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

特許第5237441号
(P5237441)

(45)発行日　平成25年7月17日(2013.7.17)　(24)登録日　平成25年4月5日(2013.4.5)

(51)Int.Cl.		F I		
H04W 12/04	(2009.01)	H04W	12/04	
H04W 36/00	(2009.01)	H04W	36/00	
H04W 52/02	(2009.01)	H04W	52/02	１１０

請求項の数 28　(全 23 頁)

(21)出願番号	特願2011-511710 (P2011-511710)
(86)(22)出願日	平成21年5月19日 (2009.5.19)
(65)公表番号	特表2011-525069 (P2011-525069A)
(43)公表日	平成23年9月8日 (2011.9.8)
(86)国際出願番号	PCT/US2009/044571
(87)国際公開番号	WO2009/151896
(87)国際公開日	平成21年12月17日 (2009.12.17)
審査請求日	平成23年1月26日 (2011.1.26)
(31)優先権主張番号	12/127,377
(32)優先日	平成20年5月27日 (2008.5.27)
(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】ワイヤレス通信のためのセキュリティキーを維持するための方法およびシステム

(57)【特許請求の範囲】

【請求項１】

ワイヤレス通信のためにワイヤレスデバイスによって使用される1つまたは複数のセキュリティキーを維持するための方法であって、

通信イベントがいつ生じるべきかを決定することと、

少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの寿命を監視することと、

前記少なくとも1つのセキュリティキーが終了しそうであると識別される場合、前記通信イベントを遅延させることと、および

終了しそうであると識別された前記少なくとも1つのセキュリティキーを更新することと

を具備する方法。

【請求項２】

いずれのセキュリティキーも終了しそうでないと識別されるまで、決定することと、監視することと、遅延させることと、および更新することとの前記ステップを繰り返すことと、および

前記通信イベントを開始することと

をさらに具備する請求項1に記載の方法。

【請求項３】

前記通信イベントは、ハンドオーバーイベントであり、および

少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視することは、前記少なくとも1つのセキュリティキーの残りの寿命と前記ハンドオーバーイベントの予期される期間とを比較することを含む、請求項1に記載の方法。

【請求項４】

前記通信イベントは、電力節約モードであり、および

少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視することは、前記少なくとも1つのセキュリティキーの残りの寿命と前記電力節約モードの低電力状態の期間とを比較することを含む、請求項1に記載の方法。

【請求項５】

前記電力節約モードは、スリープモードを含む、請求項4に記載の方法。

【請求項６】

前記電力節約モードは、休止モードを含む、請求項4に記載の方法。

【請求項７】

前記ワイヤレスデバイスは、IEEE802.16（Institute of Electrical and Electronics Engineers）ファミリー規格の1つまたは複数の規格に準拠するフレームを使用して通信する、請求項1に記載の方法。

【請求項８】

ワイヤレス通信のためにワイヤレスデバイスによって使用される1つまたは複数のセキュリティキーを維持するように構成されている装置であって、

通信イベントがいつ生じるべきかを決定するための論理と、

少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの寿命を監視するための論理と、

前記少なくとも1つのセキュリティキーが終了しそうであると識別される場合、前記通信イベントを遅延させるための論理と、および

終了しそうであると識別された前記少なくとも1つのセキュリティキーを更新するための論理と

を具備する装置。

【請求項９】

いずれのセキュリティキーも終了しそうでないと識別されるまで、決定するための論理と、監視するための論理と、遅延させるための論理と、および更新するための論理とを繰り返すための論理と、および

前記通信イベントを開始するための論理と

をさらに具備する請求項8に記載の装置。

【請求項１０】

前記通信イベントは、ハンドオーバーイベントであり、および

少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視するための前記論理は、前記少なくとも1つのセキュリティキーの残りの寿命と前記ハンドオーバーイベントの予期される期間とを比較するための論理を含む、請求項8に記載の装置。

【請求項１１】

前記通信イベントは、電力節約モードであり、および

少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視するための前記論理は、前記少なくとも1つのセキュリティキーの残りの寿命と前記電力節約モードの低電力状態の期間とを比較するための論理を含む、請求項8に記載の装置。

【請求項１２】

前記電力節約モードは、スリープモードを含む、請求項11に記載の装置。

【請求項１３】
前記電力節約モードは、休止モードを含む、請求項11に記載の装置。
【請求項１４】
前記装置は、IEEE802.16（Institute of Electrical and Electronics Engineers）ファミリー規格の1つまたは複数の規格に準拠するフレームを使用して通信するための論理を含む、請求項8に記載の装置。
【請求項１５】
ワイヤレス通信のためにワイヤレスデバイスによって使用される1つまたは複数のセキュリティキーを維持するための装置であって、
通信イベントがいつ生じるべきかを決定するための手段と、
少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの寿命を監視するための手段と、
前記少なくとも1つのセキュリティキーが終了しそうであると識別される場合、前記通信イベントを遅延させるための手段と、および
終了しそうであると識別された前記少なくとも1つのセキュリティキーを更新するための手段と
を具備する装置。
【請求項１６】
いずれのセキュリティキーも終了しそうでないと識別されるまで、決定するための手段と、監視するための手段と、遅延させるための手段と、および更新するための手段とを繰り返すための手段と、および
前記通信イベントを開始するための手段と
をさらに具備する請求項15に記載の装置。
【請求項１７】
前記通信イベントは、ハンドオーバーイベントであり、および
少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視するための前記手段は、前記少なくとも1つのセキュリティキーの残りの寿命と前記ハンドオーバーイベントの予期される期間とを比較するための手段を含む、請求項15に記載の装置。
【請求項１８】
前記通信イベントは、電力節約モードであり、および
少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視するための前記手段は、前記少なくとも1つのセキュリティキーの残りの寿命と前記電力節約モードの低電力状態の期間とを比較するための手段を含む、請求項15に記載の装置。
【請求項１９】
前記電力節約モードは、スリープモードを含む、請求項18に記載の装置。
【請求項２０】
前記電力節約モードは、休止モードを含む、請求項18に記載の装置。
【請求項２１】
前記装置は、IEEE802.16（Institute of Electrical and Electronics Engineers）ファミリー規格の1つまたは複数の規格に準拠するフレームを使用して通信するための論理を含む、請求項15に記載の装置。
【請求項２２】
ワイヤレス通信のためにワイヤレスデバイスによって使用される1つまたは複数のセキュリティキーを維持するためのコンピュータプログラムであって、
複数のマイクロプロセッサに、通信イベントがいつ生じるべきかを決定させるための命令と、
前記複数のマイクロプロセッサに、少なくとも1つのセキュリティキーが前記通信イベ

ントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの寿命を監視させるための命令と、
前記複数のマイクロプロセッサに、前記少なくとも1つのセキュリティキーが終了しそうであると識別される場合、前記通信イベントを遅延させることをさせるための命令と、および
前記複数のマイクロプロセッサに、終了しそうであると識別された前記少なくとも1つのセキュリティキーを更新させるための命令と
を具備する、コンピュータプログラム。
【請求項２３】
前記複数のマイクロプロセッサに、いずれのセキュリティキーも終了しそうでないと識別されるまで、決定させるための命令と、前記複数のマイクロプロセッサに、監視させるための命令と、前記複数のマイクロプロセッサに、遅らせることをさせるための命令と、および更新させるための命令とを繰り返させるための命令と、および
前記複数のマイクロプロセッサに、前記通信イベントを開始させるための命令と
をさらに具備する、請求項22に記載のコンピュータプログラム。
【請求項２４】
前記通信イベントは、ハンドオーバーイベントであり、および
前記複数のマイクロプロセッサに、少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視するための前記命令は、前記複数のマイクロプロセッサに、前記少なくとも1つのセキュリティキーの残りの寿命と前記ハンドオーバーイベントの予期される期間とを比較させるための命令を含む、請求項22に記載のコンピュータプログラムプロダクト。
【請求項２５】
前記通信イベントは、電力節約モードであり、および
前記複数のマイクロプロセッサに、少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視させるための前記命令は、前記複数のマイクロプロセッサに、前記少なくとも1つのセキュリティキーの残りの寿命と前記電力節約モードの低電力状態の期間とを比較させるための命令を含む、請求項22に記載のコンピュータプログラム。
【請求項２６】
前記電力節約モードは、スリープモードを含む、請求項25に記載のコンピュータプログラム。
【請求項２７】
前記電力節約モードは、休止モードを含む、請求項25に記載のコンピュータプログラム。
【請求項２８】
前記複数のコンピュータプログラムは、IEEE802.16（Institute of Electrical and Electronics Engineers）ファミリー規格の1つまたは複数の規格に準拠するフレームを使用して通信させるための命令を含む、請求項22に記載のコンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本件開示のある実施形態は、一般に、ワイヤレス通信に関係し、より詳細には、ワイヤレスデバイスにおける移動状態にわたるようなワイヤレス通信のためのセキュリティキーを維持することに関係する。
【背景技術】
【０００２】
IEEE802.16に基づくOFDMおよびOFDMAワイヤレス通信システムは、複数のサブキャリアの周波数の直交性に基づいて、システムにおいてサービスを提供するために登録されてい

るワイヤレスデバイス（つまり、移動局）と通信するために基地局のネットワークを使用し、およびマルチパスフェージングおよび干渉に対する抵抗のような広帯域ワイヤレス通信のためのいくつかの技術的利点を達成するために実装されることができる。各々の基地局（BS）は、移動局（MS）へおよびMSからデータを伝達する無線周波数（RF）信号を送信および受信する。

【０００３】

そのようなシステムにおいて、セキュリティプロトコルは、ネットワークおよび移動局がAK（認証キー）およびTEK（トラヒック暗号化キー）キーのような正当なセキュリティキーを共有することをしばしば要求する。これらのセキュリティキーは、両方の搬送接続のみならず両方の管理接続のために使用される。異なるセキュリティキーは、異なる寿命を有し、前記規格は、それらの寿命に依存してネットワークおよび移動局が当該キーを周期的に更新することを必要とする。セキュリティキーの寿命が、当該キーが更新される前に終了する場合、移動局とネットワークとの間の通信は、新しいセキュリティキーが成功的に交渉されるまで停止させられる。

【０００４】

残念ながら、新しいキーを交渉することは、ユーザ経験をそこなう比較的長い処理であり得る。基地局間のハンドオーバーの間にセキュリティキー寿命が終了する場合、移動局と新しい基地局との間の通信は、新しいセキュリティキーが成功的に交渉されるまで遅延させられる。したがって、ハンドオーバーによって生じるトラヒックにおいていくらかの中断を増す。

【発明の概要】

【０００５】

本件明細書において提供される技術は、ハンドオーバーモード、休止モード、およびスリープモードのような様々な移動システム状態、または通信イベントにわたってセキュリティキーが維持されることを可能にする。

【０００６】

ある実施形態は、ワイヤレス通信のためにワイヤレスデバイスによって使用される1つまたは複数のセキュリティキーを維持するための方法であって、通信イベントがいつ生じるべきかを決定することと、少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視することと、前記少なくとも1つのセキュリティキーが終了しそうであると識別される場合前記通信イベントを遅延させることと、および終了しそうであると識別された前記少なくとも1つのセキュリティキーを更新することとの1つまたは任意の組合せを含む方法を提供する。ある実施形態において、前記方法は、いずれのセキュリティキーも終了しそうでないと識別されるまで、決定することと、監視することと、遅延させることと、および更新することとの前記ステップを繰り返すことと、および前記通信イベントを開始することとを含むことができる。ある実施形態において、前記通信イベントは、ハンドオーバーイベント、電力節約モード、スリープモード、または休止モードを含むことができる。ある実施形態において、前記方法は、IEEE802.16（Institute of Electrical and Electronics Engineers）ファミリー規格のうちの1つまたは複数の規格に準拠するフレームを使用して通信することを含むことができる。

【０００７】

ある実施形態は、ワイヤレス通信のためにワイヤレスデバイスによって使用される1つまたは複数のセキュリティキーを維持するように構成されている装置であって、通信イベントがいつ生じるべきかを決定するための論理と、少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視するための論理と、前記少なくとも1つのセキュリティキーが終了しそうであると識別される場合前記通信イベントを遅延させるための論理と、および終了しそうであると識別された前記少なくとも1つのセキュリティキーを更新するための論理との1つまたは任意の組合せを含む装置を提供する。ある実施形態におい

て、前記装置は、いずれのセキュリティキーも終了しそうでないと識別されるまで、決定するための論理と、監視するための論理と、遅延させるための論理と、および更新するための論理とを繰り返すための論理と、および前記通信イベントを開始するための論理とを含むことができる。ある実施形態において、前記通信イベントは、ハンドオーバーイベント、電力節約モード、スリープモード、または休止モードを含むことができる。ある実施形態において、前記装置は、IEEE802.16（Institute of Electrical and Electronics Engineers）ファミリー規格のうちの1つまたは複数の規格に準拠するフレームを使用して通信するための論理を含むことができる。

【０００８】

ある実施形態は、ワイヤレス通信のためにワイヤレスデバイスによって使用される1つまたは複数のセキュリティキーを維持するための装置であって、通信イベントがいつ生じるべきかを決定するための手段と、少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視するための手段と、前記少なくとも1つのセキュリティキーが終了しそうであると識別される場合前記通信イベントを遅延させるための手段と、および終了しそうであると識別された前記少なくとも1つのセキュリティキーを更新するための手段との1つまたは任意の組合せを含む装置を提供する。ある実施形態において、前記装置は、いずれのセキュリティキーも終了しそうでないと識別されるまで、決定するための手段と、監視するための手段と、遅延させるための手段と、および更新するための手段とを繰り返すための手段と、および前記通信イベントを開始するための手段とを含むことができる。ある実施形態において、前記通信イベントは、ハンドオーバーイベント、電力節約モード、スリープモード、または休止モードを含むことができる。ある実施形態において、前記装置は、IEEE802.16（Institute of Electrical and Electronics Engineers）ファミリー規格のうちの1つまたは複数の規格に準拠するフレームを使用して通信するための手段を含むことができる。

【０００９】

ある実施形態は、1セットの命令を内蔵するコンピュータ可読媒体を具備する、ワイヤレス通信のためにワイヤレスデバイスによって使用される1つまたは複数のセキュリティキーを維持するためのコンピュータプログラムプロダクトであって、命令の前記セットは、1つまたは複数のプロセッサによって実行され、命令の前記セットは、通信イベントがいつ生じるべきかを決定するための命令と、少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視するための命令と、前記少なくとも1つのセキュリティキーが終了しそうであると識別される場合前記通信イベントを遅延させるための命令と、および終了しそうであると識別された前記少なくとも1つのセキュリティキーを更新するための命令との1つまたは任意の組合せを含む、コンピュータプログラムプロダクトを提供する。ある実施形態において、命令の前記セットは、いずれのセキュリティキーも終了しそうでないと識別されるまで、決定するための命令と、監視するための命令と、遅延させるための命令と、および更新するための命令とを繰り返すための命令と、および前記通信イベントを開始するための命令とを含むことができる。ある実施形態において、前記通信イベントは、ハンドオーバーイベント、電力節約モード、スリープモード、または休止モードを含むことができる。ある実施形態において、命令の前記セットは、IEEE802.16（Institute of Electrical and Electronics Engineers）ファミリー規格のうちの1つまたは複数の規格に準拠するフレームを使用して通信するための命令を含むことができる。

【図面の簡単な説明】

【００１０】

本件開示の上述の特徴が詳細に理解されることができるように、実施形態に対する言及によってさらに具体的な記載（上で簡潔な要約が与えられている）が提供されることができる。そのような実施形態のうちのいくつかが添付の図面に例示されている。しかしながら、添付の図面は、あくまで本件開示のある典型的実施形態を例示するものであって、そ

の範囲を制限するものと考えてはならないということが理解されるべきである。というのは、本件記載は、他の等しく効果的な実施形態に対しても妥当するからである。
【図１】図1は、本件開示のある実施形態にしたがって、ワイヤレス通信システムの一例を例示している。
【図２】図2は、本件開示のある実施形態にしたがって、ワイヤレスデバイスにおいて利用されることができる様々なコンポーネントを例示している。
【図３】図3は、本件開示のある実施形態にしたがって、直交周波数分割多重および直交周波数分割多元接続（OFDM／OFDMA）技術を利用するワイヤレス通信システム内で使用されることができる送信機の一例および受信機の一例を例示している。
【図４】図4は、本件開示の実施形態にしたがって、セキュリティキーを交渉するための移動局と基地局との間のトランザクションの一例を例示している。
【図５】図5は、本件開示の実施形態にしたがって、基地局間のハンドオーバーにわたってセキュリティキーを維持するためのオペレーションの一例を例示している。
【図５Ａ】図5Aは、図5のオペレーションの一例を実行することができるコンポーネントのブロック図である。
【図６Ａ】図6Aは、本件開示の実施形態にしたがって、通常のハンドオーバーおよび遅延ハンドオーバーの間のタイミングにおける中断の一例をそれぞれ例示している。
【図６Ｂ】図6Bは、本件開示の実施形態にしたがって、通常のハンドオーバーおよび遅延ハンドオーバーの間のタイミングにおける中断の一例をそれぞれ例示している。
【図７】図7は、本件開示の実施形態にしたがって、スリープモードにおける利用不能な期間にわたってセキュリティキーを維持するためのオペレーションの一例を例示している。
【図７Ａ】図7Aは、図7のオペレーションの一例を実行することができるコンポーネントのブロック図である。
【図８】図8は、本件開示の実施形態にしたがって、休止モードにおける利用不能な期間にわたってセキュリティキーを維持するためのオペレーションの一例を例示している。
【図８Ａ】図8Aは、図8のオペレーションの一例を実行することができるコンポーネントのブロック図である。
【発明の詳細な説明】
【００１１】
本件開示のある実施形態は、ハンドオーバーモード、休止モード、およびスリープモードのような様々な移動デバイス状態、または通信イベントにわたってセキュリティキーが維持されることを可能にする。セキュリティキーの寿命を監視することによって、ハンドオーバープロセスまたはデバイス利用不能状態の間にキーの寿命が終了しないことを確実にするためにキーが更新されることができる。その結果、トラフィックにおける中断の合計継続時間は、セキュリティキーの長い再交渉を回避することによって低減されることができる。
【００１２】
例示的ワイヤレス通信システム
本件開示の方法および装置は、広帯域ワイヤレス通信システムにおいて利用されることができる。本件明細書において使用されるように、用語「広帯域ワイヤレス」とは、一般に、所与のエリアにわたる音声、インターネットおよび／またはデータのネットワーク接続のようなワイヤレスサービスの任意の組み合わせを提供することができる技術のことをいう。
【００１３】
WiMAX（Worldwide Interoperability for Microwave Accessを表す）は、長距離にわたって高いスループットの広帯域接続を提供する規格ベースの広帯域ワイヤレス技術である。今日、WiMAXの２つの主要なアプリケーションがある。これらは、固定WiMAXおよびモバイルWiMAXである。固定WiMAXアプリケーションは、例えば、家庭およびビジネスへの広帯域接続を可能にするポイント・ツー・マルチポイントである。モバイルWiMAXは、広帯域

スピードにおけるセルラーネットワークの完全な移動性を提案する。

【００１４】

モバイルWiMAXは、OFDM（直交周波数分割多重）およびOFDMA（直交周波数分割多元接続）技術に基づいている。OFDMは、様々な高いデータレート通信システムにおける広い採用を最近見い出したデジタルマルチキャリア変調技術である。OFDMにより、送信ビットストリームは、複数の低いレートのサブストリームに分割される。各々のサブストリームは、複数の直交サブキャリアの１つにより変調され、複数の並列サブチャネルのうちの１つのサブチャネル上で送られる。OFDMAは、異なる時間スロットにおいてユーザにサブキャリアが割り当てられる多元接続技術である。OFDMAは、広く様々なアプリケーション、データレート、およびサービス品質要求を多くのユーザに用立てることができる柔軟な多元接続技術である。

【００１５】

ワイヤレスインターネットおよびワイヤレス通信における急速な成長は、ワイヤレス通信サービスの分野において高いデータレートの要求を高めることになった。OFDM／OFDMAシステムは、今日、最も将来性のある研究分野のうちの１つ、およびワイヤレス通信の次世代のための重要な技術、とみなされている。これは、OFDM／OFDMA変調方式が、通常のシングルキャリア変調方式にまさって、変調の効率、スペクトルの効率、柔軟性および強いマルチパス耐性のような多くの利点を提供することができるという事実に起因する。

【００１６】

IEEE802.16ｘは、固定型および移動型広帯域ワイヤレス接続（BWA）システムのための空間インターフェースを定義するための新規の規格組織である。これらの規格は、少なくとも4つの異なる物理層（PHY）および１つのメディアアクセス制御（MAC）層を定義する。4つの物理層のうちOFDM物理層およびOFDMA物理層は、固定型および移動型BWAエリアにおいてそれぞれ最も広く普及している。

【００１７】

図1は、本件開示の実施形態が採用されることができるワイヤレス通信システム100の一例を例示している。ワイヤレス通信システム100は、広帯域ワイヤレス通信システムであってもよい。ワイヤレス通信システム100は、いくつかのセル102のために通信を提供することができる。セル102の各々は、基地局104によってサービスされる。基地局104は、ユーザ端末106と通信する固定局であってもよい。基地局104は、アクセスポイント、ノードB、またはなんらかの他の用語で代替的に呼ばれてもよい。

【００１８】

図1は、システム100の全体にわたって分散される様々なユーザ端末106を図示している。ユーザ端末106は、遠隔局、アクセス端末、端末、加入者ユニット、移動局、局、ユーザ設備などと代替的に呼ばれてもよい。ユーザ端末106は、セルラー電話、携帯情報端末（PDA）、ハンドヘルドデバイス、ワイヤレスモデム、ラップトップコンピュータ、パーソナルコンピュータなどのようなワイヤレスデバイスであってもよい。

【００１９】

基地局104とユーザ端末106との間のワイヤレス通信システム100における送信のために様々なアルゴリズムおよび方法が使用されてもよい。例えば、OFDM/OFDMA技術にしたがって基地局104とユーザ端末106との間で信号が送信および受信されることができる。この場合、ワイヤレス通信システム100は、OFDM/OFDMAシステムと呼ばれてもよい。

【００２０】

基地局104からユーザ端末106への送信を容易にする通信リンクは、ダウンリンク108と呼ばれてもよく、ユーザ端末106から基地局104への送信を容易にする通信リンクは、アップリンク110と呼ばれてもよい。代替的に、ダウンリンク108は、順方向リンクまたは順方向チャネルと呼ばれてもよく、アップリンク110は、逆方向リンクまたは逆方向チャネルと呼ばれてもよい。

【００２１】

セル102は、複数のセクター112に分割されることができる。セクター112は、セル102内

の物理的カバレッジエリアである。ワイヤレス通信システム100内の基地局104は、セル102の特定のセクター112内に電力の流れを集中するアンテナを利用することができる。そのようなアンテナは、指向性アンテナと呼ばれてもよい。

【００２２】

図2は、ワイヤレス通信システム100内で採用されることができるワイヤレスデバイス202において利用されることができる様々なコンポーネントを例示している。ワイヤレスデバイス202は、本件明細書において説明される様々な方法を実装するように構成されていてもよいデバイスの一例である。ワイヤレスデバイス202は、基地局104またはユーザ端末106であってもよい。

【００２３】

ワイヤレスデバイス202は、ワイヤレスデバイス202のオペレーションを制御するプロセッサ204を含むことができる。プロセッサ204はまた、中心処理装置（CPU）と呼ばれてもよい。メモリ206（読み出し専用メモリ（ROM）およびランダムアクセスメモリ（RAM）の両方を含んでもよい）は、プロセッサ204に命令およびデータを提供する。メモリ206のうちの一部はまた、不揮発性のランダムアクセスメモリ（NVRAM）を含んでもよい。プロセッサ204は、典型的に、メモリ206内に記憶されるプログラム命令に基づいて論理および算術演算を実行する。メモリ206における命令は、本件明細書において説明される方法を実装するために実行可能であってもよい。

【００２４】

ワイヤレスデバイス202はまた、ワイヤレスデバイス202と遠隔位置との間のデータの送信および受信を可能にするために送信機210および受信機212を含むことができるハウジング208を含んでもよい。送信機210および受信機212は、１つの送受信機214に統合されることができる。アンテナ216は、ハウジング208に取り付けられてもよく、送受信機214に電気的に結合されてもよい。ワイヤレスデバイス202はまた、複数の送信機、複数の受信機、複数の送受信機、および／または複数のアンテナ（図示されていない）を含む。

【００２５】

ワイヤレスデバイス202はまた、送受信機214によって受信される信号レベルを検出および量子化するために使用されることができる信号検出器218を含んでもよい。信号検出器218は、全体のエネルギー、擬似雑音（PN）チップごとのパイロットエネルギー、電力スペクトル密度、および他の信号としてそのような信号を検出することができる。ワイヤレスデバイス202はまた、処理信号における使用のためにデジタル信号プロセッサ（DSP）220を含むことができる。

【００２６】

ワイヤレスデバイス202の様々なコンポーネントは、バスシステム222によって一緒に結合されることができる。バスシステム222は、データバスに加えて、電力バス、制御信号バス、および状態信号バスを含むことができる。

【００２７】

図3は、OFDM/OFDMAを利用するワイヤレス通信システム100内で使用されることができる送信機302の一例を例示している。送信機302のうちの複数の部分は、ワイヤレスデバイス202の送信機210において実装されることができる。送信機302は、ダウンリンク108上でユーザ端末106にデータ306を送信するために基地局104において実装されることができる。送信機302はまた、アップリンク110上で基地局104にデータ306を送信するためにユーザ端末106において実装されることができる。

【００２８】

送信されるデータ306は、直並列（S/P）変換器308への入力として提供されるよう図示されている。S/P変換器308は、送信データをN個の並列データストリーム310に分割することができる。

【００２９】

N個の並列データストリーム310は、次に、マッパー312への入力として提供されることができる。マッパー312は、N個のコンスタレーションポイント（信号点配置）上にN個の

並列データストリーム310をマップすることができる。当該マッピングは、BPSK（2値位相シフトキーイング）、QPSK（直交位相シフトキーイング）、8PSK（8位相シフトキーイング）、QAM（直交振幅変調）などのようないくつかの変調コンスタレーションを使用してなされることができる。したがって、マッパー312は、N個の並列シンボルストリーム316を出力することができる。ここにおいて、各々のシンボルストリーム316は、IFFT（逆高速フーリエ変換）320のN個の直交サブキャリアのうちの１つに対応する。これらのN個の並列シンボルストリーム316は、周波数ドメインで表わされ、IFFTコンポーネント320によってN個の並列の時間ドメインのサンプルストリーム318に変換されることができる。

【００３０】

用語についての簡単な注意がこれから提供される。周波数ドメインにおけるN個の並列変調は、周波数ドメインにおけるN個の変調シンボルと等しい。当該N個の変調シンボルは、周波数ドメインにおけるN個のマッピングおよびNポイントIFFTと等しい。当該N個のマッピングおよびNポイントIFFTは、時間ドメインにおける１つの（有用な）OFDMシンボルと等しい。当該OFDMシンボルは、時間ドメインにおけるN個のサンプルと等しい。時間ドメインにおける１つのOFDMシンボル、Nsは、Ncp（OFDMシンボルごとのガードサンプルの数）+N（OFDMシンボルごとの有用なサンプルの数）と等しい。

【００３１】

N個の並列の時間ドメインのサンプルストリーム318は、並直列（P/S）変換器324によってOFDM/OFDMAシンボルストリーム322に変換されることができる。ガード挿入コンポーネント326は、OFDM/OFDMAシンボルストリーム322における連続するOFDM/OFDMAシンボルの間にガードインターバルを挿入することができる。ガード挿入コンポーネント326の出力は、次に、無線周波数（RF）フロントエンド328によって所望の送信周波数帯域にアップコンバートされることができる。アンテナ330は、次に、結果の信号332を送信することができる。

【００３２】

図3はまた、OFDM/OFDMAを利用するワイヤレスデバイス202内で使用されることができる受信機304の一例を例示している。受信機304の複数の部分は、ワイヤレスデバイス202の受信機212において実装されてもよい。受信機304は、ダウンリンク108上で基地局104からデータ306を受信するためのユーザ端末106において実装されてもよい。受信機304はまた、アップリンク110上でユーザ端末106からデータ306を受信するための基地局104において実装されてもよい。

【００３３】

送信信号332は、ワイヤレスチャネル334にわたって移動をしているよう図示されている。信号332’がアンテナ330’によって受信されるとき、受信信号332’は、RFフロントエンド328’によってベースバンド信号にダウンコンバートされることができる。ガード除去コンポーネント326’は、次に、ガード挿入コンポーネント326によってOFDM/OFDMAシンボルの間に挿入されたガードインターバルを除去することができる。

【００３４】

ガード除去コンポーネント326’の出力は、S/P変換器324’に提供されることができる。S/P変換器324’は、OFDM/OFDMAシンボルストリーム322’をN個の並列の時間ドメインのシンボルストリーム318’に分割することができる。ここにおいて、当該シンボルストリーム318’の各々は、N個の直交サブキャリアのうちの１つに対応する。高速フーリエ変換（FFT）コンポーネント320’は、N個の並列の時間ドメインのシンボルストリーム318’を周波数ドメインに変換し、N個の並列の周波数ドメインのシンボルストリーム316’を出力することができる。

【００３５】

デマッパー312’は、マッパー312によって実行されたシンボルマッピング・オペレーションの逆を実行することができる。それによって、N個の並列のデータストリーム310’を出力する。P/S変換器308’は、N個の並列のデータストリーム310’を結合して単一のデータストリーム306’に変換することができる。理想的には、このデータストリーム306’は

、送信機302への入力として提供されたデータ306に対応する。エレメント308’、310’、312’、316’、320’、318’および324’は、ベースバンドプロセッサ340’においてすべて見つけ出されることができる。

【００３６】

基地局ハンドオーバーにわたるセキュリティキーの維持

基地局間でハンドオーバーをするための移動局のための様々な技術がIEEE802.16e-2005規格においてサポートされる。MSによって報告される測定結果に基づいて、BSまたはMSによってハンドオーバー決定がなされることができる。MSは、RFスキャンを周期的に行い、近隣の基地局の信号品質を測定することができる。例えば、現在のセルを越える1つのセル、信号フェーディングまたは干渉に至る位置を変えるMS、またはより高いサービス品質（QoS）を必要とするMSからの信号強度に基づいてハンドオーバー決定がなされてもよい。それとは関係なく、ハンドオーバー決定がいったんなされると、MSは、新しいBSのダウンリンク送信との同期を開始し、スキャニングの間にレンジングがなされていなければレンジングを行い、および以前のBSとの接続を終了する。

【００３７】

WiMAXセキュリティプロトコルにしたがって、ハンドオーバーの後に新しいBSとデータを交換する前に、MSは、正当なセキュリティキーを確立している必要がある。以前に交渉された1セットのセキュリティキーの寿命の前にハンドオーバー手順が完了されると仮定すると、ハンドオーバーのすぐ後にデータ交換が始まってもよい。これに対して、ハンドオーバー手順の間に1つまたは複数のセキュリティキーのための寿命が終了する場合、新しいBSとの正当なセキュリティキーをMSが交渉することができるまで新しいBSとのデータ交換が遅延させられる。したがって、トラヒックにおける中断の合計は、このキー交渉の長さによって増加させられるのであって、その増加は、ユーザ経験を著しく低下させるのに十分な相当な値となる可能性がある。

【００３８】

図4は、本件開示の実施形態にしたがって、セキュリティキーを交渉するためのMSとBSとの間のトランザクションの一例を例示している。例示されているように、セキュリティプロトコルは、AK（認証キー）およびTEK（トラヒック暗号キー）キーのような1セットの異なるタイプの正当なセキュリティキーを確立するためのBSおよびMSを必要とするかもしれない。これらのセキュリティキーは、両方の送信接続のみならず両方の管理接続のために使用されてもよい。

【００３９】

AKは、BSに送られる認証要求402を介してMSによって交渉されてもよい。これに応答して、BSは、AKを生成することができ、認証応答404においてAKについての対応するキーシーケンス番号および対応する寿命を送ることができる。同様の方法で、TEKは、BSに送られるTEKキー要求406を介して交渉されてもよい。これに応答して、BSは、TEKキーを生成することができ、TEKキー応答408においてTEKおよびTEKキーについての対応する寿命を送ることができる。正当なキーを確立した後、MSとBSとの間のデータ交換410が起きてもよい。

【００４０】

例示されているように、異なるセキュリティキーは、異なる寿命（TAK412およびTTEK414）を有していてもよく、規格は、それらの寿命の長さに依存してキーを周期的に更新するためのネットワークおよび移動局を必要としてもよい。キーが更新される前にセキュリティキー寿命が終了する場合、MSとBSとの間のデータ交換は、新しいセキュリティキーが成功的に交渉されるまで停止させられる。

【００４１】

図5は、本件開示の実施形態にしたがって、基地局間のハンドオーバーの間にセキュリティキーが終了することを回避するために、MSにおいて実行されることができるオペレーション500の一例を例示している。オペレーション500は、502において、ハンドオーバー決定をするためにサービングおよび近隣の基地局信号品質を監視することによって始まる

。

【００４２】

肯定的なハンドオーバー決定がいったんなされると、504において、ハンドオーバープロセスを実際に開始する前にセキュリティキー寿命の状態がチェックされてもよい。ハンドオーバープロセスは、正当なキーが確立され、ハンドオーバープロセスの後に正当なまま維持することを確実にするために、必要な場合は遅延させられてもよい。

【００４３】

例えば、キー交渉（現在のサービング基地局との）が進行している場合、506においての決定にしたがって、ハンドオーバープロセスは、遅延させられてもよい。ハンドオーバープロセスは、例えば、512において肯定的なハンドオーバー決定を取り消すことによって、および514において交渉が完了するのを待つことによって遅延させられるかもしれない。キー交渉が完了するまで待つことは、完全な寿命を備えるセキュリティキーを確実にしてもよい。したがって、肯定的なハンドオーバー決定が再びなされる場合、504において、キーは、ハンドオーバープロセスの後もなお正当であるはずである。

【００４４】

キー寿命はまた、508において、いずれかのキーがハンドオーバープロセスの完了の前に終了しそうであるかを決定するために調査されてもよい。この決定のために、キーの残りの寿命が予測ハンドオーバー時間に対して比較されることができる。この比較は、たぶん、控えめに見積もっておくための最悪のシナリオ条件を考慮に入れてなされるであろう。ハンドオーバーの完了の前に１つまたは複数のキーが終了しそうである場合、MSは、510において、終了するキーのために交渉を開始してもよい。MSは、512において、肯定的なハンドオーバー決定を取り消すことによって、および514において、交渉が完了することを待つことによってハンドオーバープロセスを再び遅延させてもよい。

【００４５】

現在継続中のキー交渉がなく（506につき）、かつ、終了しているキーがないまたはハンドオーバーの間に終了しそうなキーがない（508につき）場合、MSは、516において、肯定的なハンドオーバーのプロセスに進んでもよい。

【００４６】

図6Aおよび6Bは、図5のオペレーションにしたがってハンドオーバープロセスを遅延させることが基地局間のハンドオーバーにより経験する全体のトラヒック中断時間を低減することをどのように助けることができるかを例示している。図6Aを最初に参照して、ハンドオーバーの間にセキュリティキーが終了することを可能にするハンドオーバープロセスの図の一例が例示されている。

【００４７】

図6Aにおける事例は、第1の基地局（BS-A）による通常のオペレーション602の間に確立されるTEKセキュリティキーが、第2の基地局（BS-B）へのハンドオーバープロセス604の間に終了する寿命TTEK610を有すると仮定する。データ送信がBS-Bを再開する前に正当なセキュリティキーが必要とされるので、MSは、ハンドオーバーの後にキー交渉606を開始しなければならない。その結果、トラヒック608Aにおける中断の合計は、ハンドオーバー時間を超えてキー交渉が完了するまで延長される。

【００４８】

これに対し、図6Bは、トラヒック608Bにおいて、低減された全体の中断という結果となる「遅延」ハンドオーバープロセスを例示している。図6Bにおける事例は、第1の基地局（BS-A）による通常のオペレーション602の間に確立されたTEKセキュリティキーが、第2の基地局（BS-B）へのハンドオーバープロセス604の間に終了する寿命TTEK610を有すると再び仮定する。

【００４９】

しかしながら、セキュリティキー寿命を監視することによって、MSは、TEKキー寿命がハンドオーバープロセス604の間に終了するかもしれないと決定するかもしれない。これに応答して、MSは、ハンドオーバープロセスを遅延させることができ、キー交渉606を開

始することができる。キー交渉606の間、終了するTEKキーは、まだ正当であり、したがって、MSは、BS-Aとトラヒックをまだ交換することができる。したがって、キー交渉606の間、トラヒックにおける中断がない。

【００５０】

キー交渉606の完了の後、MSは、ハンドオーバープロセス604の十分後に終了する寿命TTEK’610’を備える新しいTEKキーを有する。その結果、通常のオペレーション602は、ハンドオーバープロセス604の後にキー交渉の追加の遅延によらずに（新しく交渉されたTEKキーを使用して）MSとBS-Bとの間のデータ交換を始めることができる。したがって、ハンドオーバープロセスの間に終了するように設定されたセキュリティキーを更新するためにハンドオーバープロセスを遅延させることによって、図6Bのトラヒック608Bにおける全体の中断は、図6Aのトラヒック608Aにおける全体の中断よりも著しく少なくなることができる。

【００５１】

スリープ状態および休止状態にわたるセキュリティキーの維持

WiMAX規格は、MSがデータをアクティブに送信または受信していないとき特定の回路の電力を落とすことによって、可搬型の加入者局がバッテリー寿命を延ばすことを可能にする電力節約状態を定義する。例えば、スリープモードにおいて、MSは、サービングBSと交渉される予め定義された時間の間の利用不能な時間（スリープウィンドウと呼ばれる）の間MS自身を効果的にオフにする。スリープウィンドウの間に、MSに低電力状態から抜け出させるトラヒックまたはメッセージを監視するために（リスニングウィンドウにおいて）MSは起きる。

【００５２】

スリープウィンドウは、デバイスが所属する特定の電力節約等級（PSC）に応じて、固定されているものであってもよく、または指数的に増加するものであってもよい。PSCタイプは、MSが取り扱っている特定の接続のトラヒックのタイプに基づいて決定されることができる。PSC1は、典型的に、ベストエフォート（BE）および非リアルタイム可変レート（NRT-VR）トラヒックに使用される。PSC2は、固定長のスリープウィンドウを有し、典型的に、USG（unsolicited grant service）のために使用される。PSC3は、１回のスリープウィンドウを有するものであって、典型的には、MSが次のトラヒックの到来時を知っている場合に、マルチキャストトラヒックまたは管理トラヒックのために使用されるものである。

【００５３】

残念ながら、MSがスリープモードにおいて利用不能であるとき、セキュリティキーは、スリープウィンドウの間に終了するかもしれない。上で説明されたようなハンドオーバープロセスとほぼ同様に、スリープウィンドウの間にキーが終了する場合、利用可能なインターバル（リスニングウィンドウ）にMSが入った後に新しいキーが交渉されなければならない。ユーザが送信しなければならないデータを有している場合、そのデータの送信は、新しいキーが成功的に交渉されるまで遅延させられ、それによって、全体のデータスループットに否定的に影響を与える。これは、MSからのトラヒックのみならず、ネットワークからMSへのトラヒックにも影響を与える。したがって、セキュリティキーが終了した後にキーの交渉をしなければならないことに関連する遅延は、終了するキーと関連する特定のサービスフローに対するサービス品質（QoS）侵害という結果となり得る。

【００５４】

しかしながら、本件開示の実施形態は、MSがスリープモードにあるときキーの終了時間を監視することによって、これらの遅延を回避することを助けることができる。スリープモードにおける利用不能なウィンドウにおいてキーが終了することをMSが検出する場合、MSは、スリープモードを早めに（例えば、自然な抜け出しを生じさせるイベントの前に）終了することを決定し、かつ、ネットワークと新しいキーを交渉してもよい。

【００５５】

図7は、702においてアクティブにさせられる、スリープモードにおける利用不能な期間

にわたってセキュリティキーを維持するためのオペレーション700の一例を例示している。704において、キーの残りの寿命が監視される。706において、MSがスリープウィンドウにあるとき、利用不能な期間の間にいずれかのキーが終了するように設定されているかどうかの決定がなされる。この決定のために、キーの残りの寿命は、例えば、スリープウィンドウが固定であるか、または指数的に増加しているかどうかを考慮に入れて、予期されるスリープウィンドウと比較されてもよい。いずれのキーも終了しそうでない場合、デバイスは、スリープウィンドウに入り、かつ、スリープモードのままでいることが許されることができる。

【００５６】

反対に、1つまたは複数のキーがスリープウィンドウの間に終了するように設定されている場合、708において、MSは、スリープモードを早めに終わらせることができ、710において、新しい単一のキー（または複数のキー）を交渉することができる。当該終了するキーを更新するためにスリープモードから早めに抜け出すことは、データトラヒックを中断するかもしれない長いキーの再交渉を防ぐことを助けることができる。キー交渉が完了し、当該終了するキー（複数）が更新された後、MSは、スリープモードを再びアクティブにすることができる。

【００５７】

現行版のWiMAX規格では選択的ではあるけれど、休止モードは、MSのコンポーネントが電源オフにされたままの状態でもって、いっそう大きな電力節約を実施することができる。MSのコンポーネントが電源オフにされている間、MSは、DLブロードキャストトラヒックをまだ受信していながら、未登録状態である。MSは、ページングメッセージをチェックするため、および自身のページンググループを更新するために周期的に起きる。

【００５８】

残念ながら、休止モードにおける電力節約状態の間にセキュリティキーが終了するかもしれない。キーが終了する場合、ユーザが接続を作ること（例えば、音声電話）を開始するとき、新しいキーが成功的に交渉されるまで当該接続が遅延させられる。その結果、接続セットアップ時間は、延ばされる。これは、ユーザ経験に対して否定的な影響を有するかもしれない。

【００５９】

図8は、802においてアクティブにされる、休止モードにおける低電力状態にわたってセキュリティキーを維持するためのオペレーション800の一例を例示している。804において、キーの残りの寿命が監視される。806において、MSが休止モードの低電力状態にあるとき、いずれかのキーが終了するように設定されているかどうかの決定がなされる。この決定のために、キーの残りの寿命は、低電力状態の予期される期間と比較されることができる。

【００６０】

1つまたは複数のキーが終了するように設定されている場合、MSは、808において早めに休止モードを終了させ、810において、新しいキー（または複数のキー）を交渉することができる。当該終了するキーを更新するために早めに休止モードから抜け出すことは、コールのセットアップにおける遅延という結果となり得る長いキーの交渉を回避することを助けることができる。キーの交渉が完了した後、および終了するキー（複数）が更新された後、MSは、休止モードに再び入ることができる。

【００６１】

上で説明された方法の様々なオペレーションは、図面において例示されている手段および機能ブロックに対応する様々なハードウェアおよび／またはソフトウェアコンポーネント（複数）および／またはモジュール（複数）によって実行されてもよい。一般に、対応する対の片方の手段および機能の図を有する図において例示されている方法があるところにおいて、オペレーションブロックは、同様の番号付けを備える手段および機能ブロックに対応する。例えば、図5において例示されているブロック502ないし516は、図5Aにおいて例示されている手段および機能ブロック502Aないし516Aに対応する。

【００６２】
情報および信号は、様々な異なる技術および技法のうちのいずれかを使用して表わされてもよい。例えば、上記説明全体を通じて参照されることができるデータ、命令、コマンド、情報、信号などは、電圧、電流、電磁波、磁場または磁粒子、光波動場または光粒子、またはこれらのものの任意の組み合わせによって表わされることができる。
【００６３】
本件開示に関連して説明された様々な例示的な論理ブロック、モジュール、および回路は、汎用目的プロセッサ、デジタル信号プロセッサ（DSP）、特定用途集積回路（ASIC）、フィールドプログラマブルゲートアレイ（FPGA）または他のプログラマブル論理デバイス（PLD）、離散的ゲートまたはトランジスタ論理、離散的ハードウェアコンポーネント、またはこれらのものの任意の組み合わせであって、本件明細書記載の機能を実行するように設計されたものによって実装または実行されることができる。汎用目的プロセッサは、マイクロプロセッサであってもよいが、その代わりに、任意の産業上利用可能なプロセッサ、コントローラ、マイクロコントローラ、または状態機械であってもよい。プロセッサは、コンピュータ計算デバイスの組み合わせとして、例えば、DSPとマイクロプロセッサとの組み合わせ、複数のマイクロプロセッサ、DSPコアと結合した1つまたは複数のマイクロプロセッサ、または他の任意の同様の機器構成として、実装されることもできる。
【００６４】
本件開示に関連して説明された方法またはアルゴリズムのステップは、ハードウェア、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、またはその2つの組み合わせにおいて直接具体化されることができる。ソフトウェアモジュールは、当該技術分野において知られている任意の形式の記憶媒体の中に在ることができる。記憶媒体のいくつかの例は、ランダムアクセスメモリ（RAM）、読み出し専用メモリ（ROM）、フラッシュメモリ、EPROMメモリ、EEPROMメモリ、レジスタ、ハードディスク、リムーバルディスク、CD-ROMなどを含んで使用されてもよい。ソフトウェアモジュールは、単一の命令、または多くの命令を具備してもよく、およびいくつかの異なるコードセグメント上、異なるプログラムの間、および複数の記憶媒体にわたって分散されることができる。記憶媒体は、プロセッサが記憶媒体から情報を読み出す、または記憶媒体に情報を書き込むことができるように、プロセッサと結合されていてもよい。そのかわりに、記憶媒体がプロセッサと一体化されていてもよい。
【００６５】
本件明細書において開示された方法は、説明された方法を達成するための1つまたは複数のステップまたは動作を具備する。当該方法、ステップ、および／または動作は、特許請求の範囲から逸脱しない範囲で相互に交換されることができる。言い換えると、ステップまたは動作の固有の順番が明記されない限り、順番および／または固有のステップおよび／または動作の使用は、特許請求の範囲を逸脱しない範囲で修正されることができる。
【００６６】
説明された機能は、ハードウェア、ソフトウェア、ファームウェア、またはこれらのものの任意の組み合わせにおいて実装されることができる。ソフトウェアにおいて実装される場合、当該機能は、命令または1つまたは複数のセットの命令としてコンピュータ可読媒体または記憶媒体上に記憶されることができる。記憶媒体は、コンピュータ、または1つまたは複数の処理デバイスによってアクセスされることができる任意の利用可能な媒体であってもよい。実例として、次のものには制限されないが、そのようなコンピュータ可読媒体は、RAM、ROM、EEPROM、CD-ROMまたは他の光ディスク記憶、磁気ディスク記憶または他の磁気記憶デバイス、または任意の他の媒体であって、コンピュータによってアクセス可能な命令またはデータ構造の形式で所望のプログラムコードを搬送または記憶するために使用されることができる媒体を具備することができる。本件明細書において使用されているようなディスク（diskおよびdisc）は、コンパクトディスク（CD）、レーザディスク、光ディスク、デジタル汎用ディスク（DVD）、フレキシブルディスク、およびブルーレイ（登録商標）ディスクを含む。なお、ディスク（disc）がレーザにより光学的にデー

タを再生するのに対し、ディスク（disk）は、通常磁気的にデータを再生する。

【００６７】

ソフトウェアまたは命令はまた、送信媒体上で送信されてもよい。例えば、ソフトウェアが、同軸ケーブル、光ファイバーケーブル、より対線、デジタル加入者ライン（DSL）、またはワイヤレス技術（例えば、赤外線、無線、および電磁波）を使用して、ウェブサイト、サーバー、または他の遠隔ソースから送信される場合、当該同軸ケーブル、光ファイバーケーブル、より対線、ＤＳＬ、またはワイヤレス技術（例えば、赤外線、無線、および電磁波）は、媒体の定義に含まれる。

【００６８】

さらに、本件明細書記載の方法および技術を実行するためのモジュールおよび／または他の適切な手段は、ダウンロードされることができおよび／またはそうでなければ、適用可能なものとしてユーザ端末および／または基地局によって得られることができることが認識されるべきである。例えば、そのようなデバイスは、本件明細書記載の方法を実行するための手段の送信を容易にするためにサーバーに結合されることができる。代替的に、本件明細書記載の様々な方法は、ユーザ端末および／または基地局がデバイスへの記憶媒体を結合または提供することに基づく様々な方法を得ることができるように記憶手段（例えば、RAM、ROM、コンパクトディスク（CD）またはフレキシブルディスクなどのような物理記憶媒体）によって提供されることができる。さらに、本件明細書記載の方法および技術をデバイスに提供するための任意の他の適切な技術が利用されることができる。

【００６９】

特許請求の範囲は、上で例示された寸分違わない構成およびコンポーネントに制限されないことが理解される。特許請求の範囲から逸脱することの範囲で上に記載された方法および装置のアレンジメント、オペレーション、および詳細において、様々な修正、変更、およびバリエーションがなされることができる。

以下に本件出願当初の特許請求の範囲に記載された発明を付記する。

［１］ワイヤレス通信のためにワイヤレスデバイスによって使用される1つまたは複数のセキュリティキーを維持するための方法であって、

通信イベントがいつ生じるべきかを決定することと、

少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視することと、

前記少なくとも1つのセキュリティキーが終了しそうであると識別される場合、前記通信イベントを遅延させることと、および

終了しそうであると識別された前記少なくとも1つのセキュリティキーを更新することと

を具備する方法。

［２］いずれのセキュリティキーも終了しそうでないと識別されるまで、決定することと、監視することと、遅延させることと、および更新することとの前記ステップを繰り返すことと、および

前記通信イベントを開始することと

をさらに具備する［１］に記載の方法。

［３］前記通信イベントは、ハンドオーバーイベントであり、および

少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視することは、前記少なくとも1つのセキュリティキーの残りの寿命と前記ハンドオーバーイベントの予期される期間とを比較することを含む、［１］に記載の方法。

［４］前記通信イベントは、電力節約モードであり、および

少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視することは、前記少なくとも1つのセキュリティキーの残りの寿命と前記電力節約モードの低電力状

態の期間とを比較することを含む、［１］に記載の方法。
［５］前記電力節約モードは、スリープモードを含む、［４］に記載の方法。
［６］前記電力節約モードは、休止モードを含む、［４］に記載の方法。
［７］前記ワイヤレスデバイスは、IEEE802.16（Institute of Electrical and Electronics
Engineers）ファミリー規格の1つまたは複数の規格に準拠するフレームを使用して通信する、［１］に記載の方法。
［８］ワイヤレス通信のためにワイヤレスデバイスによって使用される1つまたは複数のセキュリティキーを維持するように構成されている装置であって、
通信イベントがいつ生じるべきかを決定するための論理と、
少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視するための論理と、
前記少なくとも1つのセキュリティキーが終了しそうであると識別される場合、前記通信イベントを遅延させるための論理と、および
終了しそうであると識別された前記少なくとも1つのセキュリティキーを更新するための論理と
を具備する装置。
［９］いずれのセキュリティキーも終了しそうでないと識別されるまで、決定するための論理と、監視するための論理と、遅延させるための論理と、および更新するための論理とを繰り返すための論理と、および
前記通信イベントを開始するための論理と
をさらに具備する［８］に記載の装置。
［１０］前記通信イベントは、ハンドオーバーイベントであり、および
少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視するための前記論理は、前記少なくとも1つのセキュリティキーの残りの寿命と前記ハンドオーバーイベントの予期される期間とを比較するための論理を含む、［８］に記載の装置。
［１１］前記通信イベントは、電力節約モードであり、および
少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視するための前記論理は、前記少なくとも1つのセキュリティキーの残りの寿命と前記電力節約モードの低電力状態の期間とを比較するための論理を含む、［８］に記載の装置。
［１２］前記電力節約モードは、スリープモードを含む、［１１］に記載の装置。
［１３］前記電力節約モードは、休止モードを含む、［１１］に記載の装置。
［１４］前記装置は、IEEE802.16（Institute of Electrical and Electronics Engineers）ファミリー規格の1つまたは複数の規格に準拠するフレームを使用して通信するための論理を含む、［８］に記載の装置。
［１５］ワイヤレス通信のためにワイヤレスデバイスによって使用される1つまたは複数のセキュリティキーを維持するための装置であって、
通信イベントがいつ生じるべきかを決定するための手段と、
少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視するための手段と、
前記少なくとも1つのセキュリティキーが終了しそうであると識別される場合、前記通信イベントを遅延させるための手段と、および
終了しそうであると識別された前記少なくとも1つのセキュリティキーを更新するための手段と
を具備する装置。
［１６］いずれのセキュリティキーも終了しそうでないと識別されるまで、決定するため

