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

特許第5144751号
(P5144751)

(45)発行日　平成25年2月13日(2013.2.13)　(24)登録日　平成24年11月30日(2012.11.30)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601B
H04L 9/32	(2006.01)	H04L	9/00	675A
H04W 12/06	(2009.01)	H04Q	7/00	183
H04W 12/04	(2009.01)	H04Q	7/00	182

請求項の数 40　(全 22 頁)

(21)出願番号	特願2010-507636 (P2010-507636)
(86)(22)出願日	平成20年5月7日 (2008.5.7)
(65)公表番号	特表2010-529710 (P2010-529710A)
(43)公表日	平成22年8月26日 (2010.8.26)
(86)国際出願番号	PCT/US2008/062966
(87)国際公開番号	WO2008/137965
(87)国際公開日	平成20年11月13日 (2008.11.13)
審査請求日	平成21年12月11日 (2009.12.11)
(31)優先権主張番号	60/916,530
(32)優先日	平成19年5月7日 (2007.5.7)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	12/113,860
(32)優先日	平成20年5月1日 (2008.5.1)
(33)優先権主張国	米国 (US)

(73)特許権者　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100109830
弁理士　福原　淑弘

最終頁に続く

(54)【発明の名称】複数の認証の効率的なサポートのための方法及び装置

(57)【特許請求の範囲】

【請求項１】

無線通信システムにおける複数のＥＡＰベースの認証のための方法であって、

第１のタイプのアクセスのために、第１のＥＡＰベースの認証において第１のマスタ・セッション鍵（ＭＳＫ）を生成することと、

前記第１のマスタ・セッション鍵（ＭＳＫ）から第１の一時セッション鍵（ＴＳＫ）を生成することと、

第２のタイプのアクセスのために、前記第１の一時セッション鍵（ＴＳＫ）を用いて第２のＥＡＰベースの認証を実行することと、

前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了した後、第１のタイプのアクセスと第２のタイプのアクセスとを提供することと、

前記第２のＥＡＰベースの認証において、第２のマスタ・セッション鍵（ＭＳＫ）を生成すること、

前記第２のマスタ・セッション鍵（ＭＳＫ）から、第３のＥＡＰベースの認証において用いられる第２の一時セッション鍵（ＴＳＫ）を生成することと

を備える方法。

【請求項２】

前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とは、単一のセッションの一部である、請求項１に記載の複数のＥＡＰベースの認証のための方法。

【請求項３】

前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了したかを示すインジケータ・メッセージを生成することを更に備える、請求項１に記載の複数のＥＡＰベースの認証のための方法。

【請求項４】

前記インジケータ・メッセージは、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了したことを示す値１と、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが完了しなかったことを示す値０とを有する、請求項３に記載の複数のＥＡＰベースの認証のための方法。

【請求項５】

前記インジケータ・メッセージは、ＶａｌｉｄＰＭＫＥｘｉｓｔｓフラグである、請求項４に記載の複数のＥＡＰベースの認証のための方法。

【請求項６】

複数のＥＡＰベースの認証が正しく完了したかを示すインジケータ・メッセージを生成することを更に備える、請求項１に記載の複数のＥＡＰベースの認証のための方法。

【請求項７】

前記第１のＥＡＰベースの認証は、第１の認証タイプを含むＥＡＰ要求／アイデンティティ・メッセージを含み、前記第２のＥＡＰベースの認証は、第２の認証タイプを含むＥＡＰ要求／アイデンティティ・メッセージを含む、請求項１に記載の複数のＥＡＰベースの認証のための方法。

【請求項８】

前記第１のタイプのアクセスはアクセス端末（ＡＴ）に関連し、前記第２のタイプのアクセスはユーザに関連する、請求項１に記載の複数のＥＡＰベースの認証のための方法。

【請求項９】

前記第１のタイプのアクセスは、ラジオ・ネットワークへのアクセスを備え、前記第２のタイプのアクセスは、インターネット・サービス・プロバイダ（ＩＳＰ）を介したアクセスを備える、請求項１に記載の複数のＥＡＰベースの認証のための方法。

【請求項１０】

前記第１のタイプのアクセスは特定のデバイスに関連し、前記第２のタイプのアクセスは特定のサーバに関連する、請求項１に記載の複数のＥＡＰベースの認証のための方法。

【請求項１１】

無線通信システムにおいて動作可能な複数のＥＡＰベースの認証のための装置であって、

第１のタイプのアクセスのために、第１のＥＡＰベースの認証において第１のマスタ・セッション鍵（ＭＳＫ）を生成する手段と、

前記第１のマスタ・セッション鍵（ＭＳＫ）から第１の一時セッション鍵（ＴＳＫ）を生成する手段と、

第２のタイプのアクセスのために、前記第１の一時セッション鍵（ＴＳＫ）を用いて、第２のＥＡＰベースの認証を実行する手段と、

前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了した後、前記第１のタイプのアクセスと前記第２のタイプのアクセスとを提供する手段と、

前記第２のＥＡＰベースの認証において第２のマスタ・セッション鍵（ＭＳＫ）を生成する手段と、

前記第２のマスタ・セッション鍵（ＭＳＫ）から、第３のＥＡＰベースの認証において用いられる第２の一時セッション鍵（ＴＳＫ）を生成する手段と

を備える装置。

【請求項１２】

前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とは、単一のセッションの一部である、請求項１１に記載の複数のＥＡＰベースの認証のための装置。

【請求項１３】

前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了したか

を示すインジケータ・メッセージを生成する手段を更に備える、請求項１１に記載の複数のＥＡＰベースの認証のための装置。
【請求項１４】
前記インジケータ・メッセージは、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了したことを示す値１と、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが完了しなかったことを示す値０とを有する、請求項１３に記載の複数のＥＡＰベースの認証のための装置。
【請求項１５】
前記インジケータ・メッセージは、ＶａｌｉｄＰＭＫＥｘｉｓｔｓフラグである、請求項１４に記載の複数のＥＡＰベースの認証のための装置。
【請求項１６】
複数のＥＡＰベースの認証が正しく完了したかを示すインジケータ・メッセージを生成する手段を更に備える、請求項１１に記載の複数のＥＡＰベースの認証のための装置。
【請求項１７】
前記第１のＥＡＰベースの認証は、第１の認証タイプを含むＥＡＰ要求／アイデンティティ・メッセージを含み、前記第２のＥＡＰベースの認証は、第２の認証タイプを含むＥＡＰ要求／アイデンティティ・メッセージを含む、請求項１１に記載の複数のＥＡＰベースの認証のための装置。
【請求項１８】
前記第１のタイプのアクセスはアクセス端末（ＡＴ）に関連し、前記第２のタイプのアクセスはユーザに関連する、請求項１１に記載の複数のＥＡＰベースの認証のための装置。
【請求項１９】
前記第１のタイプのアクセスは、ラジオ・ネットワークへのアクセスを備え、前記第２のタイプのアクセスは、インターネット・サービス・プロバイダ（ＩＳＰ）を介したアクセスを備える、請求項１１に記載の複数のＥＡＰベースの認証のための装置。
【請求項２０】
前記第１のタイプのアクセスは特定のデバイスに関連し、前記第２のタイプのアクセスは特定のサーバに関連する、請求項１１に記載の複数のＥＡＰベースの認証のための装置。
【請求項２１】
コンピュータに、第１のタイプのアクセスのために、第１のＥＡＰベースの認証において第１のマスタ・セッション鍵（ＭＳＫ）を生成させるコードと、
コンピュータに、前記第１のマスタ・セッション鍵（ＭＳＫ）から第１の一時セッション鍵（ＴＳＫ）を生成させるコードと、
コンピュータに、第２のタイプのアクセスのために、前記第１の一時セッション鍵（ＴＳＫ）を用いて第２のＥＡＰベースの認証を実行させるコードと、
コンピュータに、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了した後、第１のタイプのアクセスと第２のタイプのアクセスとを提供させるコードと、
コンピュータに、前記第２のＥＡＰベースの認証において第２のマスタ・セッション鍵（ＭＳＫ）を生成させるコードと、
コンピュータに、前記第２のマスタ・セッション鍵（ＭＳＫ）から、第３のＥＡＰベースの認証において用いられる第２の一時セッション鍵（ＴＳＫ）を生成させるコードと
を備えるコンピュータ読取可能な記録媒体。
【請求項２２】
前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とは、単一のセッションの一部である請求項２１に記載のコンピュータ読取可能な記録媒体。
【請求項２３】
コンピュータに、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが

正しく完了したかを示すインジケータ・メッセージを生成させるコードを更に備える請求項２１に記載のコンピュータ読取可能な記録媒体。

【請求項２４】

前記インジケータ・メッセージは、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了したことを示す値１と、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが完了しなかったことを示す値０とを有する請求項２３に記載のコンピュータ読取可能な記録媒体。

