｖ４では、ＭＩＰｖ４クライアントはＦＡと同じ場所に設置される。ＰＭＩＰｖ６では、ＰＭＩＰｖ６クライアントはＭＡＧと呼ばれるネットワーク要素の中に置かれ、ＨＡはローカルモビリティエージェント（ＬＭＡ）と呼ばれる。

７．ＳＰＩ（セキュリティパラメータインデックス）によって識別されたＭＮ－ＨＡキーが利用可能でない場合、ＨＡ２０４はＡＡＡ２０５からＭＮ－ＨＡキーを要求する。

８．ＭＮ－ＨＡ　ＳＰＩに関連したＭＮ－ＨＡキーは、ＭＮ－ＨＡ　ＡＥ検証のためにＨＡ２０４に返送される。

９．ＨＡ／ＬＭＡ２０４は、ＰＭＩＰ　ＲＲＰまたはＰＭＩＰ　ＰＢＵメッセージに応答する。一旦ＭＮ－Ａ　ＡＥが検証されると、ＨＡ／ＬＭＡ２０４はＩＰアドレスをＭＳ２０１に割り当てる。割り当てられたＭＩＰ　ＲＲＱ／ＰＢＵの中のＨｏＡ値が０．０．０．０である場合、ＨＡ２０４はＨｏＡを割り当て、そうでない場合にはＰＭＩＰ登録要求／ＰＢＵの中のＨｏＡが使用される。これがＭＳ２０１のための最初のエントリーであ

る場合、ＨＡ／ＬＭＡ２０４はＭＳ２０１のために結合キャッシュを作成する。この時点で、ＡＳＮ２０３とＨＡ／ＬＭＡ２０４の間でＰＭＩＰトンネルが確立される。

１０．ＡＳＮ２０３の課金クライアントはＡｃｃｔ－Ｒｅｑｕｅｓｔ（ｓｔａｒｔ）メッセージをＡＡＡ２０５に送信する。

１１．課金要求メッセージを受信すると、ＡＡＡ２０５はＡｃｃｔ－Ｒｅｓｐｏｎｓｅメッセージを課金クライアントに送信する。

１２．ＡＳＮ２０３のＤＨＣＰプロキシは、ＤＨＣＰＯＦＦＥＲメッセージをＭＳ２０１に送信する。

１３．ＭＳ２０１は、ＤＨＣＰＯＦＦＥＲで受信されたアドレス情報に加えて、ＤＨＣＰプロキシへのＤＨＣＰＲＥＱＵＥＳＴメッセージとともに受信された第１ＤＨＣＰＯＦＦＥＲメッセージに応答する。

１４．ＤＨＣＰプロキシは、このＩＰアドレス、および、その開示が参照により本明細書に組み込まれているＲＦＣ２１３１で定義されているようなその他の構成パラメータの使用を、ＤＨＣＰＡＣＫメッセージを送信することによって承認する。

１５．ここでＭＳ２０１は、アップリンク／ダウンリンクトラフィックが交換されることが可能なように、ＷｉＭＡＸネットワークに接続される。

【００２８】

同様の概念は、ＭＳ１０２が、この例の中でのＩＥＥＥ８０２．１１のＷｉＦｉプロトコルなどの他のアクセス技術を通じて動作する場合に使用される。ＥＡＰアクセス認証の結果として生成されるＭＳＫが、ＩＷＫ機能１２０と呼ばれる特殊インターフェースノードのワイヤレスインターフェース機能（ＷＩＦ）１１８に配置される認証機能に届けられる場合を除いて、ＥＡＰ認証は依然としてＭＳ１０２とＡＡＡサーバ１１２の間で実行される。ＩＷＫ１２０に配置されるＰＭＩＰ機能のためのＭＮ－ＨＡキーもまた、Ｒ３＋インターフェースを介してＡＡＡ１１２から届けられる。

【００２９】

図２Ｂは、アクセス技術がＷｉＦｉである場合のための初期ネットワークエントリー手順２２０の１つの実施形態を示す。示されているように、列挙された手順２２０のステップを参照すると：

１．ＷｉＦｉ　ＳＴＡ（通信デバイス）２２１は電源を入れられてＷｉＦｉシグナリングを捕らえ、次いでネットワークの発見および選択を実行する。

２．ＳＴＡ２２１は、ＷｉＦｉ　ＡＮ２２２との８０２．１１アソシエーションを確立する。

３．ＳＴＡ２２１は８０２．１Ｘ／ＥＡＰＯＬ、およびＥＡＰ－ＴＬＳおよびＥＡＰ－ＡＫＡなどの様々なＥＡＰ方法を使用して、ＷｉＦｉ　ＡＮ２２２に対して認証を行う。ＷｉＦｉ　ＡＮ２２２は、後でＷｉＦｉ　ＳＴＡ２２１の代わりに認証を促進するＷＩＦ２２３のＡＡＡプロキシにＥＡＰメッセージを転送する。ＷＩＦ２２３からのＡＡＡ要求は、アクセス技術を識別するＮＡＳ型を含む。認証の間、ＡＡＡサーバ２２５で生成されたＭＳＫはＷｉＦｉ　ＡＮ２２２に転送され、次いでＷｉＦｉ認証の終わりに、ＰＭＫまたはペアマスターキー（Ｐａｉｒｗｉｓｅ　Ｍａｓｔｅｒ　Ｋｅｙ）（エアインターフェースセキュリティのために使用される２番目のキー）はＷｉＦｉ　ＡＮ２２２のＭＳＫから導き出される。

ＷｉＭＡＸ－Ｓｅｓｓｉｏｎ－ＩＤおよびＣＵＩ（課金可能ユーザＩＤ）は、ＷＩＦ２２３の課金クライアントに届けられる。

４．次いでＳＴＡ２２１は、ＷｉＦｉ　ＡＮ２２２のオーセンティケータとともに、フォーウェイハンドシェイクを実施する。フォーウェイハンドシェイク手順の間、新しいペア一時キー（Ｐａｉｒｗｉｓｅ　Ｔｒａｎｓｉｅｎｔ　Ｋｅｙ）（ＰＴＫ）がＰＭＫから導き出される。フォーウェイハンドシェイクが首尾よく完了すると、８０２．１ｘポートはブロック解除される。

５．ＳＴＡ２２１は、ホストＩＰ構成のためのＤＨＣＰサーバを発見するために、ＤＨＣＰＤＩＳＣＯＶＥＲメッセージを送信する。

６．ＷＩＦ２２３の中のＦＡ／ＭＡＧは、ＰＭＩＰ登録手順を開始するように起動される。ＥＡＰ認証手順の間に使用されたものと同じＮＡＩは、ＲＲＱ／Ｂｉｎｄｉｎｇ Ｕｐｄａｔｅメッセージの中で使用される。オプションの同時結合がサポートされ、起動されない限り、ＲＲＱメッセージでは、「Ｓ」ビットが「０」に設定される。ＰＢＵメッセージについては、ハンドオフインジケータオプションは値「１」（新しいインターフェースを介した添付）に設定されてもよく、アクセス技術型オプションは、ＲＦＣ５２１３の中に明記されているように、（ＩＥＥＥ８０２．１１ａ／ｂ／ｇを示す）値「４」に設定されてもよい。フィールドの残りの部分は、上述のものと同じ方法で初期化される。

７．ＳＰＩによって識別されたＭＮ－ＨＡキーが利用可能でない場合、ＨＡ２２４はＡＡＡ２２５からＭＮ－ＨＡキーを要求する。

８．ＭＮ－ＨＡ　ＳＰＩに関連したＭＮ－ＨＡキーは、ＭＮ－ＨＡ　ＡＥ検証のためにＨＡ２２４に返送される。

９．ＨＡ／ＬＭＡ２２４は、ＲＲＰ／ＰＭＩＰ　ＰＢＵメッセージに応答する。一旦ＭＮ－Ａ　ＡＥが検証されると、ＨＡ／ＬＭＡ２２４はＩＰアドレスをＳＴＡ２２１に割り当てる。割り当てられたＭＩＰ　ＲＲＱ／ＰＢＵの中のＨｏＡ値が０．０．０．０である場合、ＨＡ２２４はＨｏＡを割り当て、そうでない場合にはＰＭＩＰ登録要求／ＰＢＵの中のＨｏＡが使用される。これがＳＴＡ２２１のための最初のエントリーである場合、ＨＡ／ＬＭＡ２２４はＳＴＡ２２１のために結合キャッシュを作成する。この時点で、ＷＩＦ２２３とＨＡ／ＬＭＡ２２４の間でＰＭＩＰトンネルが確立される。

１０．ＷＩＦ２２３の課金クライアントはＡｃｃｔ－Ｒｅｑｕｅｓｔ（ｓｔａｒｔ）メッセージをＡＡＡ２２５に送信する。

１１．課金要求メッセージを受信すると、ＡＡＡ２２５はＡｃｃｔ－ＲｅｓｐｏｎｓｅメッセージをＷＩＦ２２３の課金クライアントに送信する。

１２．ＷＩＦ２２３のＤＨＣＰプロキシは、ＤＨＣＰＯＦＦＥＲメッセージをＳＴＡ２２１に送信する。

１３．ＳＴＡ２２１は、ＤＨＣＰＯＦＦＥＲで受信されたアドレス情報に加えて、ＤＨＣＰプロキシへのＤＨＣＰＲＥＱＵＥＳＴメッセージとともに受信された第１ＤＨＣＰＯＦＦＥＲメッセージに応答する。

１４．ＷＩＦ２２３のＤＨＣＰプロキシは、このＩＰアドレス、およびその他の構成パラメータの使用を承認する。

１５．ここでＳＴＡ２２１は、アップリンク／ダウンリンクトラフィックが交換されることができるように、ＷｉＦｉネットワークに接続される。

【００３０】

他のアクセス技術を通して依然として動作中でありながら、１つのアクセス技術に事前登録することが、通信デバイス（ＭＳ／ＳＴＡ）にとって望ましい場合があることが認識されよう。このことは、トンネルを作って対象とするアクセス技術のシグナリングを現在サービス中のアクセス技術のシグナリングカプセルの中に通し、このカプセル化されたシグナリングを、ＩＷＫ機能を通じて対象とするアクセス技術に届けることによって達成されてもよい。

【００３１】

しかしながら既存のＥＡＰオペレーションによれば、このシグナリングは対象とするアクセス技術に達するときに、アクセスの認証を試み、そうする間に新しいＭＳＫおよび新しいＥＭＳＫを含む新しいセキュリティアソシエーションを生成する。この新しいＭＳＫはＩＷＫに届けられ、ＭＳ／ＳＴＡが実際に対象とする技術へのハンドオフを実行するまで、そのオーセンティケータの中に保持されることが可能である。しかしながら既存のＥＡＰオペレーションでは、ＡＡＡの中のＥＭＳＫは現在のセッションに関連した現時点でアクティブのＥＭＳＫを置換し、ＭＩＰ－ＲＫなどのＥＭＳＫから計算された全ての第２キーもまた再計算されることになる。

【００３２】

これによって、ネットワークによって想定されるセキュリティアソシエーションとモバ

イルによって処理されるセキュリティアソシエーションとの間に格差が生じ、したがって接続が切断する。

【００３３】

この問題に対処するために、本発明の例示的原理は有利にも、複数アクセス技術での同時モバイル登録を可能にするために、複数アクティブの明確に識別可能なセキュリティアソシエーション（コンテキスト）を維持するために動作する。