の手段と、監視するための手段と、遅延させるための手段と、および更新するための手段とを繰り返すための手段と、および
前記通信イベントを開始するための手段と
をさらに具備する［１５］に記載の装置。
［１７］前記通信イベントは、ハンドオーバーイベントであり、および
少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視するための前記手段は、前記少なくとも1つのセキュリティキーの残りの寿命と前記ハンドオーバーイベントの予期される期間とを比較するための手段を含む、［１５］に記載の装置。
［１８］前記通信イベントは、電力節約モードであり、および
少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視するための前記手段は、前記少なくとも1つのセキュリティキーの残りの寿命と前記電力節約モードの低電力状態の期間とを比較するための手段を含む、［１５］に記載の装置。
［１９］前記電力節約モードは、スリープモードを含む、［１８］に記載の装置。
［２０］前記電力節約モードは、休止モードを含む、［１８］に記載の装置。
［２１］前記装置は、IEEE802.16（Institute of Electrical and Electronics Engineers）ファミリー規格の1つまたは複数の規格に準拠するフレームを使用して通信するための論理を含む、［１５］に記載の装置。
［２２］1セットの命令を内蔵するコンピュータ可読媒体を具備する、ワイヤレス通信のためにワイヤレスデバイスによって使用される1つまたは複数のセキュリティキーを維持するためのコンピュータプログラムプロダクトであって、命令の前記セットは、1つまたは複数のプロセッサによって実行され、および命令の前記セットは、
通信イベントがいつ生じるべきかを決定するための命令と、
少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視するための命令と、
前記少なくとも1つのセキュリティキーが終了しそうであると識別される場合、前記通信イベントを遅延させるための命令と、および
終了しそうであると識別された前記少なくとも1つのセキュリティキーを更新するための命令と
を具備する、コンピュータプログラムプロダクト。
［２３］命令の前記セットは、
いずれのセキュリティキーも終了しそうでないと識別されるまで、決定するための命令と、監視するための命令と、遅らせるための命令と、および更新するための命令とを繰り返すための命令と、および
前記通信イベントを開始するための命令と
をさらに具備する、［２２］に記載のコンピュータプログラムプロダクト。
［２４］前記通信イベントは、ハンドオーバーイベントであり、および
少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視するための前記手段は、前記少なくとも1つのセキュリティキーの残りの寿命と前記ハンドオーバーイベントの予期される期間とを比較するための手段を含む、［２２］に記載のコンピュータプログラムプロダクト。
［２５］前記通信イベントは、電力節約モードであり、および
少なくとも1つのセキュリティキーが前記通信イベントの間に終了しそうであるかどうかを識別するために前記1つまたは複数のセキュリティキーの前記寿命を監視するための前記手段は、前記少なくとも1つのセキュリティキーの残りの寿命と前記電力節約モードの低電力状態の期間とを比較するための手段を含む、［２２］に記載のコンピュータプログラムプロダクト。

［２６］前記電力節約モードは、スリープモードを含む、［２５］に記載のコンピュータプログラムプロダクト。
［２７］前記電力節約モードは、休止モードを含む、［２５］に記載のコンピュータプログラムプロダクト。
［２８］前記装置は、IEEE802.16（Institute of Electrical and Electronics Engineers）ファミリー規格の1つまたは複数の規格に準拠するフレームを使用して通信するための命令を含む、［２２］に記載のコンピュータプログラムプロダクト。

【図１】

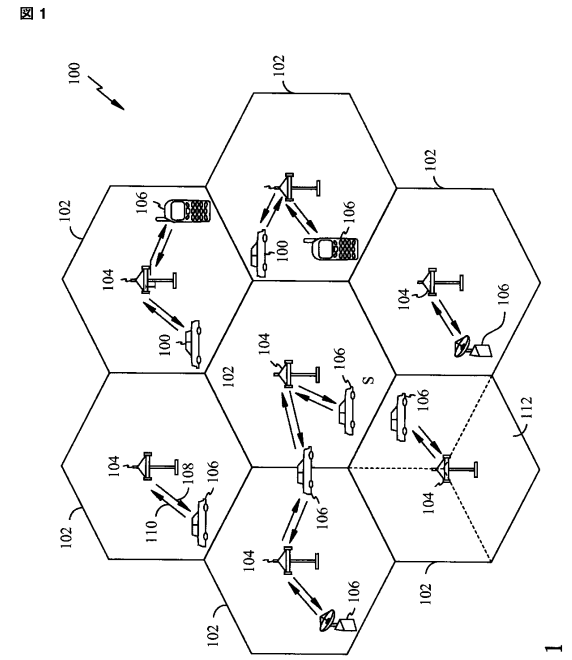

FIG. 1

【図２】

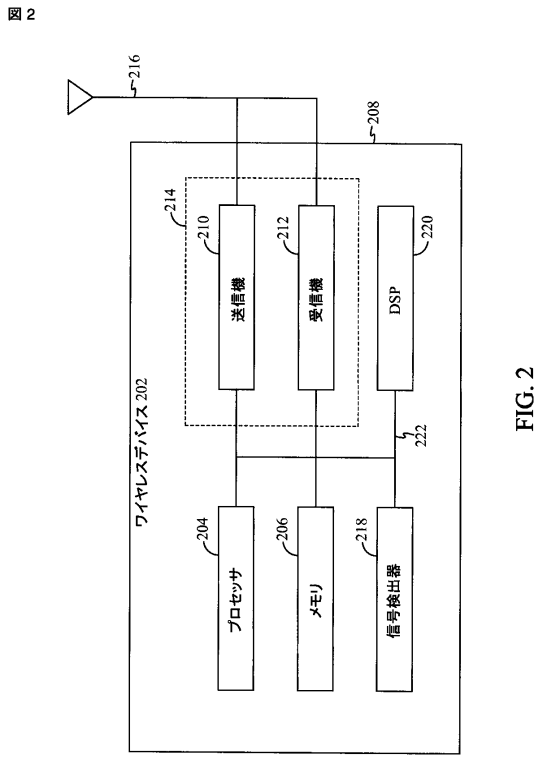

FIG. 2

【図３】

図 3

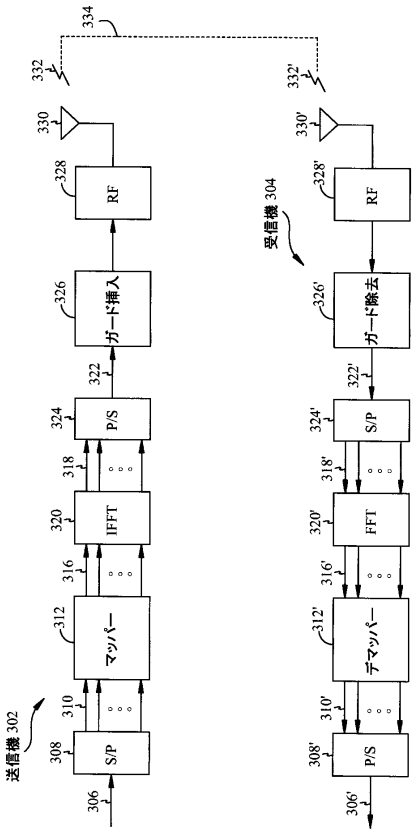

FIG. 3

【図４】

図 4

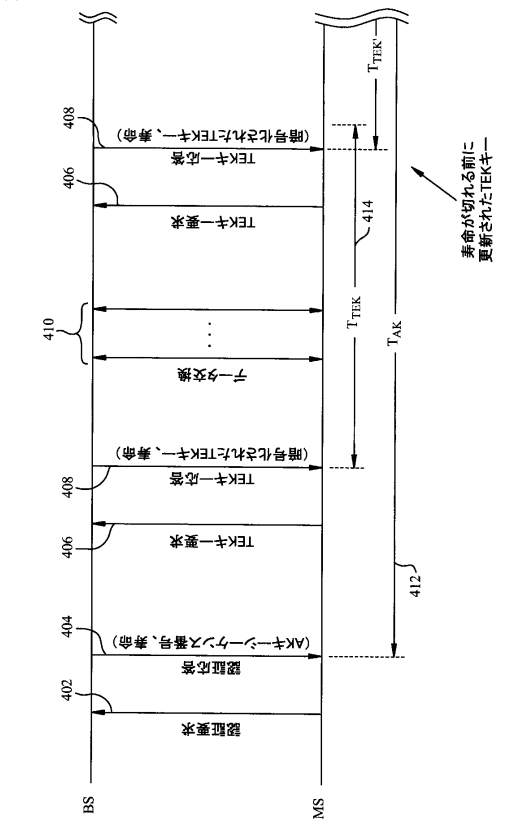

FIG. 4

【図５】

図 5

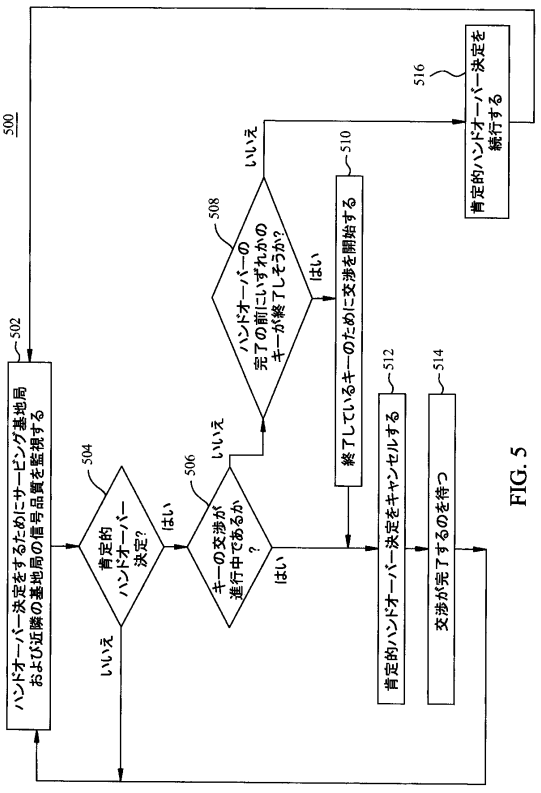

FIG. 5

【図５Ａ】

図 5A

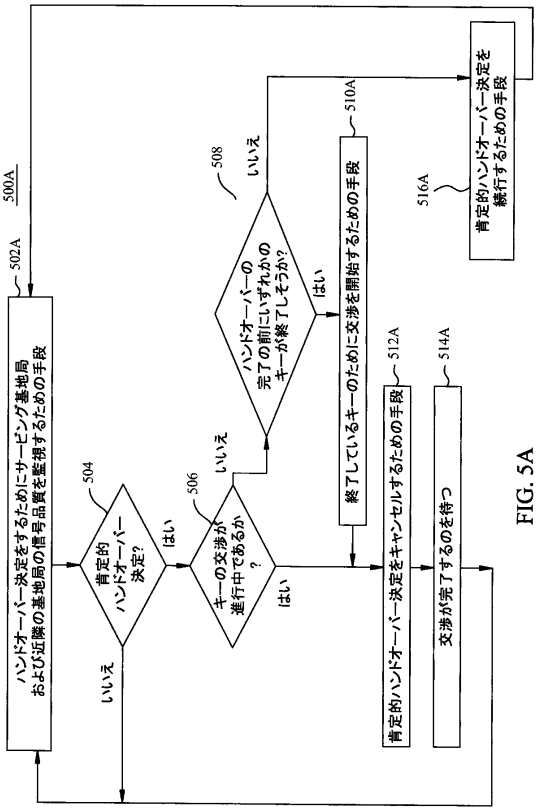

FIG. 5A

【図６Ａ】

図 6A

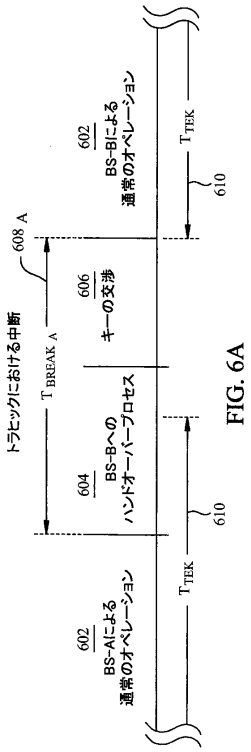

FIG. 6A

【図６Ｂ】

図 6B

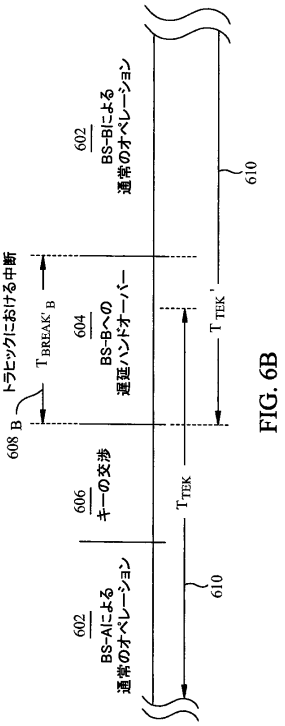

FIG. 6B

【図７】

図 7

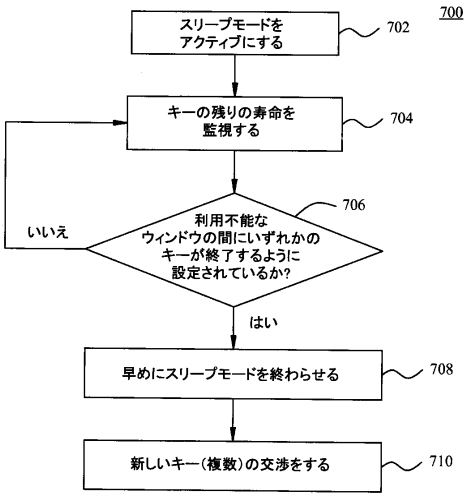

FIG. 7

【図７Ａ】

図 7A

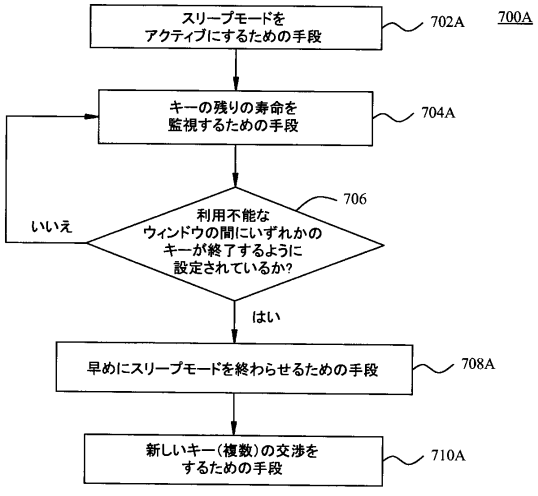

FIG. 7A

【図８】

図 8

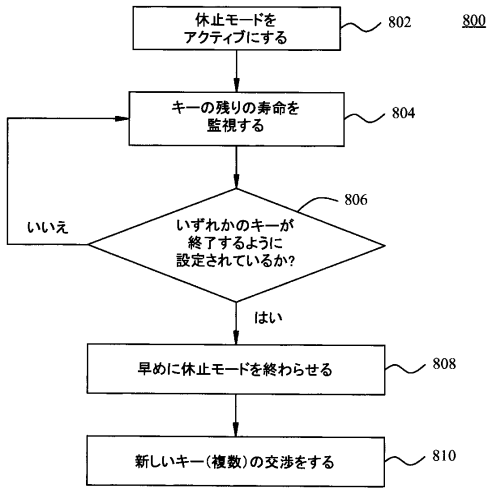

FIG. 8

【図８Ａ】

図 8A

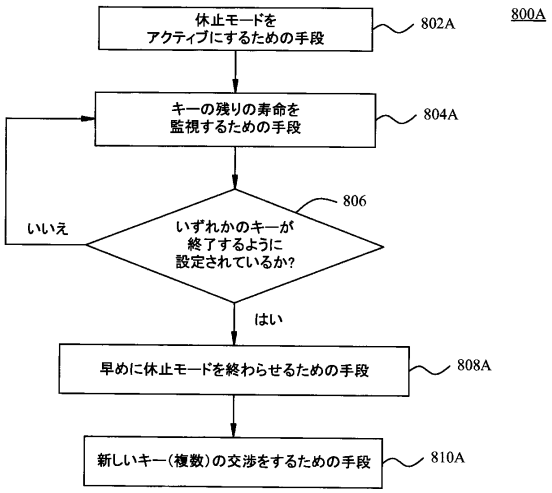

FIG. 8A

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 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 チン、シャン
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
(72)発明者 チン、トム
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

審査官 米倉 明日香

(56)参考文献 国際公開第２００８／００１７２６（WO，Ａ１）
特開２００５－２６０９８７（ＪＰ，Ａ）
特開２００６－６０３３６（ＪＰ，Ａ）
特開２００８－４８０１８（ＪＰ，Ａ）
国際公開第２００５／０８６４１２（WO，Ａ１）
国際公開第２００９／１３６９８１（WO，Ａ１）

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