【請求項２５】

前記インジケータ・メッセージは、ＶａｌｉｄＰＭＫＥｘｉｓｔｓフラグである請求項２４に記載のコンピュータ読取可能な記録媒体。

【請求項２６】

コンピュータに、複数のＥＡＰベースの認証が正しく完了したかを示すインジケータ・メッセージを生成させるコードを更に備える請求項２１に記載のコンピュータ読取可能な記録媒体。

【請求項２７】

前記第１のＥＡＰベースの認証は、第１の認証タイプを含むＥＡＰ要求／アイデンティティ・メッセージを含み、前記第２のＥＡＰベースの認証は、第２の認証タイプを含むＥＡＰ要求／アイデンティティ・メッセージを含む請求項２１に記載のコンピュータ読取可能な記録媒体。

【請求項２８】

前記第１のタイプのアクセスはアクセス端末（ＡＴ）に関連し、前記第２のタイプのアクセスはユーザに関連する請求項２１に記載のコンピュータ読取可能な記録媒体。

【請求項２９】

前記第１のタイプのアクセスは、ラジオ・ネットワークへのアクセスを備え、前記第２のタイプのアクセスは、インターネット・サービス・プロバイダ（ＩＳＰ）を介したアクセスを備える請求項２１に記載のコンピュータ読取可能な記録媒体。

【請求項３０】

前記第１のタイプのアクセスは特定のデバイスに関連し、前記第２のタイプのアクセスは特定のサーバに関連する請求項２１に記載のコンピュータ読取可能な記録媒体。

【請求項３１】

無線通信システムにおいて動作可能な複数のＥＡＰベースの認証のための装置であって、

第１のタイプのアクセスのために、第１のＥＡＰベースの認証において第１のマスタ・セッション鍵（ＭＳＫ）を生成し、

前記第１のマスタ・セッション鍵（ＭＳＫ）から第１の一時セッション鍵（ＴＳＫ）を生成し、

第２のタイプのアクセスのために、前記第１の一時セッション鍵（ＴＳＫ）を用いて第２のＥＡＰベースの認証を実行し、

前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了した後、第１のタイプのアクセスと第２のタイプのアクセスとを提供し、

前記第２のＥＡＰベースの認証において第２のマスタ・セッション鍵（ＭＳＫ）を生成し、

前記第２のマスタ・セッション鍵（ＭＳＫ）から、第３のＥＡＰベースの認証において用いられる第２の一時セッション鍵（ＴＳＫ）を生成する

ように構成されたプロセッサと、

前記プロセッサに接続され、データを格納するメモリと

を備える装置。

【請求項３２】

前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とは、単一のセッションの一部である、請求項３１に記載の複数のＥＡＰベースの認証のための装置。

【請求項３３】
前記プロセッサは更に、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了したかを示すインジケータ・メッセージを生成するように構成されている、請求項３１に記載の複数のＥＡＰベースの認証のための装置。
【請求項３４】
前記インジケータ・メッセージは、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了したことを示す値１と、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが完了しなかったことを示す値０とを有する、請求項３３に記載の複数のＥＡＰベースの認証のための装置。
【請求項３５】
前記インジケータ・メッセージは、ＶａｌｉｄＰＭＫＥｘｉｓｔｓフラグである、請求項３４に記載の複数のＥＡＰベースの認証のための装置。
【請求項３６】
前記プロセッサは更に、複数のＥＡＰベースの認証が正しく完了したかを示すインジケータ・メッセージを生成するように構成された、請求項３１に記載の複数のＥＡＰベースの認証のための装置。
【請求項３７】
前記第１のＥＡＰベースの認証は、第１の認証タイプを含むＥＡＰ要求／アイデンティティ・メッセージを含み、前記第２のＥＡＰベースの認証は、第２の認証タイプを含むＥＡＰ要求／アイデンティティ・メッセージを含む、請求項３１に記載の複数のＥＡＰベースの認証のための装置。
【請求項３８】
前記第１のタイプのアクセスはアクセス端末（ＡＴ）に関連し、前記第２のタイプのアクセスはユーザに関連する、請求項３１に記載の複数のＥＡＰベースの認証のための装置。
【請求項３９】
前記第１のタイプのアクセスは、ラジオ・ネットワークへのアクセスを備え、前記第２のタイプのアクセスは、インターネット・サービス・プロバイダ（ＩＳＰ）を介したアクセスを備える、請求項３１に記載の複数のＥＡＰベースの認証のための装置。
【請求項４０】
前記第１のタイプのアクセスは特定のデバイスに関連し、前記第２のタイプのアクセスは特定のサーバに関連する、請求項３１に記載の複数のＥＡＰベースの認証のための装置。
【発明の詳細な説明】
【優先権主張】
【０００１】
本特許出願は、本願の譲受人に譲渡され、参照によって本願に明確に組みこまれた、２００７年５月７日出願の“METHOD AND APPARATUS FOR EFFICIENT SUPPORT FOR MULTIPLE AUTHENTICATIONS”と題された米国特許仮出願第６０／９１６，５３０号に対する優先権を主張する。
【技術分野】
【０００２】
本発明は、一般に無線通信に関し、特に、複数の認証に関する。
【背景技術】
【０００３】
無線通信システムは、例えば音声、データ等のような様々なタイプの通信コンテンツを提供するために広く開発されている。これらのシステムは、利用可能なシステム・リソース（例えば、帯域幅及び送信電力）を共有することによって多くのユーザとの通信をサポートすることができる多元接続システムであることができる。そのような多元接続システムの例は、符号分割多元接続（ＣＤＭＡ）システム、時分割多元接続（ＴＤＭＡ）システ

ム、周波数分割多元接続（ＦＤＭＡ）システム、３ＧＰＰ　ＬＴＥシステム、及び直交周波数分割多元接続（ＯＦＤＭＡ）システムを含む。

【０００４】

一般に、無線多元接続通信システムは、複数の無線端末のための通信を同時にサポートすることができる。各端末は、順方向リンク及び逆方向リンクでの送信を介して１つ又は複数の基地局と通信する。順方向リンク（すなわち、ダウンリンク）は、基地局から端末への通信リンクを称し、逆方向リンク（すなわち、アップリンク）は、端末から基地局への通信リンクを称する。この通信リンクは、単一入力単一出力システム、複数入力単一出力システム、又は複数入力複数出力（ＭＩＭＯ）システムを介して確立されうる。

【発明の概要】

【０００５】

本発明の局面は、無線通信システムにおける複数のＥＡＰベースの認証のための方法に存在することができる。この方法において、第１のタイプのアクセスのために、第１のＥＡＰベースの認証において第１のマスタ・セッション鍵（ＭＳＫ）が生成される。第１の一時セッション鍵（ＴＳＫ）が第１のマスタ・セッション鍵（ＭＳＫ）から生成される。第２のタイプのアクセスのために、第１の一時セッション鍵（ＴＳＫ）を用いて第２のＥＡＰベースの認証が実行される。第１のタイプのアクセス及び第２のタイプのアクセスは、第１及び第２のＥＡＰベースの認証が正しく完了した後、提供される。

【０００６】

本発明の更に詳細な局面において、この方法は更に、第２のＥＡＰベースの認証において第２のマスタ・セッション鍵（ＭＳＫ）を生成することを備えることができる。また、この方法は更に、第２のマスタ・セッション鍵（ＭＳＫ）から第２の一時セッション鍵（ＴＳＫ）を生成することを備えることもできる。第２の一時セッション鍵（ＴＳＫ）は、第３の認証において用いられうる。あるいは、この方法は更に、第２のマスタ・セッション鍵（ＭＳＫ）が第２のＥＡＰベースの認証において生成されなかった場合、第３のＥＡＰベースの認証のために第１の一時セッション鍵（ＴＳＫ）を用いることを備えることができる。第１及び第２のＥＡＰベースの認証は、単一のセッションの一部であることができる。

【０００７】

本発明の他の更に詳細な局面において、この方法は更に、第１及び第２のＥＡＰベースの認証が正しく完了したかを示すインジケータ・メッセージを生成することを備えることができる。インジケータ・メッセージは、第１及び第２のＥＡＰベースの認証が正しく完了したことを示す１の値と、第１及び第２のＥＡＰベースの認証が完了しなかったことを示す０の値とを有することができる。このインジケータ・メッセージは、ＶａｌｉｄＰＭＫＥｘｉｓｔｓフラグであることができる。