【００３４】

本発明の例示的実施形態によって、ＡＡＡサーバ１１２はアクセス認証を求める要求を受信すると、どのアクセス技術からこの要求が来たのかを示す（ＡＳＮ－ＧＷサーバ１１４またはＷＩＦ１１８の中の）オーセンティケータのＮＡＳ（ネットワークアクセスサーバ）型を確認する。ＮＡＳ型は、ＡＡＡ　ＲＡＤＩＵＳ（その開示が参照により本明細書に組み込まれているＩＥＴＦ　ＲＦＣ２８６５、「Ｒｅｍｏｔｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｄｉａｌ　Ｉｎ　Ｕｓｅｒ　Ｓｅｒｖｉｃｅ」、２０００年６月）およびダイアメータ（その開示が参照により本明細書に組み込まれているＩＥＴＦ　ＲＦＣ４００５、「Ｄｉａｍｅｔｅｒ　Ｎｅｔｗｏｒｋ　Ａｃｃｅｓｓ　Ｓｅｒｖｅｒ　Ａｐｐｌｉｃａｔｉｏｎ」、２００５年８月）のシグナリングの標準的属性である。技術固有の情報を伴うＡＡＡシグナリングを強化するためのいくつかのベンダー固有属性（ＶＳＡ）は、各々のアクセス技術基準の中で定義される。例えば、ＷｉＭＡＸフォーラムはその固有のＶＳＡを、その開示が参照により本明細書に組み込まれているステージ３文書、ＷＭＦ－Ｔ３３－００ｘ－Ｒ０１５ｖ０１－Ｊ＿Ｎｅｔｗｏｒｋ－Ｓｔａｇｅ３＿Ｖ＆Ｖの中で定義している。

【００３５】

オペレーションの中で、これが最初のネットワークアクセスであり、ＡＡＡサーバが、いかなるこのモバイルのための現時点でアクティブのセキュリティコンテキストも持たない場合、ＡＡＡサーバは通常のＥＡＰ認証手順を実施し、結果として生じるセキュリティコンテキストをアクティブとして保存する。すなわち上記のように、ＭＳＫは生成されてオーセンティケータに届けられ、ＥＭＳＫは生成されて保存され、ＥＭＳＫに関連した固有セキュリティパラメータインデックス（ＳＰＩ）は生成されて保存され、ＭＩＰ－ＲＫおよびそのＳＰＩは生成されて保存され、ＭＮ－ＨＡおよびその関連ＭＮ－ＨＡ　ＳＰＩは生成されて保存される。

【００３６】

オペレーションの中で、ＡＡＡサーバはすでにこのアクセス技術のためのセキュリティコンテキストを持つ場合、再認証を実施し、古いコンテキストを新しいコンテキストと置き換える。

【００３７】

しかしながら本発明の実施形態による改良型のオペレーションでは、ＡＡＡサーバはすでにこのアクセス技術のためのセキュリティコンテキストを持つ場合、再認証を実施し、このアクセス技術のためだけに古いコンテキストを新しいコンテキストと置き換え、その他の利用可能なセキュリティコンテキストをそのまま残す。

【００３８】

本発明の実施形態によるさらなる改良型オペレーションでは、ＡＡＡサーバがすでにこのモバイルのためのセキュリティコンテキストを持っているが、他のアクセス技術から要求が着ている場合、ＡＡＡサーバは、このモバイルのサブスクリプション記録を確認して、そのモバイルが対象とするアクセス技術からのアクセスが可能であり、そのために認可されているかどうかを検証し、そうでない場合要求を拒否する。

【００３９】

本発明の実施形態による他の改良型オペレーションでは、要求が複数モードＭＳに関連しており、アクセス技術がこのモバイルのためにサポートされ、認可される場合、ＡＡＡサーバはＥＡＰアクセス認証を実施して、現在サービス中の技術のためのすでに存在しているコンテキストと同時に、新しいコンテキストを保存する。

【００４０】
本発明の実施形態によるさらなる改良型オペレーションでは、要求が、ＨＡによって要求されるＭＮ－ＨＡキーなどのコンテキスト関連のパラメータのためにＡＡＡサーバに来る場合、ＡＡＡサーバは、要求に含まれる関連したＳＰＩに基づいて、どのコンテキストを使用するのかを判定する。
【００４１】
本発明の実施形態によるさらなる改良型オペレーションでは、固有のセキュリティコンテキストがその存続期間の終了、固有のアクセス技術での登録抹消、または任意のポリシー関連の制限のために失効する場合、ＡＡＡサーバは、他のアクティブのコンテキストを有効のままにしておきながら、この固有コンテキストを削除する。
【００４２】
本発明の実施形態によるさらなる改良型オペレーションでは、セッションが終了した後、全ての関連したセキュリティコンテキストは削除される。
【００４３】
同様の機能的論理は、複数モードモバイルデバイス（ＭＳ）が固有のアクセス技術にアクセスし、事前登録し、そのために認証される際に、固有のアクセス技術のためのセキュリティコンテキストを生成するＭＳに適用される。
【００４４】
したがって本発明の例示的原理は、同一のセッションのための任意の所与の時間に、ＭＳ（通信デバイス）と通信システムの間の複数アクティブのセキュリティアソシエーションを生成して、維持し、これらのコンテキスト、それらの使用、それらの置換およびそれら非推奨を明確に区別する方法を提供する。このように、１つの技術から他の技術へのハンドオフの性能を犠牲にすることなく、多数の対象とする技術への事前登録を可能にする。
【００４５】
したがって、本発明の例示的原理によって、アクティブモードでＷｉＭＡＸまたはＷｉＦｉアクセスネットワークのいずれかに接続されながら、ＷｉＭＡＸ／ＷｉＦｉ通信デバイスは代替アクセス技術（すなわちＷｉＦｉまたはＷｉＭＡＸ）に対して事前登録および事前認証することができる。アクティブのサービス中ネットワークでセキュリティコンテキストを維持するために、事前登録および事前認証が実行される異なるアクセス技術に関連した、同じデバイスのための第２セキュリティコンテキストをＡＡＡは生成する。
【００４６】
同じＮＡＩ（ネットワークアクセス識別子）を使用して、各アクセス技術のための固有のセキュリティコンテキストを生成するために、各ＮＡＳは認証ネットワークへのＡＡＡ要求メッセージの中でその型を報告する。ＡＡＡはＡＡＡ要求メッセージを受信すると、例えばネットワークアクセスサーバ（ＮＡＳ）型などの報告されたアクセスネットワークの型を確認し、モバイルのＮＡＩに基づいて、要求が最初のネットワークアクセスのためのものなのか、またはデバイスのためのさらなるセキュリティコンテキストを必要とする事前登録のためのものなのかを判定する。
【００４７】
最初のネットワークアクセスのために、ＡＡＡはＥＡＰ認証手順を実施し、結果として生じるセキュリティコンテキストおよびその関連したセキュリティパラメータインデックス（ＳＰＩ）をデバイスのためのアクティブのものとして保存する。同様に、ＭＳは計算されたセキュリティコンテキストを最初のネットワークアクセスに関連付ける。
【００４８】
異なるアクセス技術での事前登録の間に、二重モードデバイスのサプリカントは、（これもまた第２サプリカントによって処理されることが可能な）異なるアクセス技術に関連した第２セキュリティコンテキストを作り出す。同様にＡＡＡは、デバイスが事前登録しているアクセス技術に関連した同じセッションのために第２セキュリティコンテキストを作り出す。

