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

特許第4826834号
(P4826834)

(45)発行日　平成23年11月30日(2011.11.30)　(24)登録日　平成23年9月22日(2011.9.22)

| (51)Int.Cl. | | F I | | |
|---|---|---|---|---|
| H04W 24/04 | (2009.01) | H04Q | 7/00 | 242 |
| H04W 80/04 | (2009.01) | H04Q | 7/00 | 602 |
| H04W 12/00 | (2009.01) | H04Q | 7/00 | 180 |
| H04W 8/26 | (2009.01) | H04Q | 7/00 | 160 |

請求項の数 12　(全 12 頁)

(21)出願番号　特願2008-204498(P2008-204498)
(22)出願日　平成20年8月7日(2008.8.7)
(65)公開番号　特開2010-41592(P2010-41592A)
(43)公開日　平成22年2月18日(2010.2.18)
審査請求日　平成20年8月7日(2008.8.7)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100123788
弁理士　宮崎　昭夫
(74)代理人　100106138
弁理士　石橋　政幸
(74)代理人　100127454
弁理士　緒方　雅昭
(72)発明者　前佛　創
東京都港区芝五丁目７番１号　日本電気株式会社内

審査官　桑江　晃

最終頁に続く

(54)【発明の名称】通信システム、接続装置、情報通知方法、プログラム

(57)【特許請求の範囲】
【請求項１】
端末と、前記端末の移動を管理するサーバ装置と、前記端末を前記サーバ装置と接続する接続装置と、を有してなる通信システムであって、
前記接続装置は、
前記端末のＭＡＣ（Media Access Control）アドレスを記録するとともに、前記端末に対する保守機能の実行要否を表す保守機能実行要否情報を該端末のＭＡＣアドレスと対応付けて記録し、
前記端末のＭＡＣアドレスと対応付けられた保守機能実行要否情報を含むメッセージを、Ｍｏｂｉｌｅ　ＩＰ（Internet Protocol）を用いて前記サーバ装置に送信する、通信システム。
【請求項２】
前記メッセージはＲｅｇｉｓｔｒａｔｉｏｎ　Ｒｅｑｕｅｓｔメッセージである、請求項１に記載の通信システム。
【請求項３】
前記接続装置は、
前記Ｒｅｇｉｓｔｒａｔｉｏｎ　ＲｅｑｕｅｓｔメッセージにＥｘｔｅｎｓｉｏｎフィールドを追加し、該Ｅｘｔｅｎｓｉｏｎフィールドに前記保守機能実行要否情報を含める、請求項２に記載の通信システム。
【請求項４】

端末を、該端末の移動を管理するサーバ装置と接続する接続装置であって、
前記端末のＭＡＣアドレスを記録するとともに、前記端末に対する保守機能の実行要否を表す保守機能実行要否情報を該端末のＭＡＣアドレスと対応付けて記録する記録部と、
前記端末のＭＡＣアドレスと対応付けられた保守機能実行要否情報をメッセージに含める制御部と、
前記メッセージを、Ｍｏｂｉｌｅ　ＩＰを用いて前記サーバ装置に送信する送信部と、を有する接続装置。
【請求項５】
前記メッセージはＲｅｇｉｓｔｒａｔｉｏｎ　Ｒｅｑｕｅｓｔメッセージである、請求項４に記載の接続装置。
【請求項６】
前記制御部は、
前記Ｒｅｇｉｓｔｒａｔｉｏｎ　ＲｅｑｕｅｓｔメッセージにＥｘｔｅｎｓｉｏｎフィールドを追加し、該Ｅｘｔｅｎｓｉｏｎフィールドに前記保守機能実行要否情報を含める、請求項５に記載の接続装置。
【請求項７】
端末を、該端末の移動を管理するサーバ装置と接続する接続装置による情報通知方法であって、
前記端末のＭＡＣアドレスを記録するとともに、前記端末に対する保守機能の実行要否を表す保守機能実行要否情報を該端末のＭＡＣアドレスと対応付けて記録する記録ステップと、
前記端末のＭＡＣアドレスと対応付けられた保守機能実行要否情報をメッセージに含める制御ステップと、
前記メッセージを、Ｍｏｂｉｌｅ　ＩＰを用いて前記サーバ装置に送信する送信ステップと、を有する情報通知方法。
【請求項８】
前記メッセージはＲｅｇｉｓｔｒａｔｉｏｎ　Ｒｅｑｕｅｓｔメッセージである、請求項７に記載の情報通知方法。
【請求項９】
前記制御ステップでは、
前記Ｒｅｇｉｓｔｒａｔｉｏｎ　ＲｅｑｕｅｓｔメッセージにＥｘｔｅｎｓｉｏｎフィールドを追加し、該Ｅｘｔｅｎｓｉｏｎフィールドに前記保守機能実行要否情報を含める、請求項８に記載の情報通知方法。
【請求項１０】
端末を、該端末の移動を管理するサーバ装置と接続する接続装置に、
前記端末のＭＡＣアドレスを記録するとともに、前記端末に対する保守機能の実行要否を表す保守機能実行要否情報を該端末のＭＡＣアドレスと対応付けて記録する記録手順と、
前記端末のＭＡＣアドレスと対応付けられた保守機能実行要否情報をメッセージに含める制御手順と、
前記メッセージを、Ｍｏｂｉｌｅ　ＩＰを用いて前記サーバ装置に送信する送信手順と、を実行させるプログラム。
【請求項１１】
前記メッセージはＲｅｇｉｓｔｒａｔｉｏｎ　Ｒｅｑｕｅｓｔメッセージである、請求項１０に記載のプログラム。
【請求項１２】
前記制御手順では、
前記Ｒｅｇｉｓｔｒａｔｉｏｎ　ＲｅｑｕｅｓｔメッセージにＥｘｔｅｎｓｉｏｎフィールドを追加し、該Ｅｘｔｅｎｓｉｏｎフィールドに前記保守機能実行要否情報を含める、請求項１１に記載のプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信システム、接続装置、情報通知方法、プログラムに関する。
【背景技術】
【０００２】
ＷｉＭＡＸ（Worldwide Interoperability for Microwave Access）　Ｆｏｒｕｍで策定されたＳｐｅｃには、図３に示すような無線通信システムが規定されている。
【０００３】
図３に示すように、ＷｉＭＡＸの無線通信システムは、ＭＳ（Mobile Station）１０と、ＡＳＮ（Access Service Network）内に配置されたＢＳ（Base Station）２０およびＡＳＮ－ＧＷ（ASN-Gateway）３０と、ＣＳＮ（Connectivity Service Network）内に配置されたＨＡ（Home Agent）４０およびＡＡＡ（Authentication, Authorization, Accounting）サーバ５０と、を有している（例えば、特許文献１，２参照）。
【０００４】
ＢＳ２０は、端末であるＭＳ１０と無線通信を行う基地局であり、ＡＳＮ－ＧＷ３０は、ＭＳ１０をＢＳ２０を介してＣＳＮと接続する接続装置である。
【０００５】
ＨＡ４０は、ＭＳ１０の移動を管理するサーバ装置であり、ＡＡＡサーバ５０は、ＭＳ１０に対する認証、許可、および課金を行うサーバ装置である。なお、図３においては、ＨＡ４０は、インターネットと接続されているが、インターネット以外のＩＰ（Internet Protocol）ネットワーク（企業内ネットワークなど）にも接続可能である。
【０００６】
ＷｉＭＡＸの無線通信システムにおいては、ＭＳ１０に対する認証として、ＭＳ１０がＡＳＮに接続されているかを認証するデバイス認証と、ＭＳ１０のユーザがＡＳＮのサービスの契約者であるかを認証するユーザ認証と、が行われる。
【０００７】
ここで、関連するＷｉＭＡＸの無線通信システムにおけるデバイス／ユーザ認証シーケンスについて、図４を参照して説明する。
【０００８】
なお、ここでは、Ｐｒｏｘｙ　Ｍｏｂｉｌｅ　ＩＰｖ４を適用した場合のデバイス／ユーザ認証シーケンスについて説明する。
【０００９】
また、ここでは、図４に示したデバイス／ユーザ認証シーケンスの前に、不図示のＤＬ（Down Link）－ＭＡＰシーケンスにおいて、ＢＳ２０は、ＭＳ１０からＭＳ１０のＭＡＣ（Media Access Control）アドレスを取得し、また、不図示のＭＳ－ＰｒｅＡｔｔａｃｈｍｅｎｔシーケンスにおいて、ＡＳＮ－ＧＷ３０は、ＢＳ２０からＭＳ１０のＭＡＣアドレスを取得し、ＡＳＮ内ではＭＳ１０をＭＡＣアドレスにより識別可能になっているものとする。
【００１０】
図４に示すように、まず、ＡＳＮ－ＧＷ３０は、ステップ４０１において、ＢＳ２０を介してＭＳ１０に対し、Ａｕｔｈ．Ｒｅｌａｙプロトコルを用いて、ＥＡＰ（Extensible Authentication Protocol）によるデバイス／ユーザ認証の開始およびＩｄｅｎｔｉｔｙの送付を要求するＥＡＰ　ＲＱ（Request）／Ｉｄｅｎｔｉｔｙメッセージを送信する。
【００１１】
次に、ＭＳ１０は、ステップ４０２において、ＢＳ２０およびＡＳＮ－ＧＷ３０を介してＡＡＡサーバ５０に対し、ＥＡＰ　ＲＱ／Ｉｄｅｎｔｉｔｙメッセージに対する応答として、ＥＡＰを用いて、ＭＳ１０の疑似のＮＡＩ（Network Access Identity）であるＰｓｅｕｄｏ－ＩｄｅｎｔｉｔｙおよびＭＡＣアドレスを含む、ＥＡＰ　ＲＰ（Response）／Ｉｄｅｎｔｉｔｙメッセージを送信する。

【００１２】
これにより、ＡＳＮ－ＧＷ３０は、ＭＳ１０のＰｓｅｕｄｏ－Ｉｄｅｎｔｉｔｙを取得し、取得済みのＭＡＣアドレスと対応付ける。また、ＡＡＡサーバ５０は、ＭＳ１０のＰｓｅｕｄｏ－ＩｄｅｎｔｉｔｙおよびＭＡＣアドレスを取得する。
【００１３】
次に、ＡＡＡサーバ５０は、ＭＳ１０に対するデバイス認証に成功すると、ステップ４０３において、ＡＳＮ－ＧＷ３０およびＢＳ２０を介してＭＳ１０に対し、ＥＡＰを用いて、デバイス認証に成功したことを通知するメッセージ（このメッセージの名称は認証方式によって異なる）を送信する。さらに、ＡＡＡサーバ５０は、ステップ４０４において、ＡＳＮ－ＧＷ３０およびＢＳ２０を介してＭＳ１０に対し、ＭＳ１０の真のＮＡＩであるＴｒｕｅ－Ｉｄｅｎｔｉｔｙの送付を要求するＥＡＰ　ＲＱメッセージを送信する。
【００１４】
次に、ＭＳ１０は、ステップ４０５において、ＢＳ２０およびＡＳＮ－ＧＷ３０を介してＡＡＡサーバ５０に対し、ＥＡＰ　ＲＱメッセージに対する応答として、ＥＡＰを用いて、ＭＳ１０のＴｒｕｅ－Ｉｄｅｎｔｉｔｙを含む、ＥＡＰ　ＲＰメッセージを送信する。
【００１５】
これにより、ＡＡＡサーバ５０は、ＭＳ１０のＴｒｕｅ－Ｉｄｅｎｔｉｔｙを取得し、取得済みのＰｓｅｕｄｏ－Ｉｄｅｎｔｉｔｙと対応付ける。
【００１６】
次に、ＡＡＡサーバ５０は、ＭＳ１０に対するユーザ認証に成功すると、ステップ４０６において、ＡＳＮ－ＧＷ３０に対し、ＥＡＰを用いて、ユーザ認証に成功したことを通知するＥＡＰ　Ｓｕｃｃｅｓｓメッセージを送信する。続いて、ＡＳＮ－ＧＷ３０は、ステップ４０７において、ＢＳ２０を介してＭＳ１０に対し、Ａｕｔｈ．Ｒｅｌａｙプロトコルを用いて、ＥＡＰ　Ｓｕｃｃｅｓｓメッセージを転送する。
【００１７】
次に、ＭＳ１０は、セッションを確立するために、ステップ４０８において、ＢＳ２０を介してＡＳＮ－ＧＷ３０に対し、ＤＨＣＰ（Dynamic Host Configuration Protocol）を用いて、ＩＰ（Internet Protocol）アドレスの割当を要求するＤＨＣＰ　Ｄｉｓｃｏｖｅｒメッセージを送信する。
【００１８】
次に、ＡＳＮ－ＧＷ３０は、ステップ４０９において、ＨＡ４０に対し、Ｍｏｂｉｌｅ　ＩＰを用いて、ＭＳ１０のＰｓｅｕｄｏ－Ｉｄｅｎｔｉｔｙを含む、ＭＳ１０のＣＳＮへの接続を要求するＲＲＱ（Registration Request）メッセージを送信する。
【００１９】
これにより、ＨＡ４０は、ＭＳ１０のＰｓｅｕｄｏ－Ｉｄｅｎｔｉｔｙを取得する。よって、ＨＡ４０は、以降、ユーザ識別情報として、ＮＡＩを使用可能となる。
【００２０】
このとき、ＨＡ４０に通知されるＮＡＩがＰｓｅｕｄｏ－Ｉｄｅｎｔｉｔｙである理由は以下の通りである。すなわち、ＡＳＮ－ＧＷ３０からＨＡ４０に通知されるＮＡＩは、Ｍｏｂｉｌｅ　ＩＰのＥｘｔｅｎｓｉｏｎフィールドに含まれるものであるため、ＩＰｓｅｃ（Security Architecture for IP）などのセキュリティトンネルを使用しなければ、プレーンデータがＡＳＮおよびