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

特許第4809433号
(P4809433)

(45)発行日　平成23年11月9日(2011.11.9)　(24)登録日　平成23年8月26日(2011.8.26)

(51)Int.Cl.		F I		
H04W 4/06	(2009.01)	H04Q	7/00	125
H04W 12/10	(2009.01)	H04Q	7/00	185
H04W 68/10	(2009.01)	H04Q	7/00	525
H04M 11/04	(2006.01)	H04M	11/04	
H04M 3/487	(2006.01)	H04M	3/487	

請求項の数 8　(全 16 頁)　最終頁に続く

(21)出願番号　特願2008-522478 (P2008-522478)
(86)(22)出願日　平成19年6月19日 (2007.6.19)
(86)国際出願番号　PCT/JP2007/062346
(87)国際公開番号　WO2007/148701
(87)国際公開日　平成19年12月27日 (2007.12.27)
審査請求日　平成20年12月18日 (2008.12.18)
(31)優先権主張番号　特願2006-169435 (P2006-169435)
(32)優先日　平成18年6月19日 (2006.6.19)
(33)優先権主張国　日本国(JP)

前置審査

(73)特許権者　392026693
株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目１１番１号
(74)代理人　100083806
弁理士　三好　秀和
(72)発明者　北原　亮
東京都千代田区永田町二丁目１１番１号
株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　野口　勝広
東京都千代田区永田町二丁目１１番１号
株式会社エヌ・ティ・ティ・ドコモ内

審査官　松野　吉宏

最終頁に続く

(54)【発明の名称】移動通信システム、移動通信方法、配信サーバ、無線回線制御局及び移動局

(57)【特許請求の範囲】
【請求項１】
同報通信用のトラフィックチャネルを用いて、移動局に対して、配信サーバの公開鍵を送信するように構成されており、
特定の移動局に対して着信情報があることを通知するためのチャネルを用いて、前記移動局に対して、通知情報を送信するように構成されており、
前記同報通信用のトラフィックチャネルを用いて、前記移動局に対して、前記通知情報に対する電子署名を送信するように構成されており、
前記移動局は、受信した前記通知情報に対する電子署名及び前記配信サーバの公開鍵に基づいて、該通知情報の有効性について認証するように構成されていることを特徴とする移動通信システム。
【請求項２】
同報通信用のトラフィックチャネルを用いて、移動局に対して、配信サーバの公開鍵を送信する工程と、
特定の移動局に対して着信情報があることを通知するためのチャネルを用いて、前記移動局に対して、通知情報を送信する工程と、
前記同報通信用のトラフィックチャネルを用いて、前記移動局に対して、前記通知情報に対する電子署名を送信する工程と、
前記移動局が、受信した前記通知情報に対する電子署名及び前記配信サーバの公開鍵に基づいて、該通知情報の有効性について認証する工程とを有することを特徴とする移動通

信方法。
【請求項３】
同報通信用のトラフィックチャネルを用いて、移動局に対して、配信サーバの公開鍵を送信するように構成されている鍵送信部と、
前記無線装置に対して、特定の移動局に対して着信情報があることを通知するためのチャネルを用いて前記移動局に対して送信される通知情報を送信するように構成されている通知情報送信部と、
前記同報通信用のトラフィックチャネルを用いて、前記移動局に対して、前記通知情報に対する電子署名を送信するように構成されている電子署名送信部とを具備することを特徴とする配信サーバ。
【請求項４】
特定の移動局に対して着信情報があることを通知するためのチャネルを用いて、同報通信用のトラフィックチャネルを用いて配信サーバの公開鍵を受信している移動局に対して、該配信サーバから受信した通知情報を送信し、該トラフィックチャネルを用いて、該移動局に対して、該通知情報に対する電子署名を送信するように構成されている送信部を具備することを特徴とする無線回線制御局。
【請求項５】
移動局であって、
同報通信用のトラフィックチャネルを用いて、配信サーバの公開鍵を受信し、該移動局に対して着信情報があることを通知するためのチャネルを用いて、通知情報を受信し、該同報通信用のトラフィックチャネルを用いて、該通知情報に対する電子署名を受信するように構成されている受信部と、
受信した前記通知情報に対する電子署名及び前記配信サーバの公開鍵に基づいて、該通知情報の有効性について認証するように構成されている認証部とを具備することを特徴とする移動局。
【請求項６】
前記認証結果に基づいて、前記通知情報の表示方法を制御するように構成されている表示部を具備することを特徴とする請求項５に記載の移動局。
【請求項７】
前記表示部は、受信した前記通知情報を表示した後、前記認証結果が否定的であった場合、該通知情報が誤りであった旨を表示するように構成されていることを特徴とする請求項６に記載の移動局。
【請求項８】
前記表示部は、前記認証結果が否定的であった場合、受信した前記通知情報を表示しないように構成されていることを特徴とする請求項６に記載の移動局。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、無線装置が、配信サーバから送信された緊急情報を、同報通信を用いて、移動局に対して送信するように構成されている移動通信システム、移動通信方法、配信サーバ、無線回線制御局及び移動局に関する。
【背景技術】
【０００２】
従来、官公庁や地方自治体等によって発せされた地震情報や津波情報等の緊急情報を、ＣＢＳ（Ｃｅｌｌ　Ｂｒｏａｄｃａｓｔ　Ｓｅｒｖｉｃｅ）やＭＢＭＳ（Ｍｕｌｔｉｍｅｄｉａ　Ｂｒｏａｄｃａｓｔ/Ｍｕｌｔｉｃａｓｔ　Ｓｅｒｖｉｃｅ）等の同報通信を用いて移動局に送信するように構成されている緊急情報送信用の移動通信システムが知られている。
【０００３】
具体的には、かかる緊急情報送信用の移動通信システムでは、無線回線制御局ＲＮＣが

、ＣＴＣＨ（Ｃｏｍｍｏｎ　Ｔｒａｆｆｉｃ　Ｃｈａｎｎｅｌ）やＭＴＣＨ（ＭＢＭＳ　Ｔｒａｆｆｉｃ　Ｃｈａｎｎｅｌ）等の同報通信用のトラフィックチャネルを用いて、特定エリアに在圏する移動局に対して、官公庁や地方自治体等の端末から配信サーバを介して受信した上述の緊急情報を送信するように構成されている。

【０００４】

しかしながら、従来の緊急情報送信用の移動通信システムでは、移動局において、同報通信を用いて送信された緊急情報の送信者認証を行うように構成されていないため、不正な無線基地局によって偽造の緊急情報が発信されることによる誤報が発生して緊急情報の送信者の信用が喪失する可能性及び受信者の混乱の可能性があるという問題点があった。

【０００５】

（非特許文献１）

３ＧＰＰ　ＴＳ２３.０４１

（非特許文献２）

３ＧＰＰ　ＴＳ２３.２４６

【発明の開示】

【０００６】

そこで、本発明は、上述の課題に鑑みてなされたものであり、同報通信を用いて緊急情報を移動局に送信する場合に、緊急情報の送信者へのなりすましを防止することを可能とする移動通信システム、移動通信方法、配信サーバ、無線回線制御局及び移動局を提供することを目的とする。

【０００７】

本発明の第１の特徴は、無線装置が、配信サーバから送信された通知情報（緊急情報）を、同報通信を用いて、移動局に対して送信するように構成されている移動通信システムであって、前記配信サーバは、該配信サーバの公開鍵を前記移動局に対して送信するように構成されている鍵送信部を具備し、前記無線装置は、前記配信サーバから送信された前記通知情報を前記移動局に対して送信するように構成されている通知情報送信部を具備し、前記移動局は、受信した前記通知情報に対する電子署名に基づいて、前記通知情報の有効性について認証するように構成されている認証部を具備することを要旨とする。

【０００８】

本発明の第１の特徴において、前記無線装置は、無線回線制御局と無線基地局とを含み、前記通知情報送信部は、前記無線基地局に設けられており、前記無線基地局の前記通知情報送信部は、特定の移動局に対して着信情報があることを通知するためのチャネルを用いて、前記通知情報を送信するように構成されており、前記配信サーバの前記鍵送信部は、同報通信用のトラフィックチャネルを用いて、前記配信サーバの公開鍵を前記移動局に対して送信するように構成されていてもよい。

【０００９】

本発明の第１の特徴において、前記無線装置は、無線回線制御局と無線基地局とを含み、前記通知情報送信部は、前記無線回線制御局に設けられており、前記無線回線制御局の前記通知情報送信部は、特定の移動局に対して着信情報があることを通知するためのチャネルを用いて、前記通知情報を送信するように構成されており、前記配信サーバの前記鍵送信部は、同報通信用のトラフィックチャネルを用いて、前記配信サーバの公開鍵を前記移動局に対して送信するように構成されていてもよい。

【００１０】

本発明の第１の特徴において、前記配信サーバは、前記通知情報に対する電子署名を生成するように構成されている電子署名生成部と、同報通信用のトラフィックチャネルを用いて、生成した前記電子署名を前記移動局に対して送信するように構成されている電子署名送信部とを具備してもよい。

【００１１】

本発明の第１の特徴において、前記配信サーバは、前記通知情報に対する電子署名を生成するように構成されている電子署名生成部と、生成した前記電子署名を前記無線回線制

御局に対して送信するように構成されている電子署名送信部とを具備し、前記無線回線制御局の前記通知情報送信部は、特定の移動局に対して着信情報があることを通知するためのチャネルを用いて、前記通知情報と共に、前記電子署名を、前記移動局に対して送信するように構成されていてもよい。

【００１２】

本発明の第１の特徴において、前記無線回線制御局は、受信した前記通知情報に対する電子署名を生成するように構成されている電子署名生成部を具備し、前記無線回線制御局の前記通知情報送信部は、特定の移動局に対して着信情報があることを通知するためのチャネルを用いて、前記通知情報と共に、前記電子署名を、前記移動局に対して送信するように構成されていてもよい。

【００１３】

本発明の第２の特徴は、無線装置が、配信サーバから送信された通知情報を、同報通信を用いて、移動局に対して送信する移動通信方法であって、前記配信サーバが、該配信サーバの公開鍵を前記移動局に対して送信する工程と、前記無線装置が、前記配信サーバから送信された前記通知情報を前記移動局に対して送信する工程と、前記移動局が、受信した前記通知情報に対する電子署名に基づいて、前記通知情報の有効性について認証する工程とを有することを要旨とする。

【００１４】

本発明の第３の特徴は、同報通信を用いて、無線装置を介して移動局に対して通知情報を送信するように構成されている配信サーバであって、前記配信サーバの公開鍵を前記移動局に対して送信するように構成されている鍵送信部と、前記通知情報を前記無線装置に対して送信するように構成されている通知情報送信部と、前記通知情報に対する電子署名を生成するように構成されている電子署名生成部と、生成した前記電子署名を前記無線装置に対して送信するように構成されている電子署名送信部とを具備することを要旨とする。

【００１５】

本発明の第４の特徴は、配信サーバから送信された通知情報を、同報通信を用いて、移動局に対して送信するように構成されている無線回線制御局であって、特定の移動局に対して着信情報があることを通知するためのチャネルを用いて、前記配信サーバから受信した前記通知情報及び該通知情報に対する電子署名を、前記移動局に対して送信するように構成されている通知情報送信部とを具備することを要旨とする。

【００１６】

本発明の第５の特徴は、配信サーバから送信された通知情報を、同報通信を用いて、移動局に対して送信するように構成されている無線回線制御局であって、前記配信サーバから受信した前記通知情報に対する電子署名を生成するように構成されている電子署名生成部と、特定の移動局に対して着信情報があることを通知するためのチャネルを用いて、前記配信サーバから受信した前記通知情報及び生成された前記電子署名を、前記移動局に対して送信するように構成されている通知情報送信部とを具備することを要旨とする。

【００１７】

本発明の第６の特徴は、同報通信を用いて送信された通知情報を受信するように構成されている移動局であって、前記同報通信を開始するための制御チャネルを介して前記通知情報を受信するように構成されている通知情報受信部と、受信した前記通知情報に対する電子署名に基づいて、前記通知情報の有効性について認証するように構成されている認証部と、前記認証結果に基づいて、前記通知情報の表示方法を制御するように構成されている通知情報表示部とを具備することを要旨とする。

【００１８】

本発明の第６の特徴において、前記同報通信用のトラフィックチャネルを介して前記電子署名を受信するように構成されている電子署名受信部を具備し、前記表示部は、前記制御チャネルを介して受信した前記通知情報を表示した後、前記認証結果が否定的であった場合、前記通知情報が誤りであった旨を表示するように構成されていてもよい。

【００１９】
本発明の第６の特徴において、前記同報通信を開始するための制御チャネルを介して前記電子署名を受信するように構成されている電子署名受信部を具備し、前記表示部は、前記認証結果が否定的であった場合、前記制御チャネルを介して受信した前記通知情報を表示しないように構成されていてもよい。
【図面の簡単な説明】
【００２０】
【図１】図１は、本発明の第１の実施形態に係る移動通信システムの全体構成図である。
【図２】図２は、本発明の第１の実施形態に係る配信サーバの機能ブロック図である。
【図３】図３は、本発明の第１の実施形態に係る無線基地局Ｎｏｄｅ　Ｂの機能ブロック図である。
【図４】図４は、本発明の第１の実施形態に係る移動局ＵＥの機能ブロック図である。
【図５】図５は、本発明の第１の実施形態に係る移動局ＵＥにおける表示画面の一例を示す図である。
【図６】図６は、本発明の第１の実施形態に係る移動通信システムにおいて緊急情報を送信する動作を示すシーケンス図である。
【図７】図７は、本発明の第２の実施形態に係る無線回線制御局ＲＮＣの機能ブロック図である。
【図８】図８は、本発明の第２の実施形態に係る移動通信システムにおいて緊急情報を送信する動作を示すシーケンス図である。
【図９】図９は、本発明の第３の実施形態に係る無線回線制御局ＲＮＣの機能ブロック図である。
【図１０】図１０は、本発明の第３の実施形態に係る無線回線制御局ＲＮＣによって生成されるＰＣＣＨ又はＭＣＣＨの構成の一例を示す図である。
【図１１】図１１は、本発明の第３の実施形態に係る移動通信システムにおいて緊急情報を送信する動作を示すシーケンス図である。
【図１２】図１２は、本発明の第４の実施形態に係る移動通信システムにおいて緊急情報を送信する動作を示すシーケンス図である。
【発明を実施するための最良の形態】
【００２１】
（本発明の第１の実施形態に係る移動通信システム）
図１乃至図５を参照して、本発明の第１の実施形態に係る移動通信システムの構成について説明する。
【００２２】
本実施形態に係る移動通信システムは、無線装置（無線回線制御局ＲＮＣや無線基地局Ｎｏｄｅ　Ｂ）が、配信サーバ１０から送信された通知情報の一種である「緊急情報（官公庁や地方自治体等によって発せされた地震情報や津波情報等）」を、同報通信（ＣＢＳやＭＢＭＳ等）を用いて、移動局ＵＥに対して送信するように構成されている。
【００２３】
具体的には、図１に示すように、本実施形態に係る移動通信システムは、配信サーバと、複数の無線回線制御局ＲＮＣ＃１，＃２と、複数の無線基地局Ｎｏｄｅ　Ｂ＃１１，＃１２と、複数の移動局ＵＥ＃１，＃２とを具備している。
【００２４】
なお、説明の便宜上、図１の例では、無線回線制御局ＲＮＣ、無線基地局Ｎｏｄｅ　Ｂ及び移動局ＵＥについて、２つずつ記載したが、言うまでも無く、本発明は、これらの装置が２つ以上具備している場合の例にも適用可能である。
【００２５】
配信サーバ１０は、ＣＢＣ（Ｃｅｌｌ　Ｂｒｏａｄｃａｓｔ　Ｃｅｎｔｅｒ）又はＢＭ-ＳＣとして機能するものであり、地震や津波等のイベントが発生した場合に、官公庁や地方自治体等によって発せされた地震情報や津波情報等の緊急情報を受信し、かかる緊急

情報を、所定の無線回線制御局ＲＮＣに送信するように構成されている。
【００２６】
具体的には、配信サーバ１０は、鍵更新部１１と、鍵送信部１２と、緊急情報受信部１３と、電子署名生成部１４と、電子署名送信部１５と、緊急情報送信部１６とを具備している。
【００２７】
鍵更新部１１は、所定タイミングで、配信サーバ１０の公開鍵及び秘密鍵を更新するように構成されている。例えば、鍵更新部１１は、緊急情報を配信する度に、配信サーバ１０の公開鍵及び秘密鍵を更新するように構成されていてもよい。
【００２８】
鍵送信部１２は、配信サーバ１０の公開鍵を、移動局ＵＥに対して送信するように構成されている。
【００２９】
具体的には、鍵送信部１２は、ＣＢＳ又はＭＢＭＳ（同報通信）用のトラフィックチャネルである「ＣＴＣＨ（Ｃｏｍｍｏｎ　Ｔｒａｆｆｉｃ　Ｃｈａｎｎｅｌ）」又は「ＭＴＣＨ（ＭＢＭＳ　Ｔｒａｆｆｉｃ　Ｃｈａｎｎｅｌ）」を用いて、配信サーバ１０の公開鍵を、移動局ＵＥに対して送信するように構成されている。
【００３０】
緊急情報受信部１３は、官公庁や地方自治体等から、地震情報や津波情報等の緊急情報の配信要求を受信するように構成されている。ここで、かかる配信要求には、緊急情報及び当該緊急情報の配信エリア（ページングエリア又はＭＢＭＳサービスエリア）が含まれているものとする。
【００３１】
電子署名生成部１４は、配信サーバ１０の秘密鍵を用いて、緊急情報受信部１３により受信された緊急情報に対する電子署名（すなわち、緊急情報の本人性を証明するための電子署名）を生成するように構成されている。
【００３２】
電子署名送信部１５は、電子署名生成部１４により生成された上述の電子署名を、ＣＢＳ又はＭＢＭＳ（同報通信）用のトラフィックチャネル「ＣＴＣＨ」又は「ＭＴＣＨ」を用いて、生成した電子署名を移動局ＵＥに対して送信するように構成されている。
【００３３】
緊急情報送信部１６は、緊急情報受信部１３により受信された緊急情報を、３ＧＰＰＴＳ２５.４１９によって規定されているＳＡＢＰ（Ｓｅｒｖｉｃｅ　Ａｒｅａ　Ｂｒｏａｄｃａｓｔ　Ｐｒｏｔｏｃｏｌ）によって、無線回線制御局ＲＮＣに対して送信するように構成されている。
【００３４】
図３に示すように、無線基地局Ｎｏｄｅ　Ｂは、緊急情報受信部２１と、緊急情報送信部２２とを具備している。
【００３５】
緊急情報受信部２１は、無線回線制御局ＲＮＣを介して、配信サーバ１０から送信された緊急情報を受信するように構成されている。
【００３６】
具体的には、ＰＣＨ受信部３１は、無線回線制御局ＲＮＣから送信された「ＰＣＨ」を受信するように構成されている。
【００３７】
緊急情報送信部２２は、配信サーバ１０から送信された緊急情報を、移動局ＵＥに対して送信するように構成されている。
【００３８】
具体的には、緊急情報送信部２２は、「ＰＩＣＨ（Ｐａｇｉｎｇ　Ｉｎｄｉｃａｔｉｏｎ　Ｃｈａｎｎｅｌ）」又は「ＭＩＣＨ（ＭＢＭＳ　Ｉｎｄｉｃａｔｉｏｎ　Ｃｈａｎｎ

ｅｌ）」（特定の移動局（特定の群に属する移動局）に対して着信情報があることを通知するためのチャネル）を用いて、上述の緊急情報を送信するように構成されている。

【００３９】

図４に示すように、移動局ＵＥは、緊急情報受信部３１と、緊急情報表示部３２と、電子署名受信部３３と、公開鍵受信部３４と、公開鍵記憶部３５と、送信者認証部３６とを具備している。

【００４０】

緊急情報受信部３１は、ＣＢＳ又はＭＢＭＳ（同報通信）を開始するための制御チャネル「ＰＩＣＨ」又は「ＭＩＣＨ」を介して、上述の緊急情報を受信するように構成されている。

【００４１】

電子署名受信部３３は、ＣＢＳ又はＭＢＭＳ（同報通信）用のトラフィックチャネル「ＣＴＣＨ」又は「ＭＴＣＨ」を介して、上述の電子署名を受信するように構成されている。

【００４２】

公開鍵受信部３４は、ＣＢＳ又はＭＢＭＳ（同報通信）用のトラフィックチャネル「ＣＴＣＨ」又は「ＭＴＣＨ」を介して、配信サーバ１０の公開鍵を受信するように構成されている。

【００４３】

公開鍵記憶部３５は、公開鍵受信部３４により受信された配信サーバ１０の公開鍵を記憶するように構成されている。

【００４４】

送信者認証部３６は、電子署名受信部３３により受信された上述の電子署名、及び、公開鍵記憶部３５に記憶されている配信サーバ１０の公開鍵に基づいて、緊急情報表示部３２により表示された緊急情報の有効性について認証するように（すなわち、緊急情報の配信元の本人性について認証するように）構成されている。

【００４５】

緊急情報表示部３２は、緊急情報受信部３１により受信された「ＰＩＣＨ」又は「ＭＩＣＨ」に含まれている緊急情報を表示するように構成されている。

【００４６】

具体的には、緊急情報表示部３２は、図５（ａ）に示すように、表示画面上に簡易情報を表示するように構成されていてもよいし、アラームや振動によって簡易情報を受信した旨を通知するように構成されていてもよい。

【００４７】

また、緊急情報表示部３２は、送信者認証部３６による認証結果に基づいて、緊急情報の表示方法を制御するように構成されている。

【００４８】

具体的には、緊急情報表示部３２は、「ＰＩＣＨ」又は「ＭＩＣＨ」を介して受信した緊急情報を表示した後、上述の認証結果が否定的であった場合（すなわち、緊急情報の配信元の本人性が認められなかった場合）、図６（ｂ）に示すように、上述の緊急情報が誤りであった旨を表示するように構成されている。

【００４９】

（本発明の第１の実施形態に係る移動通信システムの動作）

以下、図６を参照して、本実施形態に係る移動通信システムの動作について説明する。

【００５０】

図６に示すように、ステップＳ１０００において、配信サーバ１０は、ＣＢＳ又はＭＢＭＳ用のトラフィックチャネルである「ＣＴＣＨ」又は「ＭＴＣＨ」を用いて、配信サーバ１０の公開鍵を、移動局ＵＥに送信する。

【００５１】

ステップＳ１００１において、配信サーバ１０は、官公庁や地方自治体等から、地震情

報や津波情報等の緊急情報の配信要求を受信すると、かかる配信要求に含まれている配信エリアに対応する無線回線制御局ＲＮＣに対して、緊急情報を送信する。

【００５２】

ステップＳ１００２において、無線回線制御局ＲＮＣは、受信した緊急情報を、無線基地局Ｎｏｄｅ　Ｂに送信する。

【００５３】

ステップＳ１００３において、無線基地局Ｎｏｄｅ　Ｂは、「ＰＩＣＨ」又は「ＭＩＣＨ」を用いて、移動局ＵＥに対して、上述の緊急情報を送信する。

【００５４】

ステップＳ１００４において、移動局ＵＥは、図５（ａ）に示すように、無線基地局Ｎｏｄｅ　Ｂから送信された「ＰＩＣＨ」又は「ＭＩＣＨ」に含まれている緊急情報を表示する。

【００５５】

例えば、移動局ＵＥは、「ＰＩＣＨ」又は「ＭＩＣＨ」における所定の１２ビット中の下位４ビットに「０１０１」と設定されている場合「地震の発生」を通知するための緊急情報を表示し、かかる１２ビット中の下位４ビットに「１０１０」と設定されている場合「洪水の発生」を通知するための緊急情報を表示するように構成されていてもよい。

【００５６】

ステップＳ１００５において、ＣＢＳ又はＭＢＭＳ（同報通信）を開始するための処理が行われる。

【００５７】

ステップＳ１００６において、上述の処理が完了した後、配信サーバ１０は、配信サーバ１０の公開鍵を用いて、上述の緊急情報に対する電子署名を生成して、ＣＢＳ又はＭＢＭＳ（同報通信）用のトラフィックチャネル「ＣＴＣＨ」又は「ＭＴＣＨ」を用いて、生成した電子署名を移動局ＵＥに対して送信する。

【００５８】

ステップＳ１００７において、移動局ＵＥは、受信した電子署名、及び、公開鍵記憶部３５に記憶されている配信サーバ１０の公開鍵に基づいて、ステップＳ１００４において表示された緊急情報の有効性について認証する。

【００５９】

かかる認証結果が否定的であった場合、移動局ＵＥは、図６（ｂ）に示すように、上述の緊急情報が誤りであった旨を表示する。

【００６０】

配信サーバ１０は、ステップＳ１００８において、配信サーバ１０の公開鍵及び秘密鍵を更新し、ステップＳ１００９において、ＣＢＳ又はＭＢＭＳ用のトラフィックチャネルである「ＣＴＣＨ」又は「ＭＴＣＨ」を用いて、配信サーバ１０の公開鍵を、移動局ＵＥに送信する。

【００６１】

（本発明の第１の実施形態に係る移動通信システムの作用・効果）

本実施形態に係る移動通信システムによれば、移動局ＵＥは、「ＰＩＣＨ」又は「ＭＩＣＨ」を用いて送信された緊急情報を表示した後、「ＣＴＣＨ」又は「ＭＴＣＨ」を用いて送信された当該緊急情報に対する電子署名を用いて当該緊急情報の有効性を認証するため、当該緊急情報の移動局ＵＥに対する到達遅延を短くすると共に、当該緊急情報の送信者へのなりすましを防止することができる。

【００６２】

（本発明の第２の実施形態に係る移動通信システム）

図７及び図８を参照して、本発明の第２の実施形態に係る移動通信システムについて説明する。以下、本実施形態に係る移動通信システムについて、上述の第１の実施形態に係る移動通信システムとの相違点に着目して説明する。

【００６３】

図７に示すように、無線回線制御局ＲＮＣは、緊急情報受信部４１と、緊急情報送信部４２とを具備している。

【００６４】

緊急情報受信部４１は、配信サーバ１０から送信された緊急情報を受信するように構成されている。

【００６５】

緊急情報送信部４２は、配信サーバ１０から送信された緊急情報を、移動局ＵＥに対して送信するように構成されている。

【００６６】

具体的には、緊急情報送信部４２は、「ＰＣＣＨ（Ｐａｇｉｎｇ Ｃｏｎｔｒｏｌ Ｃｈａｎｎｅｌ）」又は「ＭＩＣＨ（ＭＢＭＳ Ｃｏｎｔｒｏｌ Ｃｈａｎｎｅｌ）」（特定の移動局に対して着信情報があることを通知するためのチャネル）を用いて、上述の緊急情報を送信するように構成されている。

【００６７】

以下、図８を参照して、本実施形態に係る移動通信システムの動作について説明する。

【００６８】

図８に示すように、ステップＳ２０００において、配信サーバ１０は、ＣＢＳ又はＭＢＭＳ用のトラフィックチャネルである「ＣＴＣＨ」又は「ＭＴＣＨ」を用いて、配信サーバ１０の公開鍵を、移動局ＵＥに送信する。

【００６９】

ステップＳ２００１において、配信サーバ１０は、官公庁や地方自治体等から、地震情報や津波情報等の緊急情報の配信要求を受信すると、かかる配信要求に含まれている配信エリアに対応する無線回線制御局ＲＮＣに対して、緊急情報を送信する。

【００７０】

ステップＳ２００２において、無線回線制御局ＲＮＣは、受信した緊急情報を、「ＰＣＣＨ」又は「ＭＣＣＨ」を用いて、移動局ＵＥに対して送信する。

【００７１】

ステップＳ２００３において、移動局ＵＥは、図５（ａ）に示すように、無線回線制御局ＲＮＣから送信された「ＰＣＣＨ」又は「ＭＣＣＨ」に含まれている緊急情報を表示する。

【００７２】

例えば、移動局ＵＥは、「ＰＣＣＨ」又は「ＭＣＣＨ」における「ペイロード部（２４０ビット）（３ＧＰＰ ＴＳ３４.１０８参照）」に挿入されている緊急情報を受信した旨を表示するように構成されていてもよい。

【００７３】

ステップＳ２００４乃至ステップＳ２００８の動作については、上述のステップＳ１００５乃至Ｓ１００９の動作と同一である。

【００７４】

本実施形態に係る移動通信システムによれば、移動局ＵＥは、「ＰＣＣＨ」又は「ＭＣＣＨ」を用いて送信された緊急情報を表示した後、「ＣＴＣＨ」又は「ＭＴＣＨ」を用いて送信された当該緊急情報に対する電子署名を用いて当該緊急情報の有効性を認証するため、当該緊急情報の移動局ＵＥに対する到達遅延を短くすると共に、当該緊急情報の送信者へのなりすましを防止することができる。

【００７５】

（本発明の第３の実施形態に係る移動通信システム）

図９乃至図１１を参照して、本発明の第３の実施形態に係る移動通信システムについて説明する。以下、本実施形態に係る移動通信システムについて、上述の第１の実施形態に係る移動通信システムとの相違点に着目して説明する。

【００７６】

図９に示すように、無線回線制御局ＲＮＣは、緊急情報受信部４１と、緊急情報送信部

４２Ａと、秘密鍵受信部４３と、秘密鍵記憶部４４と、電子署名生成部４５とを具備している。

【００７７】

秘密鍵受信部４３は、配信サーバ１０から送信された配信サーバ１０の秘密鍵を受信するように構成されている。

【００７８】

秘密鍵記憶部４４は、秘密鍵受信部４３により受信された配信サーバ１０の秘密鍵を記憶するように構成されている。

【００７９】

電子署名生成部４５は、緊急情報受信部４１により受信された緊急情報、及び、秘密鍵記憶部４４に記憶されている配信サーバ１０の秘密鍵を用いて、当該緊急情報に対する電子署名を生成するように構成されている。

【００８０】

緊急情報送信部４２Ａは、「ＰＣＣＨ」又は「ＭＣＣＨ」を用いて、上述の緊急情報と共に、電子署名生成部４５により生成された電子署名を、移動局ＵＥに対して送信するように構成されている。

【００８１】

具体的には、緊急情報送信部４２Ａは、図１０（ａ）に示すように、「ＰＣＣＨ」又は「ＭＣＣＨ」における「ペイロード部（２４０ビット）」に対して、緊急情報を示す任意の文字列と、当該緊急情報に対する電子署名とを挿入するように構成されていてもよい。

【００８２】

また、緊急情報送信部４２Ａは、図１０（ｂ）に示すように、「ＰＣＣＨ」又は「ＭＣＣＨ」における「ペイロード部（２４０ビット）」に対して、緊急情報に対応するビットパターン（例えば、上述の「０１０１」や「１０１０」等）と、当該緊急情報に対する電子署名とを挿入するように構成されていてもよい。

【００８３】

以下、図１１を参照して、本実施形態に係る移動通信システムの動作について説明する。

【００８４】

図１１に示すように、ステップＳ３０００Ａにおいて、配信サーバ１０は、ＣＢＳ又はＭＢＭＳ用のトラフィックチャネルである「ＣＴＣＨ」又は「ＭＴＣＨ」を用いて、配信サーバ１０の公開鍵を、移動局ＵＥに送信する。

【００８５】

ステップＳ３０００Ｂにおいて、配信サーバ１０は、配信サーバ１０の秘密鍵を、無線回線制御局ＲＮＣに送信する。

【００８６】

ステップＳ３００１において、配信サーバ１０は、官公庁や地方自治体等から、地震情報や津波情報等の緊急情報の配信要求を受信すると、かかる配信要求に含まれている配信エリアに対応する無線回線制御局ＲＮＣに対して、緊急情報を送信する。

【００８７】

ステップＳ３００２において、無線回線制御局ＲＮＣは、受信した緊急情報、及び、秘密鍵記憶部４４に記憶されている配信サーバ１０の秘密鍵を用いて、当該緊急情報に対する電子署名を生成する。

【００８８】

ステップＳ３００３において、無線回線制御局ＲＮＣは、受信した緊急情報及び生成した電子署名を、「ＰＣＣＨ」又は「ＭＣＣＨ」を用いて、移動局ＵＥに対して送信する。

【００８９】

ステップＳ３００４において、移動局ＵＥは、受信した電子署名、及び、公開鍵記憶部３５に記憶されている配信サーバ１０の公開鍵に基づいて、当該緊急情報の有効性について認証する。

【００９０】
かかる認証結果が肯定的であった場合、移動局ＵＥは、受信した緊急情報を表示する。一方、かかる認証結果が否定的であった場合、移動局ＵＥは、上述の緊急情報が誤りであると判断して、かかる緊急情報を表示しない。
【００９１】
例えば、移動局ＵＥは、「ＰＣＣＨ」又は「ＭＣＣＨ」における所定の１２ビット中の下位４ビットに「０１０１」と設定されている場合「地震の発生」を通知するための緊急情報を表示し、かかる１２ビット中の下位４ビットに「１０１０」と設定されている場合「洪水の発生」を通知するための緊急情報を表示するように構成されていてもよい。
【００９２】
ステップＳ３００５において、ＣＢＳ又はＭＢＭＳ（同報通信）を開始するための処理が行われる。
【００９３】
配信サーバ１０は、ステップＳ３００６において、配信サーバ１０の公開鍵及び秘密鍵を更新し、ステップＳ３００７において、ＣＢＳ又はＭＢＭＳ用のトラフィックチャネルである「ＣＴＣＨ」又は「ＭＴＣＨ」を用いて、配信サーバ１０の公開鍵を、移動局ＵＥに送信し、ステップＳ３００８において、配信サーバ１０の秘密鍵を、無線回線制御局ＲＮＣに送信する。
【００９４】
（本発明の第４の実施形態に係る移動通信システム）
図１２を参照して、本発明の第３の実施形態に係る移動通信システムについて説明する。以下、本実施形態に係る移動通信システムについて、上述の第１の実施形態に係る移動通信システムとの相違点に着目して説明する。
【００９５】
以下、図１２を参照して、本実施形態に係る移動通信システムの動作について説明する。
【００９６】
図１２に示すように、ステップＳ４０００において、配信サーバ１０は、ＣＢＳ又はＭＢＭＳ用のトラフィックチャネルである「ＣＴＣＨ」又は「ＭＴＣＨ」を用いて、配信サーバ１０の公開鍵を、移動局ＵＥに送信する。
【００９７】
ステップＳ４００１において、配信サーバ１０は、官公庁や地方自治体等から、地震情報や津波情報等の緊急情報の配信要求を受信し、受信した配信要求に含まれる緊急情報、及び、配信サーバ１０の秘密鍵を用いて、当該緊急情報に対する電子署名を生成する。
【００９８】
ステップＳ４００２において、かかる配信要求に含まれている配信エリアに対応する無線回線制御局ＲＮＣに対して、緊急情報及び当該緊急情報に対する電子署名を送信する。
【００９９】
ステップＳ４００３において、無線回線制御局ＲＮＣは、受信した緊急情報及び電子署名を、「ＰＣＣＨ」又は「ＭＣＣＨ」を用いて、移動局ＵＥに対して送信する。
【０１００】
ステップＳ４００４において、移動局ＵＥは、受信した電子署名、及び、公開鍵記憶部３５に記憶されている配信サーバ１０の公開鍵に基づいて、当該緊急情報の有効性について認証する。
【０１０１】
かかる認証結果が肯定的であった場合、移動局ＵＥは、受信した緊急情報を表示する。一方、かかる認証結果が否定的であった場合、移動局ＵＥは、上述の緊急情報が誤りであると判断して、かかる緊急情報を表示しない。
【０１０２】
例えば、移動局ＵＥは、「ＰＣＣＨ」又は「ＭＣＣＨ」における所定の１２ビット中の

下位４ビットに「０１０１」と設定されている場合「地震の発生」を通知するための緊急情報を表示し、かかる１２ビット中の下位４ビットに「１０１０」と設定されている場合「洪水の発生」を通知するための緊急情報を表示するように構成されていてもよい。

【０１０３】

ステップＳ４００５において、ＣＢＳ又はＭＢＭＳ（同報通信）を開始するための処理が行われる。

【０１０４】

配信サーバ１０は、ステップＳ４００６において、配信サーバ１０の公開鍵及び秘密鍵を更新し、ステップＳ４００７において、ＣＢＳ又はＭＢＭＳ用のトラフィックチャネルである「ＣＴＣＨ」又は「ＭＴＣＨ」を用いて、配信サーバ１０の公開鍵を、移動局ＵＥに送信する。