【００４９】
アクティブセッションの間に、ＡＡＡがすでに存在しているセキュリティコンテキストに関連した同じアクセス技術、すなわち同じＮＡＩおよび（ＮＡＳ型を通じて示される）同じアクセス技術からＡＡＡ要求を受信する場合、ＡＡＡは再認証を実施して、このセキュリティコンテキストを新しく生成されたものと置換する。
【００５０】
ＡＡＡがすでにデバイスのためのセキュリティコンテキストを持っているが、ＡＡＡ要求が異なるアクセス技術から来る場合、ＡＡＡはデバイスのサブスクリプション記録を確認して、それが対象とするアクセス技術からのアクセスのために認可されているかどうかを検証し、その場合ＡＡＡはＥＡＰアクセスの事前認証を実施する。ＥＡＰ認証が首尾よく完了すると、ＡＡＡはその関連のＳＰＩとともに第２セキュリティコンテキストを生成し、それをアクティブのセキュリティコンテキストと同時に保存する。
【００５１】
モバイルが異なるアクセス技術へのアクセスを認可されない場合、ＡＡＡはＡＡＡ要求を拒否する。
【００５２】
多数のネットワーク型（複数モードデバイス）にアクセスすることができるデバイスのために、固有のセキュリティコンテキストが存続期間の終了、またはアクセス技術のうちの１つでの登録抹消のために失効する場合、ＡＡＡおよびＭＳ／ＳＴＡは他の有効なコンテキストを保持しながら失効したコンテキストを削除する。
【００５３】
複数モードデバイスについては、セッションが終了する場合、全ての関連したセキュリティコンテキストはＡＡＡ、ＮＡＳおよびＭＳで削除される。
【００５４】
図２Ｃは、ＷｉＭＡＸネットワークから８０２．１１ｉ　ＷｉＦｉネットワークへのハンドオーバ手順２４０の１つの実施形態を示す。このシナリオでは、最初にＭＳ／ＳＴＡ二重モード単一無線（単一無線とは、１つのみのトランスミッタＷｉＦｉまたはＷｉＭＡＸが任意の所与の時間に送信することができることを意味することに留意されたい）がＷｉＭＡＸネットワークに接続されることが仮定されている。さらに、ＭＳはＷｉＦｉネットワークの利用可能性およびインターワーキング機能について知ることが仮定されている。この時点で、１つまたは複数の判定基準に基づいて、ＭＳ／ＳＴＡはＷｉＦｉネットワークへのハンドオーバを決定する。ＷｉＦｉネットワークに基づくＩＥＥＥ８０２．１１ｉのためのＷｉＭＡＸからＷｉＦｉへのハンドオーバ手順は手順２４０に示されているように、多数の段階（同様のステップは、ＷｉＦｉネットワークの他の型のための簡単な方法で起動されることが可能なことに留意されたい）で構成される：
段階０：最初のＷｉＭＡＸネットワークエントリー。モバイルデバイス（ＭＳ／ＳＴＡ２４１）は最初にＷｉＭＡＸアクセスネットワーク２４２に接続される。最初のＷｉＭＡＸネットワークエントリー手順は、図２Ａのコンテキストの中で、上で詳細に説明されている。初期ネットワークエントリーの間、およびＥＡＰ手順が成功した後、ＭＳＫが生成される。これをＭＳＫ１（第１セキュリティコンテキストの一部）と呼ぶ。
【００５５】
段階１：対象とするネットワークの検出およびＷｉＦｉ－ＳＦＦ（シグナリング転送機能）の発見。ＭＳ／ＳＴＡ２４１は対象とするＡＰ（アクセスポイント）を判定するためにＷｉＦｉネットワーク信号を検出し、ＤＨＣＰまたはＤＮＳ手順を通じてＷｉＦｉ－ＳＦＦ２４３のアドレスを発見する。
【００５６】
段階２：トンネル設定およびＥＡＰ認証：
１．ＭＳ／ＳＴＡ２４１がＷｉＦｉ－ＳＦＦ２４３のアドレスを発見した後、ＭＳ／ＳＴＡ２４１はＷｉＦｉ－ＳＦＦ２４３へのＩＰトンネルを確立する。
２．トンネルを介したＥＡＰ認証手順は、その開示が参照により本明細書に組み込まれ

ているＩＥＥＥ８０２．１１ｉ仕様書に従い、以下で説明される：
－　ＭＳ／ＳＴＡ２４１はオープンシステムアルゴリズムとともに認証要求フレームを対象とするＡＰに送信し、対象とするＡＰから認証応答フレームを受信する。フレームの中のＢＳＳＩＤは、判定された対象とするＡＰのＢＳＳＩＤでなければならない。ＷｉＦｉ－ＳＦＦ２４３は、認証要求フレームの中のＢＳＳＩＤに基づいて対象とするＷｉＦｉアクセスを発見し、フレームを対象とするネットワークに転送する。
－　ＭＳ／ＳＴＡ２４１は、アソシエーション要求フレームをＡＰに送信することによって対象とするＡＰに結び付き、ＡＰからアソシエーション応答フレームを受信する。
－　ＭＳ／ＳＴＡ２４１は、ＩＰトンネルを介したＥＡＰ認証を開始するために、ＥＡＰＯＬ－Ｓｔａｒｔメッセージを対象とするＷｉＦｉアクセスネットワークに送信する。ＷｉＦｉ　ＳＦＦは、このメッセージをＷｉＦｉアクセスネットワーク２４４に配置されたオーセンティケータに転送する。
－　ＭＳ／ＳＴＡ２４１およびオーセンティケータサーバ（ＡＡＡ）２４７は、ＭＳＫ２（第２セキュリティコンテキストの一部）と呼ぶＭＳＫを導出する。オーセンティケータサーバ２４７はＭＳＫ２を、対象とするＷｉＦｉネットワーク２４４の中のオーセンティケータ、およびＷＩＦ２４３のＰＭＩＰクライアントへの任意のモビリティキーに送信する。オーセンティケータは、８０２．１１ｉ仕様書によってＭＳＫ２からＰＭＫを導出する。
３．ＭＳ／ＳＴＡ２４１は、ＷｉＦｉ　ＳＦＦ２４３とともに以前に作成されたＩＰトンネルを開放する。

【００５７】
段階３：ＷｉＦｉへのハンドオーバ：
１．ＭＳ／ＳＴＡ２４１は、ＷｉＦｉアクセスネットワークへのハンドオーバを決定する。ＷｉＦｉインターフェースは電源を入れられ、ＷｉＭＡＸインターフェースはアイドルモードに入ってもよい。
２．二重モード単一無線ＭＡ／ＳＴＡ２４１は、先に導出されたＰＭＫとともにマッピングするために、ＲＳＮ（ロバストなセキュリティネットワーク）情報の中のＰＭＫＩＤとともに、対象とするＷｉＦｉ　ＡＮ２４４へ再アソシエーションメッセージを送信する。

【００５８】
段階４：ＩＰセッションの連続性。ＭＳ／ＳＴＡ２４１は、ＨＡ２４６に固定されたＩＰアドレスを要求して受信する。この場合、要求および応答メッセージは、インターワーキング機能ＷＩＦ２４５のＤＨＣＰプロキシおよびＰＭＩＰクライアント／ＭＡＧによってプロキシされる。

【００５９】
図２Ｄは、ＷｉＦｉネットワークからＷｉＭＡＸネットワークへのハンドオーバ手順２６０の１つの実施形態を示す。このシナリオでは、最初にＭＳ／ＳＴＡがＷｉＦｉネットワークに接続されることが仮定される。さらに、ＭＳはＷｉＭＡＸネットワークの利用可能性およびインターワーキング機能について知ることが仮定されている。この時点で、１つまたは複数の判定基準に基づいて、ＭＳ／ＳＴＡはＷｉＭＡＸネットワークへのハンドオーバを決定する。ＷｉＦｉからＷｉＭＡＸへのハンドオーバ手順は、手順２６０に示されているように、多数の段階で構成される：
段階０：最初のＷｉＦｉネットワークエントリー（図２Ｄに示すステップ１）。最初に、ＭＳ／ＳＴＡ２６１はＷｉＦｉネットワークに接続される。最初のＷｉＦｉネットワークエントリー手順は、図２Ｂのコンテキストの中で、上で説明されている。初期ネットワークエントリーの間、およびＥＡＰ手順が成功した後、ＭＳＫが生成される。これをＭＳＫ１（第１セキュリティコンテキストの一部）と呼ぶ。その後、ＭＳ／ＳＴＡ２６１はＷｉＭＡＸネットワークの利用可能性を検出し、インターワーキングサポートについて知る。この時点で、１つまたは複数の判定基準に基づいて、ＭＳ／ＳＴＡはＷｉＭＡＸネットワークへのハンドオーバを決定する。ＷｉＦｉからＷｉＭＡＸへの単一無線ハンドオーバ

のための手順全体は、４つの段階で構成される。

【００６０】

段階１：対象とするネットワークの検出およびＷｉＭＡＸ－ＳＦＦの発見（図２Ｄに示すステップ２）。ＭＳ／ＳＴＡ２６１はＷｉＭＡＸネットワーク信号を検出し、ＷｉＭＡＸ　ＳＦＦ２６３のアドレスを発見する。

【００６１】

段階２：トンネルの設定および事前初期ネットワークエントリー、すなわち事前登録段階（図２Ｄに示すステップ３から１５）。ＭＳ／ＳＴＡ２６１はＷｉＭＡＸ－ＳＦＦ２６３のアドレスを発見した後、ＷｉＭＡＸネットワークの中でＷｉＭＡＸ－ＳＦＦ２６３へのトンネルを確立する。次いでＭＳ／ＳＴＡ２６１は、ＭＳ／ＳＴＡ２６１とＷｉＭＡＸ－ＳＦＦ２６３の間のトンネルを介して初期ＷｉＭＡＸネットワークエントリー手順を実行する。ＥＡＰ手順が成功した後、ＭＳＫが生成され、ＡＡＡ２６７によって送信される。これをＭＳＫ２（第２セキュリティコンテキストの一部）と呼ぶ。