【０００８】

更に、第１のＥＡＰベースの認証は、第１の認証タイプを含むＥＡＰ要求／アイデンティティ・メッセージを含むことができ、第２のＥＡＰベースの認証は、第２の認証タイプを含むＥＡＰ要求／アイデンティティ・メッセージを含むことができる。この方法は更に、第１のＥＡＰベースの認証において第１のドメイン固有ルート鍵（ＤＳＲＫ）を生成することと、第２のＥＡＰベースの認証において第２のドメイン固有ルート鍵（ＤＳＲＫ）を生成することと、第１のＤＳＲＫ及び第２のＤＳＲＫのうちの少なくとも１つを用いて、第１のタイプのアクセス又は第２のタイプのアクセスのうちの少なくとも１つのＥＡＰベースの再認証を実行することとを備えることができる。第１のタイプのアクセスはアクセス端末（ＡＴ）に関連し、第２のタイプのアクセスはユーザに関連することができる。あるいは、第１のタイプのアクセスは特定のデバイスに関連し、第２のタイプのアクセスは特定のサーバに関連する。また、第１のタイプのアクセスは、ラジオ・ネットワークへのアクセスを備えることができ、第２のタイプのアクセスは、インターネット・サービス・プロバイダ（ＩＳＰ）を介したアクセスを備えることができる。

【０００９】

本発明の別の局面は、無線通信システムにおいて動作可能な複数のＥＡＰベースの認証のための装置に存在することができる。この装置は、第１のタイプのアクセスのために、第１のＥＡＰベースの認証において第１のマスタ・セッション鍵（ＭＳＫ）を生成する手段と、第１のマスタ・セッション鍵（ＭＳＫ）から第１の一時セッション鍵（ＴＳＫ）を生成する手段と、第２のタイプのアクセスのために、第１の一時セッション鍵（ＴＳＫ）を用いて第２のＥＡＰベースの認証を実行する手段と、第１及び第２のＥＡＰベースの認証が正しく完了した後、第１のタイプのアクセス及び第２のタイプのアクセスを提供する手段とを備える。

【００１０】

本発明のまた別の局面は、コンピュータに、第１のタイプのアクセスのために、第１のＥＡＰベースの認証において第１のマスタ・セッション鍵（ＭＳＫ）を生成させるコードと、コンピュータに、第１のマスタ・セッション鍵（ＭＳＫ）から第１の一時セッション鍵（ＴＳＫ）を生成させるコードと、コンピュータに、第２のタイプのアクセスのために、第１の一時セッション鍵（ＴＳＫ）を用いて第２のＥＡＰベースの認証を実行させるコードと、コンピュータに、第１及び第２のＥＡＰベースの認証が正しく完了した後、第１のタイプのアクセス及び第２のタイプのアクセスを提供させるコードとを備えるコンピュータ読取可能媒体を備えるコンピュータ・プログラム製品に存在することができる。

【００１１】

本発明のまた別の局面は、無線通信システムにおいて動作可能な複数のＥＡＰベースの認証のための装置に存在することができる。この装置は、第１のタイプのアクセスのために、第１のＥＡＰベースの認証において第１のマスタ・セッション鍵（ＭＳＫ）を生成し、第１のマスタ・セッション鍵（ＭＳＫ）から第１の一時セッション鍵（ＴＳＫ）を生成し、第２のタイプのアクセスのために、第１の一時セッション鍵（ＴＳＫ）を用いて第２のＥＡＰベースの認証を実行し、第１及び第２のＥＡＰベースの認証が正しく完了した後、第１のタイプのアクセス及び第２のタイプのアクセスを提供するように構成されたプロセッサと、このプロセッサに接続され、データを格納するメモリとを備える。

【図面の簡単な説明】

【００１２】

本開示の特徴、性質、及び利点は、同様の参照符号が明細書を通して対応して識別する図面に関連して説明される場合、以下に記載される詳細な説明からより明らかになるであろう。

【図１】図１は、１つの実施形態に従う多元接続無線通信システムを示す。

【図２】図２は、通信システムのブロック図である。

【図３】図３は、複数の認証の例を示す。

【図４】図４は、複数の認証及びＤＳＲＫの使用の例を示す。

【発明を実施する形態】

【００１３】

本明細書で説明される技術は、例えば符号分割多元接続（ＣＤＭＡ）ネットワーク、時分割多元接続（ＴＤＭＡ）ネットワーク、周波数分割多元接続（ＦＤＭＡ）ネットワーク、直交ＦＤＭＡ（ＯＦＤＭＡ）ネットワーク、単一キャリアＦＤＭＡ（ＳＣ－ＦＤＭＡ）ネットワーク等のような様々な無線通信ネットワークのために用いられうる。「ネットワーク」及び「システム」という用語はしばしば、置換可能に用いられる。ＣＤＭＡネットワークは、例えばユニバーサル地上無線接続（ＵＴＲＡ）、ｃｄｍａ２０００等のような無線技術を実施することができる。ＵＴＲＡは、広帯域ＣＤＭＡ（Ｗ－ＣＤＭＡ）及び低チップ・レート（ＬＣＲ）を含む。ｃｄｍａ２０００は、ＩＳ－２０００規格、ＩＳ－９５規格、ＩＳ－８５６規格をカバーする。ＴＤＭＡネットワークは、例えばグローバル・システム・フォー・モバイル・コミュニケーション（ＧＳＭ）のような無線技術を実施することができる。ＯＦＤＭＡネットワークは、例えば次世代ＵＴＲＡ（Ｅ－ＵＴＲＡ）、ＩＥＥＥ　８０２．１１、ＩＥＥＥ　８０２．１６、ＩＥＥＥ　８０２．２０、Ｆｌａｓｈ－ＯＦＤＭ等のような無線技術を実施することができる。ＵＴＲＡ、Ｅ－ＵＴＲＡ、及

びＧＳＭは、ユニバーサル・モバイル・テレコミュニケーション・システム（ＵＭＴＳ）の一部である。ロング・ターム・エボリューション（ＬＴＥ）は、近々公開される、Ｅ－ＵＴＲＡを用いたＵＭＴＳである。ＵＴＲＡ、Ｅ－ＵＴＲＡ、ＧＳＭ、ＵＭＴＳ、及びＬＴＥは、“3rd Generation Partnership Project”（３ＧＰＰ）と名づけられた組織からの文書で説明される。ｃｄｍａ２０００は、“3rd Generation Partnership Project 2”（３ＧＰＰ２）と名づけられた組織からの文書で説明される。これら様々な無線技術及び規格は、当該技術において周知である。明確化のために、本技術のある局面は、以下で、ＬＴＥに関して説明され、ＬＴＥ用語が、以下の説明の多くにおいて用いられる。

【００１４】

単一キャリア周波数分割多元接続（ＳＣ－ＦＤＭＡ）は、単一キャリア変調及び周波数領域等値化を用いる技術である。ＳＣ－ＦＤＭＡは、ＯＦＤＭＡシステムと同様の性能、及びＯＦＤＭＡシステムと本質的に同一の全体的複雑さを有する。ＳＣ－ＦＤＭＡ信号は、その固有の単一キャリア構成により、低いピーク対平均電力比（ＰＡＲＲ）を有する。ＳＣ－ＦＤＭＡは特に、低いＰＡＲＲが、送信電力効率の観点からモバイル端末に非常に大きな利益をもたらすアップリンク通信において、非常に注目されている。これは現在、３ＧＰＰロング・ターム・エボリューション（ＬＴＥ）又は次世代ＵＴＲＡにおけるアップリンク多元接続スキームのために動作することが仮定されている。

【００１５】

図１を参照すると、１つの実施形態に従う多元接続無線通信システムが示される。アクセス・ポイント１００（ＡＰ）は、１つが１０４及び１０６を含み、別の１つが１０８及び１１０を含み、また別の１つが１１２及び１１４を含む、複数のアンテナ・グループを含む。図１において、各アンテナ・グループについて２つのアンテナしか示されていないが、それよりも多い又は少ないアンテナが、各アンテナ・グループのために用いられうる。アクセス端末１１６（ＡＴ）は、アンテナ１１２及び１１４と通信しており、アンテナ１１２及び１１４は、順方向リンク１２０を介してアクセス端末１１６へ情報を送信し、逆方向リンク１１８を介してアクセス端末１１６からの情報を受信する。アクセス端末１２２は、アンテナ１０６及び１０８と通信しており、アンテナ１０６及び１０８は、順方向リンク１２６を介してアクセス端末１２２へ情報を送信し、逆方向リンク１２４を介してアクセス端末１２２からの情報を受信する。周波数分割二重通信（ＦＤＤ）システムにおいて、通信リンク１１８、１２０、１２４、及び１２６は、通信のために異なる周波数を用いることができる。例えば、順方向リンク１２０は、逆方向リンク１１８によって用いられる周波数とは異なる周波数を用いることができる。

【００１６】

アクセス・ポイントは、端末と通信するために用いられる固定の局であることができ、アクセス・ポイント、ノードＢ、又はその他いくつかの用語で称されうる。アクセス端末（ＡＴ）は、アクセス端末、ユーザ機器（ＵＥ）、無線通信デバイス、端末、アクセス端末、又はその他いくつかの用語で称されうる。

【００１７】

例えばアクセス端末のようなデバイスの認証によって、認証されたデバイス、ユーザ等のみが特定のネットワークへのアクセスを有することが確実になる。認証は、デバイス認証、サービス認証等を称することができる。１つの例において、特定のセッションのために複数の認証が必要となりうる。例えば、セクタ内のネットワーク・アクセスのためにデバイス及びサーバ両方を認証することが必要とされうる。複数の認証は、例えば、ＡＴが、ラジオ・アクセス・ネットワーク・プロバイダへのアクセス認証と、ＩＰネットワーク・プロバイダへのＩＳＰ認証とを実行する必要がある場合、必要となりうる。別の例において、デバイス認証及びユーザ認証が実行されうる。本明細書に開示された例は、アクセス端末が、必要な認証全ての実行なしでアクセスを得る可能性を軽減する。

【００１８】

１つの例において、複数、例えば２つの認証が必要である場合、第１の鍵が生成され、符号化及び復号のために用いられ、その後第２の鍵が生成され、符号化／復号するために

用いられ、その後それらの鍵は結合されうる。別の例において、連続認証が実行されうる。連続認証では、第１の鍵が第１の認証において生成され、その後、第１の認証において生成された鍵を用いて第２の認証が実行されうる。この例において、鍵を結合する必要は無く、そのため、通信システムにおけるより単純な認証の実現がもたらされうる。

【００１９】

複数の認証が互いに結合されることができ、最新の認証からの一時セッション鍵（ＴＳＫ）が後続の認証を保護する。例えば、第１の認証において生成されたＴＳＫが、第２の認証において必要とされうる。別の例において、再認証の場合、単一の認証しかないことが必要となりうる。

【００２０】

本明細書に開示された例は、複数の認証サポートを提供する。１つの例において、セキュリティのために認証を結合することが必要とされうる。ここで、アクセス・ノード又はオーセンチケータ（authenticator）は、全ての認証が正しく完了した後にのみ、ＡＴがサービスを取得することを許可しなければならない。別の例において、複数の認証が繰り返される必要が無い、効率的な再認証が提供される。

【００２１】

図３は、１つずつ実行する複数の認証の例を示す。図示したように、最初のＥＡＰ交換は、ＥＡＰ要求／アイデンティティ（認証タイプ）のために暗号化されずに行われる。次に、セッションが安全にされる。図３において、第１の認証は、鍵を生成しなければならない。すなわち、ここでは「ＭＳＫ１」と示されたマスタ・セッション鍵（ＭＳＫ）を生成することが必要である。次に、鍵交換プロトコル（ＫＥＰ）が、例えば、図示されたようにＭＳＫ１であるＭＳＫからのＴＳＫ１のような、一時セッション鍵（ＴＳＫ）を生成する。第１の認証後に導出されたＴＳＫは、第２のＥＡＰ認証を保護する。２つ以上の認証が鍵を生成する場合、最新のＭＳＫが現在のＭＳＫとなる。１つの例において、第２の認証は、第２のＭＳＫを生成することも生成しないこともできる。第２のＭＳＫが第２の認証において生成された場合、ＫＥＰは、第２のＴＳＫ、例えばＴＳＫ２を生成するために第２のＭＳＫを用いる。第２のＴＳＫはその後、後続メッセージ（生成されたデータ）の保護のために用いられうる。第２のＭＳＫが第２の認証において生成されなかった場合、前に生成されたＴＳＫ、例えばＴＳＫ１がそのまま用いられうる。

【００２２】

また図３の例を参照すると、サービス提供ラジオ・ネットワーク・コントローラ（Ｓ－ＲＮＣ）は、ＫＥＰに現在のＭＳＫを用いさせる。Ｓ－ＲＮＣは、ＶａｌｉｄＰＭＫＥｘｉｓｔｓフラグを用いて、両方の認証が完了しているか否かを他のアクティブ・セット・メンバに示す。新たなアクティブ・セット・メンバは、ＥＲＰ（ＥＡＰ再認証プロトコル）及び／又はＫＥＰ（エア・インタフェース鍵交換プロトコル）の実行前にＶａｌｉｄＰＭＫＥｘｉｓｔｓフラグが示されるセッション更新を待つ。ＶａｌｉｄＰＭＫＥｘｉｓｔｓフラグは、１と０との間でトグルすることができる。ここで、１は、両方のセッションが完了したことを示し、０は、それらがまだ完了していないことを示す。セッションは、複数の認証を備えることができる。例えば、第３の認証が必要となりうる。ここで、第３のＭＳＫが生成され、第３のＴＳＫを導出するためにＫＥＰによって用いられうる。第３のＭＳＫが第３の認証において生成されなかった場合、前のＴＳＫ、例えばＴＳＫ２、ＴＳＫ$_{previous}$等が用いられうる。

【００２３】

新たなアクティブ・セット・メンバは、ＥＲＰを実行することができるが、その後、ＶａｌｉｄＰＭＫＥｘｉｓｔｓフラグが示されるまでＫＥＰの実行を待つことがある。一例において、ＥＡＰ方法のうちの１つしか鍵を生成しない場合、第１のＥＡＰ方法によって確立されたＤＳＲＫを用いて全てを行うために、ＥＲＰ交換は、別のｅＢＳのために可能とされうる。しかし、ＡＴが必要な認証全てを完了するまで、ＡＴは、ネットワークにアクセスすることができないだろう。従って、それまでＫＥＰ交換は遅延されうる。別の例において、複数のＥＡＰ方法が鍵を生成する場合、ＥＲＰもまた、最も新しく生成された

ＤＳＲＫを用いて実行する。

【００２４】

図４は、複数の認証及びドメイン固有ルート鍵（ＤＳＲＫ）使用の例を示す。ＤＳＲＫは、再認証のために用いられうる。図示したように、最新のＥＡＰ交換からのＤＳＲＫが、再認証のために用いられうる。ＡＡＡ－Ｌは、複数のＤＳＲＫを相関付けることができず、両方を格納する。ＡＴは、正しいＤＳＲＫを用いることが期待される。

【００２５】

別の局面において、誤作動しているＡＴが、Ｓ－ＲＮＣを用いて第１の認証を完了することがある。これはまた、ＡＮをアクティブ・セットに追加しうる。ここで、誤動作しているＡＴは、Ｓ－ＲＮＣからのＭＳＫ１’を用いてセッションを取得する、又は、ＤＳＲＫ１を用いてＥＲＰを行うことがある。ＡＡＡ－Ｌは、ＡＴが複数の認証を完了したかを知らない。

【００２６】

緩和は、エア・インタフェース・レベルにおいて、又はバックエンド・ネットワーク・サーバを介することができる。エア・インタフェース・レベルにおいて、Ｓ－ＲＮＣは、ＡＴが、期待された数の認証を完了することを期待する。Ｓ－ＲＮＣは、新たなＡＮにセッションを与えることができるが、このセッションには、ＰＭＫが未だ確立されていないことを示すであろうＶａｌｉｄＰＭＫＥｘｉｓｔｓフラグが存在する。ＥＡＰの完了前、セッション取得はセキュリティ・クッキーを含むことができないので、Ｓ－ＲＮＣは、任意のＡＮにセッションを与えることができる。ここで、Ｓ－ＲＮＣは、セッションが（１つ又は複数の）ＥＡＰの完了後に更新されたことを確かめるであろう。新たなＡＮは、（オプションである）ＥＲＰ及びＫＥＰを実行する前にトグルされたこのフラグ値を用いる別のセッション更新を待つであろう。更に、新たなＡＮは、ＴＳＫが確立する前、データ転送を許可しないであろう。

【００２７】

バックエンド・ネットワーク・サーバを介して、Ｓ－ＲＮＣは、ＡＴが期待された数の認証を完了することを期待する。ＡＴが期待された数より少ない数の認証を完了した場合、Ｓ－ＲＮＣは、セッションを閉じるか、又は、ＤＳＲＫを保持しているＡＡＡ－Ｌへ通知を送信する。ここで、ＡＡＡ－Ｌは、ＤＳＲＫからｒＭＳＫを導出したであろう任意のＡＮへ通知を送信する。ＡＮはその後、ＡＴとの無許可のセッションを閉じる。

【００２８】

再び図１を参照すると、アンテナの各グループ及び／又はそれらが通信するように設計されたエリアは、しばしば、アクセス・ポイントのセクタと称される。実施形態において、アンテナ・グループの各々は、アクセス・ポイント１００によってカバーされるエリアのセクタ内のアクセス端末へ通信するように設計される。