【０１０５】

なお、日本国特許出願第２００６-１６９４３５号（２００６年6月１９日出願）の全内容が、参照により、本願明細書に組み込まれている。

【０１０６】

また、「３ＧＰＰ　ＴＳ２３.０４１」及び「３ＧＰＰ　ＴＳ２３.２４６」の全内容が、参照により、本願明細書に組み込まれている。

【０１０７】

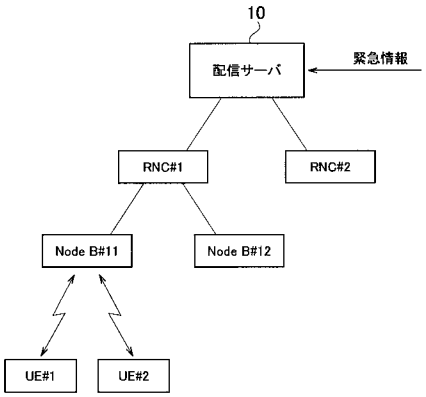
以上、上述の実施形態を用いて本発明について詳細に説明したが、当業者にとっては、本発明が本明細書中に説明した実施形態に限定されるものではないということは明らかである。本発明は、特許請求の範囲の記載により定まる本発明の趣旨及び範囲を逸脱することなく修正及び変更態様として実施することができる。従って、本明細書の記載は、例示説明を目的とするものであり、本発明に対して何ら制限的な意味を有するものではない。

【産業上の利用の可能性】

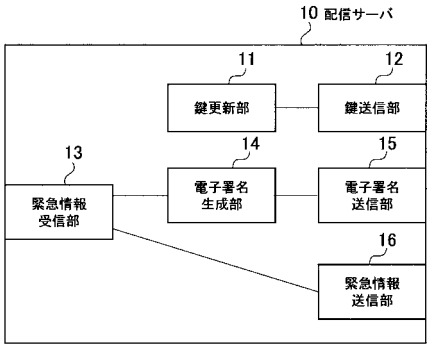
【０１０８】

以上説明したように、本発明によれば、同報通信を用いて緊急情報を移動局に送信する場合に、緊急情報の送信者へのなりすましを防止することを可能とする移動通信システム、移動通信方法、配信サーバ、無線回線制御局及び移動局を提供することができる。

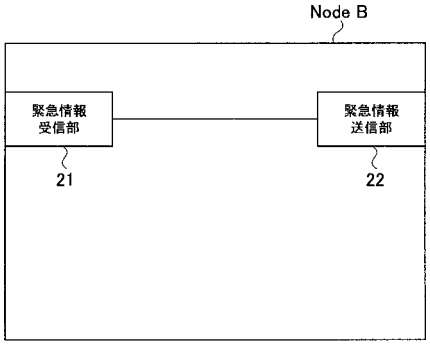
【図１】



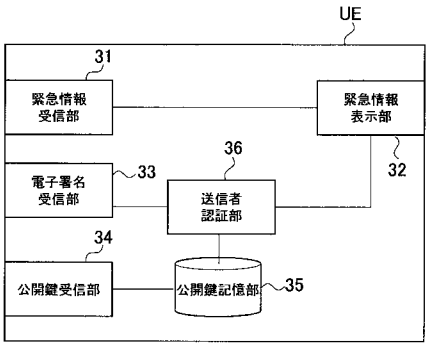
【図２】



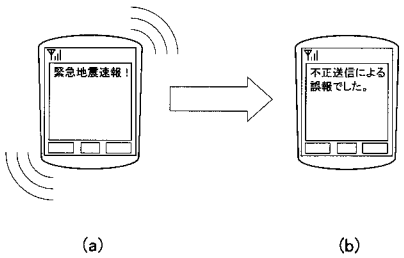
【図３】



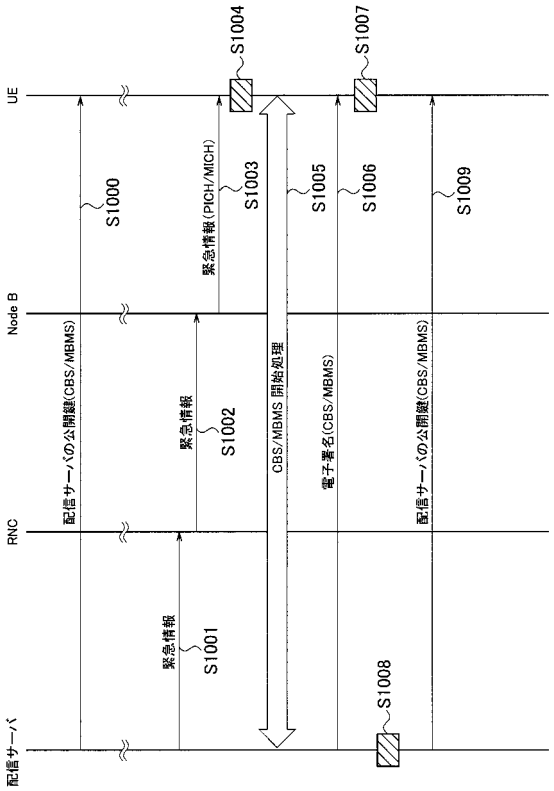
【図４】



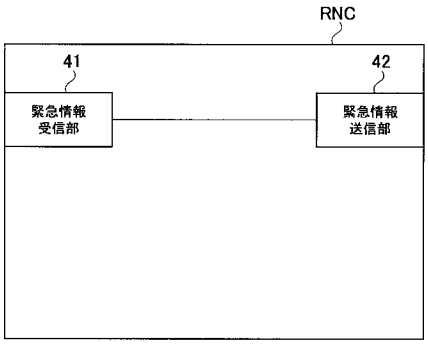
【図５】



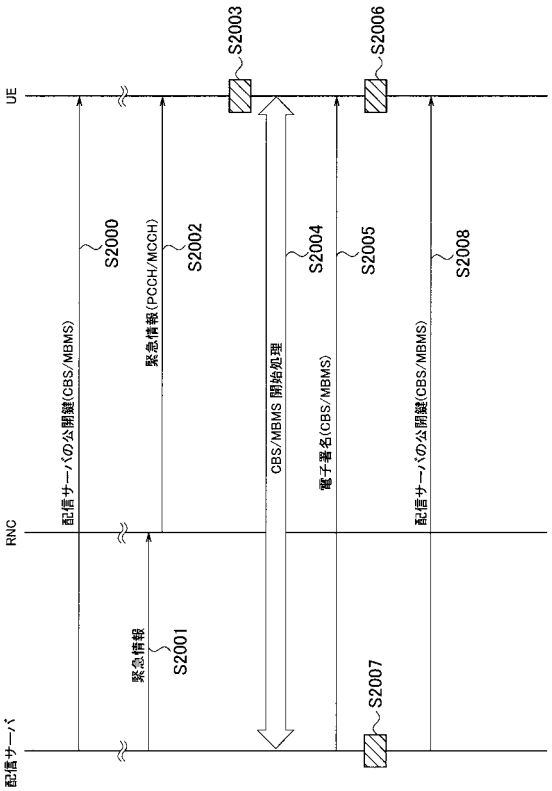
【図６】



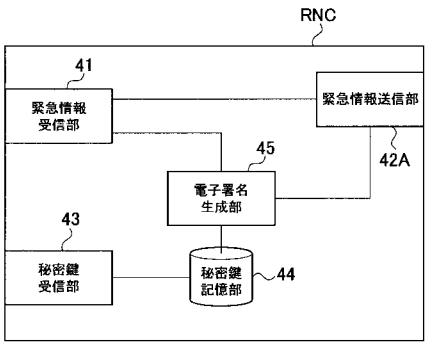
【図７】


RNC
41
緊急情報
受信部
42
緊急情報
送信部

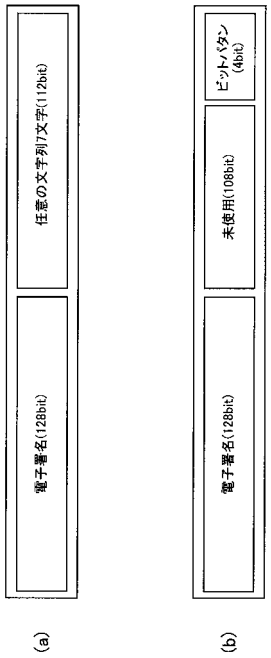
【図８】


UE
RNC
配信サーバ
S2000
配信サーバの公開鍵(CBS/MBMS)
S2001
緊急情報
S2002
緊急情報(PCCH/MCCH)
S2003
CBS/MBMS 開始処理
S2004
電子署名(CBS/MBMS)
S2005
S2006
S2007
S2008
配信サーバの公開鍵(CBS/MBMS)

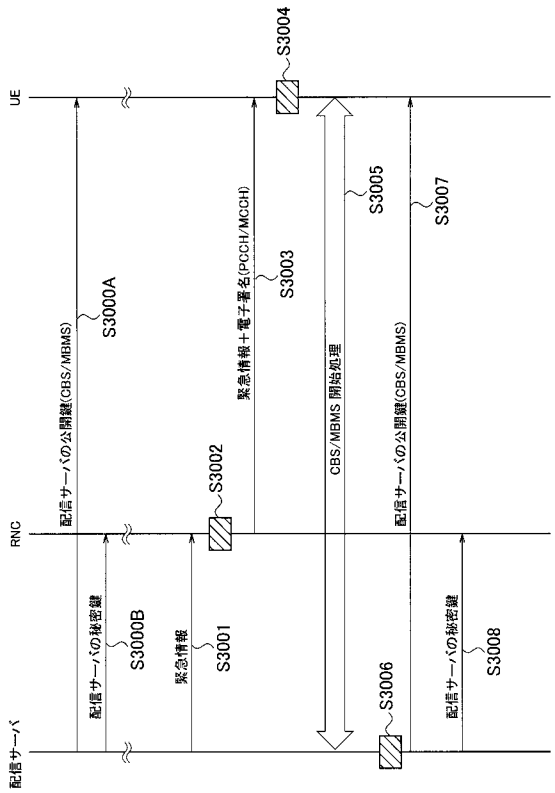
【図９】


RNC
41
緊急情報
受信部
緊急情報送信部
42A
45
電子署名
生成部
43
秘密鍵
受信部
秘密鍵
記憶部
44

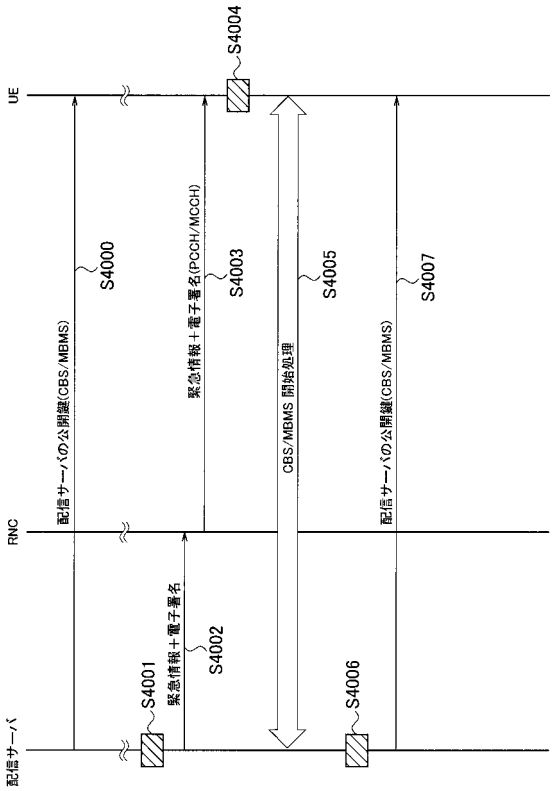
【図１０】


任意の文字列(112bit)
電子署名(128bit)
(a)
ビットパターン
(4bit)
未使用(108bit)
電子署名(128bit)
(b)

【図１１】


UE
RNC
配信サーバ
S3004
S3000A
配信サーバの公開鍵(CBS/MBMS)
S3003
緊急情報＋電子署名(PCCH/MCCH)
S3005
CBS/MBMS 開始処理
S3007
配信サーバの公開鍵(CBS/MBMS)
S3002
S3000B
配信サーバの秘密鍵
S3001
緊急情報
S3006
S3008
配信サーバの秘密鍵

【図１２】


UE
RNC
配信サーバ
S4004
S4000
配信サーバの公開鍵(CBS/MBMS)
S4003
緊急情報＋電子署名(PCCH/MCCH)
S4005
CBS/MBMS 開始処理
S4007
配信サーバの公開鍵(CBS/MBMS)
S4001
緊急情報＋電子署名
S4002
S4006

フロントページの続き

(51)Int.Cl.			FI		
H04L	***9/32***	***(2006.01)***	H04L	9/00	675B
H04L	***9/08***	***(2006.01)***	H04L	9/00	601F

(56)参考文献 特開２００３－３１８８８６（ＪＰ，Ａ）
特開２０００－２４４９７６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04B 7/24 - 7/26
H04W 4/00 - 99/00
H04L 9/08
H04L 9/32
H04M 3/487
H04M 11/04