【００６２】

段階３：アクティブまたはアイドル／アクティブ（図２Ｄに示すステップ１６から３２）を含む無線ハンドオーバアクション。ＭＳ／ＳＴＡ２６１は、ＡＳＮ２６５に存在する対象のＢＳ２６４へのハンドオーバ手順を実行する。ＭＳ／ＳＴＡ２６１はＡＳＮ２６５の中の対象とするＢＳ２６４へのハンドオーバを決定する場合、ＷｉＭＡＸに向けられた「ＳＲハンドオーバアクション」手順を実行する。

【００６３】

段階４：ネットワーク資源の解放。ＭＳ／ＳＴＡが上記段階で、ＨＡ２６６からＩＰアドレスを得た後、前のネットワークはネットワーク資源を解放する。

【００６４】

１つまたは複数の例示的実施形態では、標準的なステップおよび呼び出しフローは、ＷｉＭＡＸフォーラムのネットワーク作業グループによって定義された３Ｇ－ＷｉＭＡＸハンドオーバ手順／呼び出しフローに類似してもよく、またそれと合わせられてもよい。

【００６５】

図３は、本発明による複数アクセス技術環境で事前登録セキュリティサポートを実施するために適した通信システムの一部分の汎用ハードウェアアーキテクチャ３００を示す。図３は２つのみのエンティティを示しているが、他のエンティティが同じ、または同様の構成を持つことができることを理解されたい。したがって上述の事前登録セキュリティサポートに関して、２つのエンティティはモバイル加入者通信デバイス（図１のＭＳ１０２、および図２Ａから２ＤのＭＳ／ＳＴＡ）およびＡＡＡサーバ（図１のＡＡＡサーバ１１２、および図２Ａから２ＤのＡＡＡ）であってよい。しかしながら、図１に示す他の構成要素は、図３のコンピューティングデバイスの中に示されるものと同じ、または同様のアーキテクチャとともに実装されてもよい。したがって、簡略化するために、本発明の方法に加わってもよいすべてのデバイスは図３の中には示されない。

【００６６】

示されているように、３０２と指定される通信デバイスおよび３０４と指定されるＡＡＡサーバは、通信システム部分３０６に関連した少なくとも２つのアクセスネットワークを介して結合される。これは、図１に示す他の構成要素のうちの１つまたは複数を含んでもよく、またネットワーク事業者によって操作されるセルラー通信ネットワークなど、公的にアクセス可能な広域通信ネットワークを含んでもよい。しかしながら、本発明は特定の型のネットワークに限定されない。通常、通信デバイスは、限定はされないが携帯電話、スマートフォン、デスクトップ電話、携帯情報端末、ラップトップコンピュータ、パーソナルコンピュータ等であることが可能である。

【００６７】

当業者には容易に明らかであるように、サーバおよび通信デバイスは、コンピュータプログラム符号の制御の下で動作するプログラムされたコンピュータとして実装されてもよい。コンピュータプログラム符号は（例えばメモリ等の）コンピュータ可読ストレージ媒

体の中に保存され、符号はコンピュータのプロセッサによって実行される。この本発明の開示を考えると、当業者であれば、本明細書で説明されるプロトコルを実装するために適切なコンピュータプログラム符号を容易に作り出すことができる。

【００６８】

それにも関わらず、図３は、通信システム３０６に関連した少なくとも２つのアクセスネットワークを介して通信する各デバイス／サーバのための例示的なアーキテクチャを大まかに示す。示されているように、通信デバイス３０２はＩ／Ｏデバイス３０８－Ａ、プロセッサ３１０－Ａおよびメモリ３１２－Ａを備える。ＡＡＡサーバ３０４はＩ／Ｏデバイス３０８－Ｂ、プロセッサ３１０－Ｂおよびメモリ３１２－Ｂを備える。「プロセッサ」という用語は本明細書で使用される際、限定されないが１つまたは複数の信号プロセッサ、１つまたは複数の集積回路等を含む、中央処理ユニット（ＣＰＵ）またはその他の処理回路を含む１つまたは複数の処理回路を含むことが意図されていることを理解されたい。また「メモリ」という用語は本明細書で使用される際、ＲＡＭ、ＲＯＭ、（例えばハードドライブ等の）固定メモリデバイスまたは（ディスケットまたはＣＤＲＯＭ等の）取り外し可能メモリデバイスなど、プロセッサまたはＣＰＵに関連したメモリを含むことが意図されている。さらに、「Ｉ／Ｏデバイス」という用語は本明細書で使用される際、データを処理ユニットに入力するための１つまたは複数の（例えばキーボード、マウス等の）入力デバイスとともに、関連した結果を処理ユニットに与えるための１つまたは複数の（例えばＣＲＴディスプレイ等の）出力デバイスも含むことが意図されている。

【００６９】

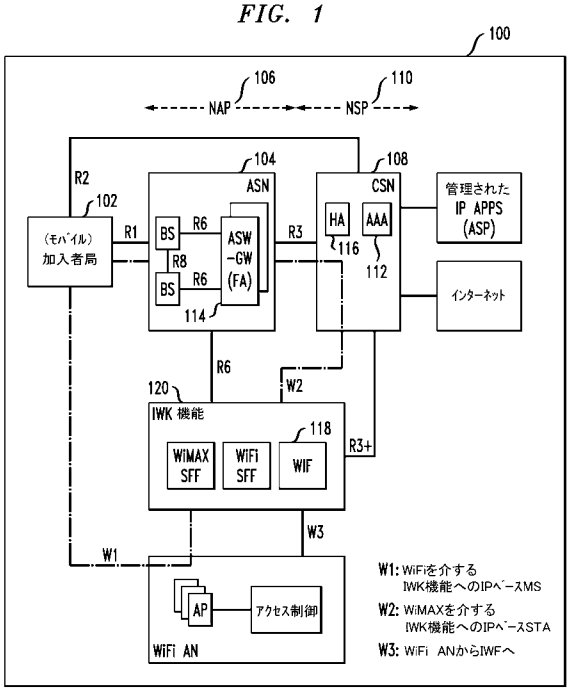
したがって、本明細書で説明される本発明の方法を実行するためのソフトウェア命令または符号は、例えばＲＯＭ、固定または取り外し可能メモリ等の関連したメモリデバイスのうちの１つまたは複数の中に保存されてもよく、利用される準備ができると、ＲＡＭにロードされ、ＣＰＵによって実行される。