【００２９】

図２は、ＭＩＭＯシステム２００における、（アクセス・ポイントとしても知られる）送信機システム２１０及び（アクセス端末としても知られる）受信機システム２５０の実施形態のブロック図である。送信機システム２１０において、多数のデータ・ストリームのためのトラヒック・データが、データ・ソース２１２から、送信（ＴＸ）データ・プロセッサ２１４へ提供される。

【００３０】

実施形態において、各データ・ストリームは、それぞれの送信アンテナを介して送信される。ＴＸデータ・プロセッサ２１４は、各データ・ストリームのために選択された特定の符号化スキームに基づいて、そのデータ・ストリームのためのトラヒック・データをインタリーブし、符号化データを提供する。

【００３１】

各データ・ストリームのための符号化データは、ＯＦＤＭ技術を用いてパイロット・データと多重化されうる。パイロット・データは一般に、周知の方式で処理される周知のデータ・パターンであり、チャネル応答を推定するために受信機システムにおいて用いられ

うる。各データ・ストリームのための多重化されたパイロットと符号化データとは、その後、変調記号を提供するために、そのデータ・ストリームのために選択された特定の変調スキーム（例えば、ＢＰＳＫ、ＱＳＰＫ、Ｍ－ＰＳＫ、又はＭ－ＱＡＭ）に基づいて変調（すなわち、記号マップ）される。各データ・ストリームのためのデータ・レート、符号化、及び変調は、プロセッサ２３０によって実行される命令によって決定されうる。

【００３２】

全てのデータ・ストリームのための変調記号が、その後、ＴＸ　ＭＩＭＯプロセッサ２２０へ提供される。ＴＸ　ＭＩＭＯプロセッサ２２０は、（例えばＯＦＤＭのための）変調記号を更に処理することができる。ＴＸ　ＭＩＭＯプロセッサ２２０はその後、N_T個の変調記号ストリームをN_T個の送信機（ＴＭＴＲ）２２２ａ乃至２２２ｔに提供する。ある実施形態において、ＭＩＭＯプロセッサ２２０は、データ・ストリームの記号及び記号が送信されるアンテナにビームフォーミング重み付けを適用する。

【００３３】

各送信機２２２は、１つ又は複数のアナログ信号を提供するために、それぞれの記号ストリームを受信及び処理し、ＭＩＭＯチャネルを介した送信のために適切な変調信号を提供するためにアナログ信号を更に調整（例えば、増幅、フィルタ、及びアップコンバート）する。送信機２２２ａ乃至２２２ｔからのN_T個の変調信号がその後、N_T個のアンテナ２２４ａ乃至２２４ｔからそれぞれ送信される。

【００３４】

受信機システム２５０において、送信された変調信号が、N_R個のアンテナ２５２ａ乃至２５２ｒによって受信され、各アンテナ２５２からの受信信号は、それぞれの受信機（ＲＣＶＲ）２５４ａ乃至２５４ｒに提供される。各受信機２５４は、それぞれの受信信号を調整（例えば、フィルタ、増幅、及びダウンコンバート）し、調整した信号をデジタル化してサンプルを提供し、対応する「受信」記号ストリームを提供するためにサンプルを更に処理する。

【００３５】

ＲＸデータ・プロセッサ２６０はその後、特定の受信機処理技術に基づいてN_R個の受信機２５４からのN_R個の受信記号ストリームを受信及び処理し、N_T個の「検出済」記号ストリームを提供する。ＲＸデータ・プロセッサ２６０はその後、各検出された記号ストリームを復調、デインタリーブ、及び復号し、データ・ストリームのためのトラヒック・データを復元する。ＲＸデータ・プロセッサ２６０による処理は、送信機システム２１０のＴＸ　ＭＩＭＯプロセッサ２２０及びＴＸデータ・プロセッサ２１４によって実行される処理と相補的である。

【００３６】

プロセッサ２７０は、どの前符号化マトリクスを用いるかを定期的に決定する（以下で説明）。プロセッサ２７０は、マトリクス・インデクス部分及びランク値部分を備える逆方向リンク・メッセージを定式化する。

【００３７】

逆方向リンク・メッセージは、通信リンク及び／又は受信データ・ストリームに関する様々なタイプの情報を備えることができる。逆方向リンク・メッセージはその後、データ・ソース２３６からの複数のデータ・ストリームのためのトラヒック・データを受け取るＴＸデータ・プロセッサ２３８によって処理され、変調器２８０によって変調され、送信機２５４ａ乃至２５４ｒによって調整され、送信機システム２１０へ送信される。

【００３８】

送信機システム２１０において、受信機システム２５０からの変調信号は、アンテナ２２４によって受信され、受信機２２２によって調整され、復調器２４０によって復調され、ＲＸデータ・プロセッサ２４２によって処理され、受信機システム２５０によって送信された逆方向リンク・メッセージが抽出される。プロセッサ２３０はその後、ビームフォーミング重み付けを決定するためにどの前符号化マトリクスを用いるかを決定し、その後、抽出されたメッセージを処理する。

【００３９】
開示された処理におけるステップの特定の順序又は序列は、典型的なアプローチの一例であることが理解される。設計優先に基づいて、処理におけるステップの特定の順序又は序列は、本開示の範囲内にあるままで並べ替えられうることが理解される。添付の方法請求項は、様々なステップの要素をサンプルの順序で示し、示された特定の順序又は序列に限定することは意味されない。
【００４０】
当業者は、情報及び信号が、様々な異なる技術及び技法のうちの任意の１つを用いて表されうることを理解するであろう。例えば、上記記載を通して参照されうるデータ、命令、コマンド、情報、信号、ビット、記号、及びチップは、電圧、電流、電磁波、磁界あるいは磁気粒子、光場あるいは光学粒子、又はそれら任意の組合せによって表されうる。
【００４１】
当業者は更に、本明細書に開示された実施形態に関連して記載された様々な論理的ブロック、モジュール、回路、及びアルゴリズム・ステップが、電子的ハードウェア、コンピュータ・ソフトウェア、又はそれら両方の組合せとして実現されうることを理解するであろう。このハードウェアとソフトウェアとの相互置換性を明確に示すために、様々な例示的構成要素、ブロック、モジュール、回路、及びステップが、それらの機能の観点から一般的に説明された。そのような機能がハードウェアとして実現されるかソフトウェアとして実現されるかは、特定のアプリケーション及びシステム全体に課された設計制約による。当業者は、特定のアプリケーションのために様々な方法で上述された機能を実現することができるが、このような実現の決定は、本開示の範囲から逸脱させるものとして解釈されてはならない。
【００４２】
本明細書に開示された実施形態に関連して記載された様々な例示的ブロック、モジュール、及び回路は、汎用プロセッサ、デジタル信号プロセッサ（ＤＳＰ）、特定用途向け集積回路（ＡＳＩＣ）、フィールド・プログラマブル・ゲート・アレイ（ＦＰＧＡ）あるいはその他のプログラマブル論理デバイス、ディスクリート・ゲートあるいはトランジスタ・ロジック、ディスクリート・ハードウェア部品、又は上述した機能を実行するために設計されたそれらの任意の組合せを用いて実現又は実行されうる。汎用プロセッサとしてマイクロプロセッサを用いることが可能であるが、その代わりに、プロセッサは、任意の従来技術によるプロセッサ、コントローラ、マイクロコントローラ、又は状態機器であることもできる。プロセッサは、例えばＤＳＰとマイクロプロセッサとの組合せ、複数のマイクロプロセッサ、ＤＳＰコアに接続された１つ又は複数のマイクロプロセッサ、又はそのような任意の構成である計算デバイスの組合せとして実現されることもできる。
【００４３】
１つ又は複数の典型的な実施形態において、上述された機能は、ハードウェア、ソフトウェア、ファームウェア、又はそれらの任意の組合せによって実現されうる。ソフトウェアによる実現の場合、機能は、コンピュータ読取可能媒体上のコード又は１つ又は複数の命令として送信されるか、あるいは格納されうる。コンピュータ読取可能媒体は、コンピュータ・プログラムを１つの場所から別の場所へ転送することを容易にする任意の媒体を含む通信媒体及びコンピュータ記憶媒体の両方を含む。記憶媒体は、コンピュータによってアクセスすることができる任意の利用可能な媒体であることができる。限定ではなく一例として、そのようなコンピュータ読取可能媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、ＣＤ－ＲＯＭ、又はその他の光学ディスク記憶媒体、磁気ディスク記憶媒体あるいはその他の磁気記憶デバイス、又は、所望のプログラム・コードを命令又はデータ構成の形式で搬送又は格納するために用いられることができ、コンピュータによってアクセスすることができるその他任意の媒体を備えることができる。例えば、ソフトウェアが、ウェブサイト、サーバ、あるいはその他の遠隔ソースから、同軸ケーブル、光ファイバーケーブル、ツイスト・ペア、デジタル加入者線（ＤＳＬ）、又は例えば赤外線、ラジオ、及びマイクロウェーブのような無線技術を用いて送信された場合、同軸ケーブル、光ファイバーケーブ

ル、ツイスト・ペア、デジタル加入者線（ＤＳＬ）、又は例えば赤外線、ラジオ、及びマイクロウェーブのような無線技術は、媒体の定義に含まれる。本明細書で用いられるように、ディスク（disk）及びディスク（disc）は、コンパクト・ディスク（disc）（ＣＤ）、レーザ・ディスク（disc）、光学ディスク（disc）、デジタル・バーサタイル・ディスク（disc）（ＤＶＤ）、フロッピー（登録商標）・ディスク（disk）、及びブルーレイ・ディスク（disc）を含む。ここで、ディスク（disk）は通常、データを磁気的に再生するが、ディスク（disc）は、レーザを用いてデータを光学的に再生する。上記の組合せもまた、コンピュータ読取可能媒体の範囲内に含まれなければならない。

【００４４】

本明細書に開示された実施形態に関連して記載された方法又はアルゴリズムのステップは、ハードウェアによって直接、プロセッサによって実行されるソフトウェア・モジュールによって、又はそれら２つの組合せによって具現化されうる。ソフトウェア・モジュールは、ＲＡＭメモリ、フラッシュ・メモリ、ＲＯＭメモリ、ＥＰＲＯＭメモリ、ＥＥＰＲＯＭメモリ、レジスタ、ハード・ディスク、リムーバブル・ディスク、ＣＤ－ＲＯＭ、又は当該技術において知られるその他任意の形式の記憶媒体に収納されうる。典型的な記憶媒体は、プロセッサがそこから情報を読み取り、またプロセッサがそこへ情報を書き込むことができるように、プロセッサに結合される。あるいは、記憶媒体はプロセッサに統合されうる。プロセッサと記憶媒体とは、ＡＳＩＣ内に存在することができる。ＡＳＩＣは、ユーザ端末内に存在することができる。あるいはプロセッサと記憶媒体とは、ユーザ端末内のディスクリート部品として存在することもできる。

【００４５】

開示された実施形態における上記記載は、当業者をして、本開示の製造又は利用を可能とするために提供される。これらの実施形態への様々な変形例もまた、当業者には明らかであって、本明細書で定義された一般原理は、本開示の精神又は範囲から逸脱することなく他の実施形態にも適用されうる。従って、本開示は、本明細書に示した実施形態に限定することは意図されておらず、本明細書に開示された原理及び新規特徴と整合が取れた最も広い範囲と一致するように意図されている。

以下に本願発明の当初の特許請求の範囲に記載された発明を付記する。

［Ｃ１］

無線通信システムにおける複数のＥＡＰベースの認証のための方法であって、

第１のタイプのアクセスのために、第１のＥＡＰベースの認証において第１のマスタ・セッション鍵（ＭＳＫ）を生成することと、

前記第１のマスタ・セッション鍵（ＭＳＫ）から第１の一時セッション鍵（ＴＳＫ）を生成することと、

第２のタイプのアクセスのために、前記第１の一時セッション鍵（ＴＳＫ）を用いて第２のＥＡＰベースの認証を実行することと、

前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了した後、第１のタイプのアクセスと第２のタイプのアクセスとを提供することと

を備える方法。

［Ｃ２］

前記第２のＥＡＰベースの認証において、第２のマスタ・セッション鍵（ＭＳＫ）を生成することを更に備える、Ｃ１に記載の複数のＥＡＰベースの認証のための方法。

［Ｃ３］

前記第２のマスタ・セッション鍵（ＭＳＫ）から第２の一時セッション鍵（ＴＳＫ）を生成することを更に備える、Ｃ２に記載の複数のＥＡＰベースの認証のための方法。

［Ｃ４］

前記第２の一時セッション鍵（ＴＳＫ）は、第３のＥＡＰベースの認証において用いられる、Ｃ３に記載の複数のＥＡＰベースの認証のための方法。

［Ｃ５］

第２のマスタ・セッション鍵（ＭＳＫ）が前記第２のＥＡＰベースの認証において生成

されなかった場合、第３のＥＡＰベースの認証のために、前記第１の一時セッション鍵（ＴＳＫ）を用いることを更に備える、Ｃ１に記載の複数のＥＡＰベースの認証のための方法。

［Ｃ６］

前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とは、単一のセッションの一部である、Ｃ１に記載の複数のＥＡＰベースの認証のための方法。

［Ｃ７］

前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了したかを示すインジケータ・メッセージを生成することを更に備える、Ｃ１に記載の複数のＥＡＰベースの認証のための方法。

［Ｃ８］

前記インジケータ・メッセージは、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了したことを示す値１と、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが完了しなかったことを示す値０とを有する、Ｃ７に記載の複数のＥＡＰベースの認証のための方法。

［Ｃ９］

前記インジケータ・メッセージは、ＶａｌｉｄＰＭＫＥｘｉｓｔｓフラグである、Ｃ８に記載の複数のＥＡＰベースの認証のための方法。

［Ｃ１０］

複数のＥＡＰベースの認証が正しく完了したかを示すインジケータ・メッセージを生成することを更に備える、Ｃ１に記載の複数のＥＡＰベースの認証のための方法。

［Ｃ１１］

前記第１のＥＡＰベースの認証は、第１の認証タイプを含むＥＡＰ要求／アイデンティティ・メッセージを含み、前記第２のＥＡＰベースの認証は、第２の認証タイプを含むＥＡＰ要求／アイデンティティ・メッセージを含む、Ｃ１に記載の複数のＥＡＰベースの認証のための方法。

［Ｃ１２］

前記第１のＥＡＰベースの認証において第１のドメイン固有ルート鍵（ＤＳＲＫ）を生成することと、

前記第２のＥＡＰベースの認証において第２のドメイン固有ルート鍵（ＤＳＲＫ）を生成することと、

前記第１のＤＳＲＫと前記第２のＤＳＲＫとのうちの少なくとも１つを用いて、前記第１のタイプのアクセスか前記第２のタイプのアクセスかのうちの少なくとも１つのＥＡＰベースの再認証を実行することと

を更に備える、Ｃ１に記載の複数のＥＡＰベースの認証のための方法。

［Ｃ１３］

前記第１のタイプのアクセスはアクセス端末（ＡＴ）に関連し、前記第２のタイプのアクセスはユーザに関連する、Ｃ１に記載の複数のＥＡＰベースの認証のための方法。

［Ｃ１４］

前記第１のタイプのアクセスは、ラジオ・ネットワークへのアクセスを備え、前記第２のタイプのアクセスは、インターネット・サービス・プロバイダ（ＩＳＰ）を介したアクセスを備える、Ｃ１に記載の複数のＥＡＰベースの認証のための方法。

［Ｃ１５］

前記第１のタイプのアクセスは特定のデバイスに関連し、前記第２のタイプのアクセスは特定のサーバに関連する、Ｃ１に記載の複数のＥＡＰベースの認証のための方法。

［Ｃ１６］

無線通信システムにおいて動作可能な複数のＥＡＰベースの認証のための装置であって、

第１のタイプのアクセスのために、第１のＥＡＰベースの認証において第１のマスタ・セッション鍵（ＭＳＫ）を生成する手段と、

前記第１のマスタ・セッション鍵（ＭＳＫ）から第１の一時セッション鍵（ＴＳＫ）を生成する手段と、
第２のタイプのアクセスのために、前記第１の一時セッション鍵（ＴＳＫ）を用いて、第２のＥＡＰベースの認証を実行する手段と、
前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了した後、前記第１のタイプのアクセスと前記第２のタイプのアクセスとを提供する手段と
を備える装置。
［Ｃ１７］
前記第２のＥＡＰベースの認証において第２のマスタ・セッション鍵（ＭＳＫ）を生成する手段を更に備える、Ｃ１６に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ１８］
前記第２のマスタ・セッション鍵（ＭＳＫ）から第２の一時セッション鍵（ＴＳＫ）を生成する手段を更に備える、Ｃ１７に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ１９］
前記第２の一時セッション鍵（ＴＳＫ）は、第３のＥＡＰベースの認証において用いられる、Ｃ１８に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ２０］
第２のマスタ・セッション鍵が前記第２のＥＡＰベースの認証において生成されなかった場合、第３のＥＡＰベースの認証のために前記第１の一時セッション鍵（ＴＳＫ）を用いる手段を更に備える、Ｃ１６に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ２１］
前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とは、単一のセッションの一部である、Ｃ１６に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ２２］
前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了したかを示すインジケータ・メッセージを生成する手段を更に備える、Ｃ１６に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ２３］
前記インジケータ・メッセージは、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了したことを示す値１と、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが完了しなかったことを示す値０とを有する、Ｃ２２に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ２４］
前記インジケータ・メッセージは、ＶａｌｉｄＰＭＫＥｘｉｓｔｓフラグである、Ｃ２３に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ２５］
複数のＥＡＰベースの認証が正しく完了したかを示すインジケータ・メッセージを生成する手段を更に備える、Ｃ１６に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ２６］
前記第１のＥＡＰベースの認証は、第１の認証タイプを含むＥＡＰ要求／アイデンティティ・メッセージを含み、前記第２のＥＡＰベースの認証は、第２の認証タイプを含むＥＡＰ要求／アイデンティティ・メッセージを含む、Ｃ１６に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ２７］
前記第１のＥＡＰベースの認証において第１のドメイン固有ルート鍵（ＤＳＲＫ）を生成する手段と、
前記第２のＥＡＰベースの認証において第２のドメイン固有ルート鍵（ＤＳＲＫ）を生成する手段と、
前記第１のＤＳＲＫと前記第２のＤＳＲＫとのうちの少なくとも１つを用いて、前記第１のタイプのアクセスか前記第２のタイプのアクセスかのうちの少なくとも１つのＥＡＰ

ベースの再認証を実行する手段と
を更に備える、Ｃ１６に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ２８］
前記第１のタイプのアクセスはアクセス端末（ＡＴ）に関連し、前記第２のタイプのアクセスはユーザに関連する、Ｃ１６に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ２９］
前記第１のタイプのアクセスは、ラジオ・ネットワークへのアクセスを備え、前記第２のタイプのアクセスは、インターネット・サービス・プロバイダ（ＩＳＰ）を介したアクセスを備える、Ｃ１６に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ３０］
前記第１のタイプのアクセスは特定のデバイスに関連し、前記第２のタイプのアクセスは特定のサーバに関連する、Ｃ１６に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ３１］
コンピュータに、第１のタイプのアクセスのために、第１のＥＡＰベースの認証において第１のマスタ・セッション鍵（ＭＳＫ）を生成させるコードと、
コンピュータに、前記第１のマスタ・セッション鍵（ＭＳＫ）から第１の一時セッション鍵（ＴＳＫ）を生成させるコードと、
コンピュータに、第２のタイプのアクセスのために、前記第１の一時セッション鍵（ＴＳＫ）を用いて第２のＥＡＰベースの認証を実行させるコードと、
コンピュータに、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了した後、第１のタイプのアクセスと第２のタイプのアクセスとを提供させるコードと
を備えるコンピュータ読取可能媒体を備えるコンピュータ・プログラム製品。
［Ｃ３２］
コンピュータに、前記第２のＥＡＰベースの認証において第２のマスタ・セッション鍵（ＭＳＫ）を生成させるコードを更に備えるＣ３１に記載のコンピュータ・プログラム製品。
［Ｃ３３］
コンピュータに、前記第２のマスタ・セッション鍵（ＭＳＫ）から第２の一時セッション鍵（ＴＳＫ）を生成させるコードを更に備えるＣ３２に記載のコンピュータ・プログラム製品。
［Ｃ３４］
前記第２の一時セッション鍵（ＴＳＫ）は、第３のＥＡＰベースの認証において用いられるＣ３３に記載のコンピュータ・プログラム製品。
［Ｃ３５］
第２のマスタ・セッション鍵（ＭＳＫ）が前記第２のＥＡＰベースの認証において生成されなかった場合、コンピュータに、第３のＥＡＰベースの認証のために前記第１の一時セッション鍵（ＴＳＫ）を用いさせるコードを更に備えるＣ３１に記載のコンピュータ・プログラム製品。
［Ｃ３６］
前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とは、単一のセッションの一部であるＣ３１に記載のコンピュータ・プログラム製品。
［Ｃ３７］
コンピュータに、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了したかを示すインジケータ・メッセージを生成させるコードを更に備えるＣ３１に記載のコンピュータ・プログラム製品。
［Ｃ３８］
前記インジケータ・メッセージは、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了したことを示す値１と、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが完了しなかったことを示す値０とを有するＣ３７に記載

のコンピュータ・プログラム製品。
［Ｃ３９］
前記インジケータ・メッセージは、ＶａｌｉｄＰＭＫＥｘｉｓｔｓフラグであるＣ３８に記載のコンピュータ・プログラム製品。
［Ｃ４０］
コンピュータに、複数のＥＡＰベースの認証が正しく完了したかを示すインジケータ・メッセージを生成させるコードを更に備えるＣ３１に記載のコンピュータ・プログラム製品。
［Ｃ４１］
前記第１のＥＡＰベースの認証は、第１の認証タイプを含むＥＡＰ要求／アイデンティティ・メッセージを含み、前記第２のＥＡＰベースの認証は、第２の認証タイプを含むＥＡＰ要求／アイデンティティ・メッセージを含むＣ３１に記載のコンピュータ・プログラム製品。
［Ｃ４２］
コンピュータに、前記第１のＥＡＰベースの認証において第１のドメイン固有ルート鍵（ＤＳＲＫ）を生成させるコードと、
コンピュータに、前記第２のＥＡＰベースの認証において第２のドメイン固有ルート鍵（ＤＳＲＫ）を生成させるコードと、
コンピュータに、前記第１のＤＳＲＫと前記第２のＤＳＲＫとのうちの少なくとも１つを用いて、前記第１のタイプのアクセスか前記第２のタイプのアクセスかのうちの少なくとも１つのＥＡＰベースの再認証を実行させるコードと
を更に備えるＣ３１に記載のコンピュータ・プログラム製品。
［Ｃ４３］
前記第１のタイプのアクセスはアクセス端末（ＡＴ）に関連し、前記第２のタイプのアクセスはユーザに関連するＣ３１に記載のコンピュータ・プログラム製品。
［Ｃ４４］
前記第１のタイプのアクセスは、ラジオ・ネットワークへのアクセスを備え、前記第２のタイプのアクセスは、インターネット・サービス・プロバイダ（ＩＳＰ）を介したアクセスを備えるＣ３１に記載のコンピュータ・プログラム製品。
［Ｃ４５］
前記第１のタイプのアクセスは特定のデバイスに関連し、前記第２のタイプのアクセスは特定のサーバに関連するＣ３１に記載のコンピュータ・プログラム製品。
［Ｃ４６］
無線通信システムにおいて動作可能な複数のＥＡＰベースの認証のための装置であって、
第１のタイプのアクセスのために、第１のＥＡＰベースの認証において第１のマスタ・セッション鍵（ＭＳＫ）を生成し、
前記第１のマスタ・セッション鍵（ＭＳＫ）から第１の一時セッション鍵（ＴＳＫ）を生成し、
第２のタイプのアクセスのために、前記第１の一時セッション鍵（ＴＳＫ）を用いて第２のＥＡＰベースの認証を実行し、
前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了した後、第１のタイプのアクセスと第２のタイプのアクセスとを提供する
プロセッサと、
前記プロセッサに接続され、データを格納するメモリと
を備える装置。
［Ｃ４７］
前記プロセッサは更に、前記第２のＥＡＰベースの認証において第２のマスタ・セッション鍵（ＭＳＫ）を生成するように構成された、Ｃ４６に記載の複数のＥＡＰベースの認証のための装置。

［Ｃ４８］
前記プロセッサは更に、前記第２のマスタ・セッション鍵（ＭＳＫ）から第２の一時セッション鍵を生成するように構成された、Ｃ４７に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ４９］
前記第２の一時セッション鍵（ＴＳＫ）は、第３のＥＡＰベースの認証において用いられる、Ｃ４８に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ５０］
前記プロセッサは更に、第２のマスタ・セッション鍵（ＭＳＫ）が前記第２のＥＡＰベースの認証において生成されなかった場合、第３のＥＡＰベースの認証のために前記第１の一時セッション鍵（ＴＳＫ）を用いるように構成された、Ｃ４６に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ５１］
前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とは、単一のセッションの一部である、Ｃ４６に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ５２］
前記プロセッサは更に、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了したかを示すインジケータ・メッセージを生成するように構成されている、Ｃ４６に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ５３］
前記インジケータ・メッセージは、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが正しく完了したことを示す値１と、前記第１のＥＡＰベースの認証と前記第２のＥＡＰベースの認証とが完了しなかったことを示す値０とを有する、Ｃ５２に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ５４］
前記インジケータ・メッセージは、ＶａｌｉｄＰＭＫＥｘｉｓｔｓフラグである、Ｃ５３に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ５５］
前記プロセッサは更に、複数のＥＡＰベースの認証が正しく完了したかを示すインジケータ・メッセージを生成するように構成された、Ｃ４６に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ５６］
前記第１のＥＡＰベースの認証は、第１の認証タイプを含むＥＡＰ要求／アイデンティティ・メッセージを含み、前記第２のＥＡＰベースの認証は、第２の認証タイプを含むＥＡＰ要求／アイデンティティ・メッセージを含む、Ｃ４６に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ５７］
前記プロセッサは更に、
前記第１のＥＡＰベースの認証において第１のドメイン固有ルート鍵（ＤＳＲＫ）を生成し、
前記第２のＥＡＰベースの認証において第２のドメイン固有ルート鍵（ＤＳＲＫ）を生成し、
前記第１のＤＳＲＫと前記第２のＤＳＲＫとのうちの少なくとも１つを用いて、前記第１のタイプのアクセスか前記第２のタイプのアクセスかのうちの少なくとも１つのＥＡＰベースの再認証を実行する
ように構成された、Ｃ４６に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ５８］
前記第１のタイプのアクセスはアクセス端末（ＡＴ）に関連し、前記第２のタイプのアクセスはユーザに関連する、Ｃ４６に記載の複数のＥＡＰベースの認証のための装置。
［Ｃ５９］

前記第１のタイプのアクセスは、ラジオ・ネットワークへのアクセスを備え、前記第２のタイプのアクセスは、インターネット・サービス・プロバイダ（ＩＳＰ）を介したアクセスを備える、Ｃ４６に記載の複数のＥＡＰベースの認証のための装置。

［Ｃ６０］

前記第１のタイプのアクセスは特定のデバイスに関連し、前記第２のタイプのアクセスは特定のサーバに関連する、Ｃ４６に記載の複数のＥＡＰベースの認証のための装置。

【図１】

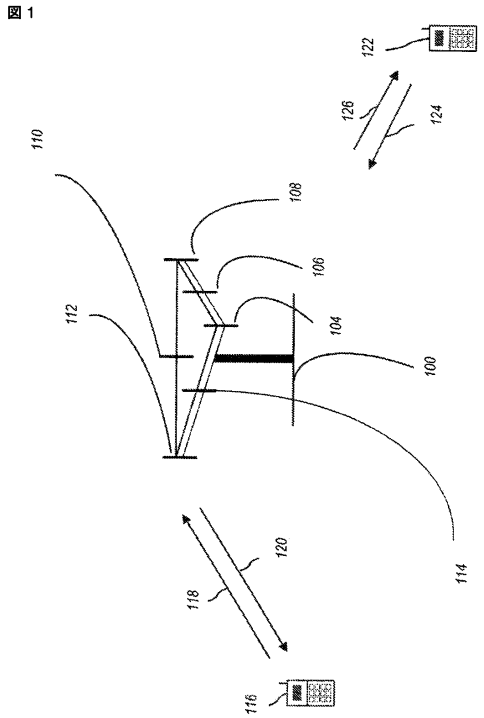

FIG. 1

【図２】

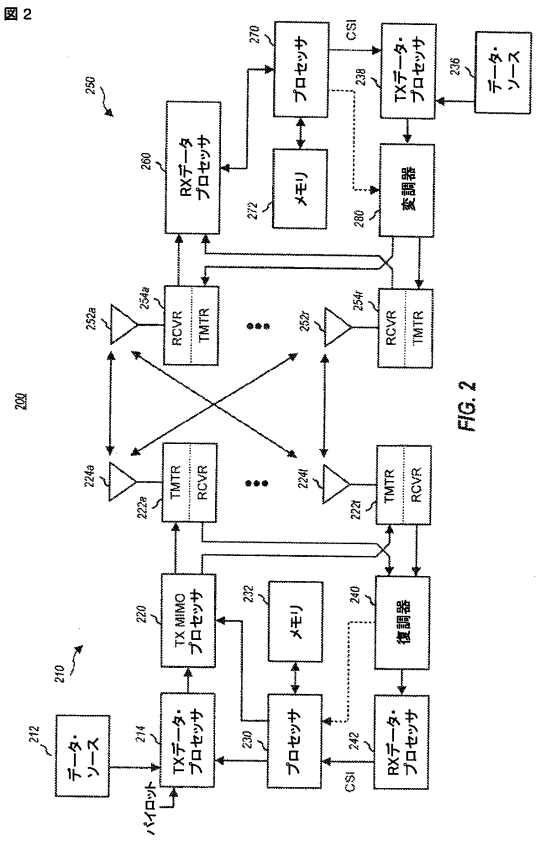

FIG. 2

【図３】

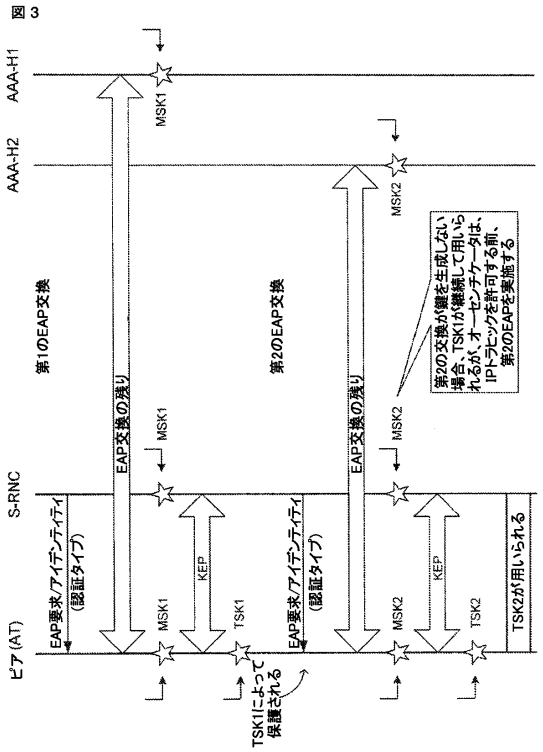

FIG. 3

【図４】

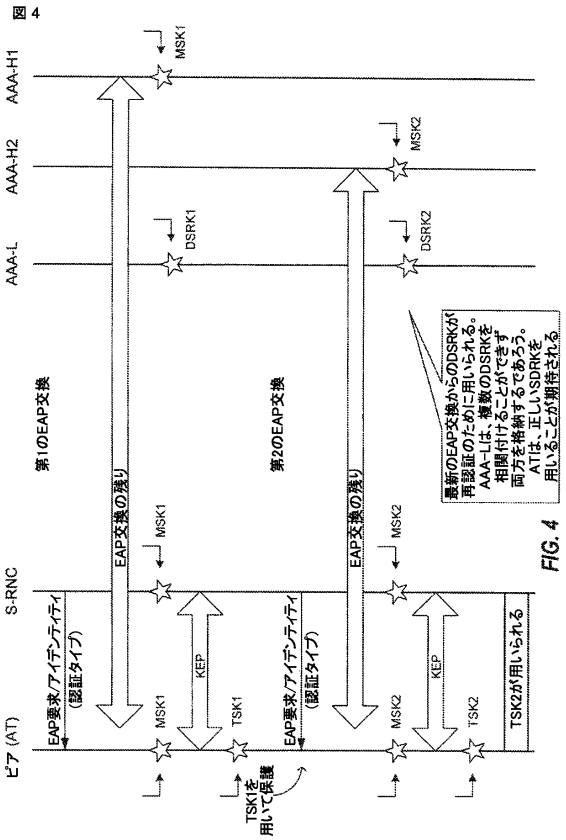

FIG. 4

フロントページの続き

(74)代理人 100075672
弁理士 峰 隆司
(74)代理人 100095441
弁理士 白根 俊郎
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100119976
弁理士 幸長 保次郎
(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100140176
弁理士 砂川 克
(74)代理人 100101812
弁理士 勝村 紘
(74)代理人 100070437
弁理士 河井 将次
(74)代理人 100124394
弁理士 佐藤 立志
(74)代理人 100112807
弁理士 岡田 貴志
(74)代理人 100111073
弁理士 堀内 美保子
(74)代理人 100134290
弁理士 竹内 将訓
(74)代理人 100127144
弁理士 市原 卓三
(74)代理人 100141933
弁理士 山下 元
(72)発明者 パトワードハン、ラビンドラ
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 ナラヤナン、ビドヤ
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 ウルピナー、ファティ
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 ドンデティ、ラクシュミナス・レディー
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 アガシェ、パラグ・アルン
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 ティンナコルンスリスプハプ、ピーラポル
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５

(72)発明者　シュ、レイモンド・ターーシェン
アメリカ合衆国、カリフォルニア州　９２１２１、サン・ディエゴ、モアハウス・ドライブ　５７７５
(72)発明者　ワン、ジュン
アメリカ合衆国、カリフォルニア州　９２１２１、サン・ディエゴ、モアハウス・ドライブ　５７７５

審査官　中里　裕正

(56)参考文献　国際公開第２００７／０３７８６９（WO，Ａ１）
国際公開第２００５／０６５１３２（WO，Ａ１）
国際公開第２００６／０７９４１９（WO，Ａ１）
国際公開第２００７／００５３１０（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L　9/08
H04L　9/32
H04W　12/04
H04W　12/06
JSTPlus/JMEDPlus/JST7580(JDreamII)