【００７０】

本明細書では、添付の図面を参照して本発明の例示的実施形態が説明されてきたが、本発明はそれらの寸分違わぬ実施形態に限定されることはなく、様々な他の変更および修正が、本発明の範囲または精神から逸脱することなく当業者によって行われてもよいということを理解されたい。

【図１】

FIG. 1



【図２Ａ】

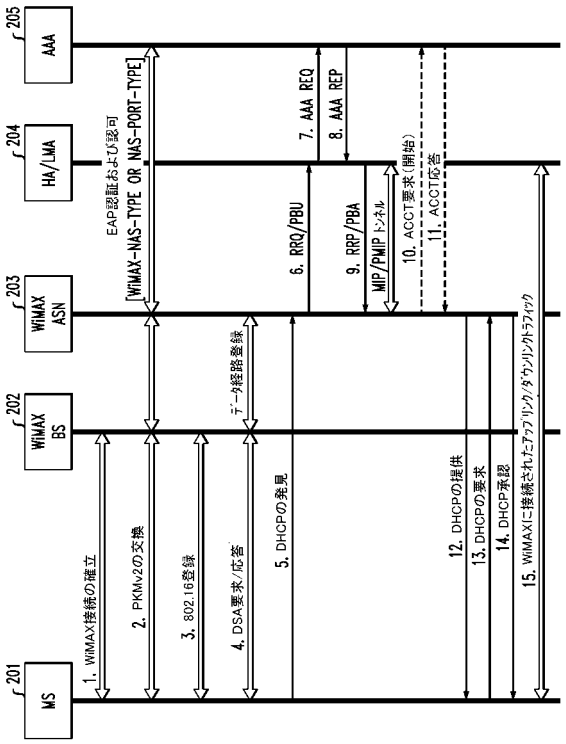


FIG. 2A
200

【図２Ｂ】

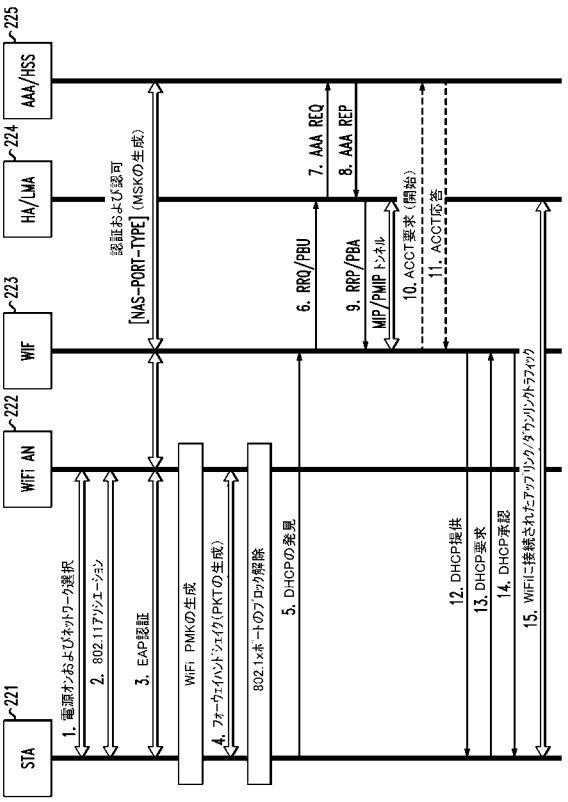


FIG. 2B
220

【図２Ｃ－１】

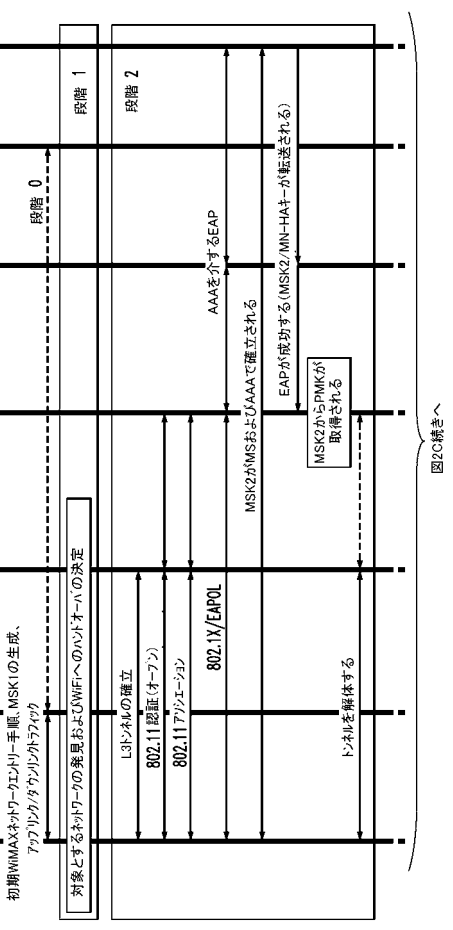


FIG. 2C
240

【図２Ｃ－２】

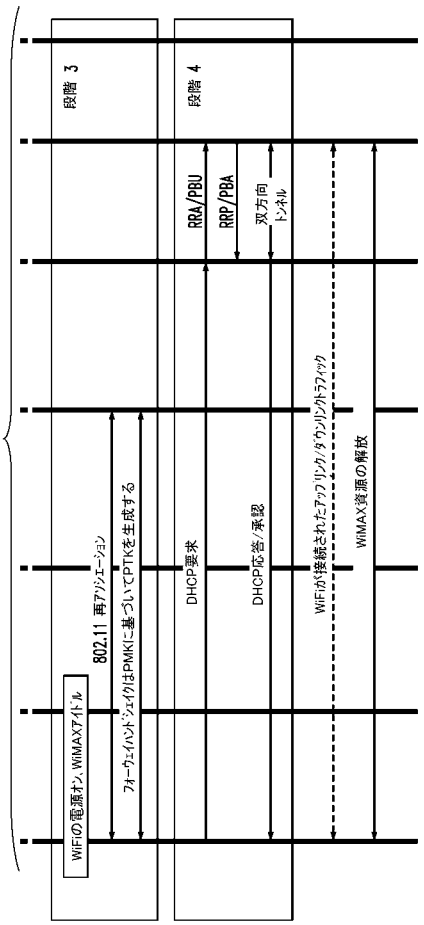


FIG. 2C 続き

【図２Ｄ－１】

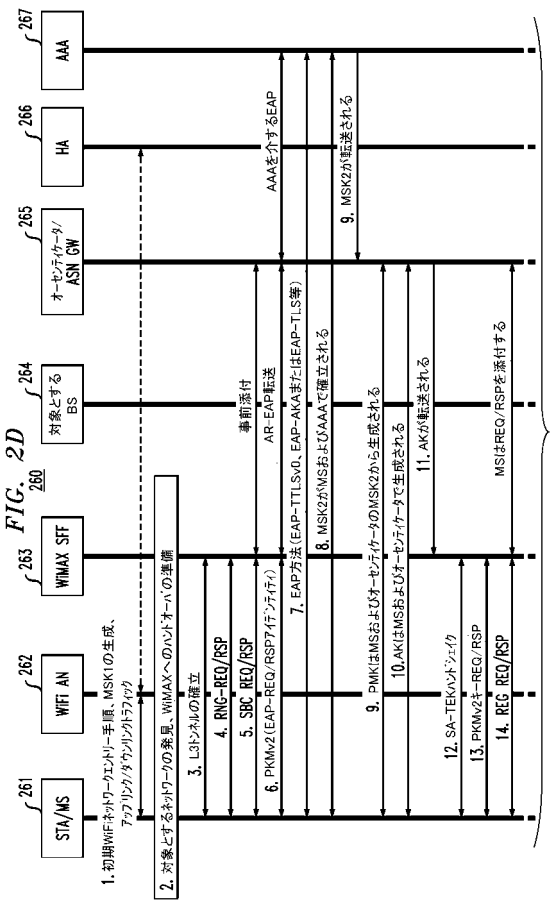


FIG. 2D

【図２Ｄ－２】

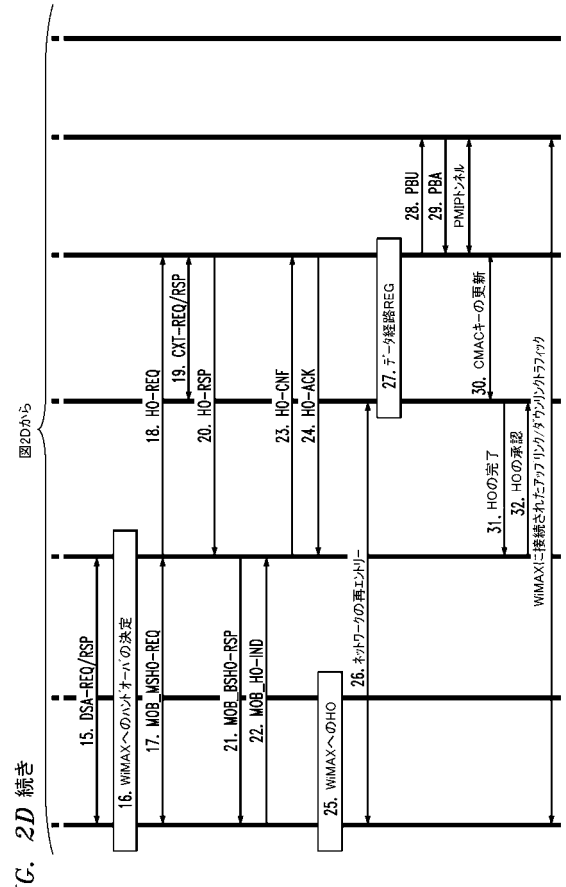


FIG. 2D 続き

【図３】

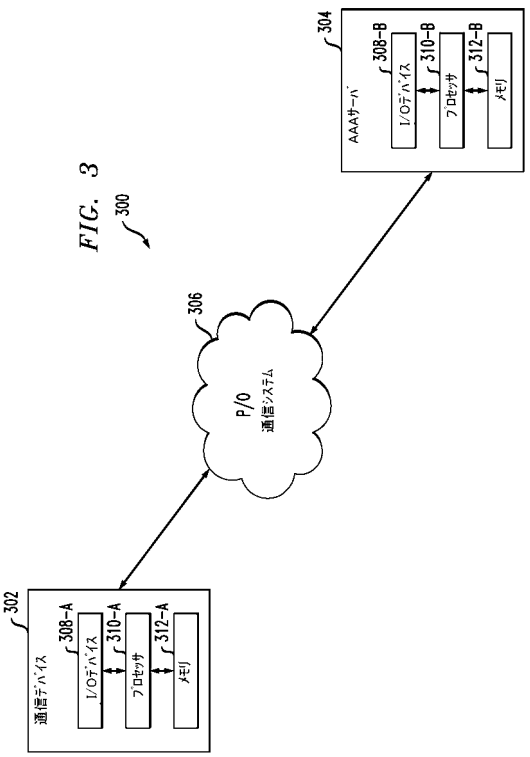


FIG. 3

フロントページの続き

審査官　米倉　明日香

(56)参考文献　国際公開第２００９／０５１４００（WO，Ａ２）
特開２００４－２６６３３１（ＪＰ，Ａ）
特開２００８－１０４００２（ＪＰ，Ａ）
国際公開第２００７／１１４６２３（WO，Ａ１）
国際公開第２００６／０２１２３６（WO，Ａ１）

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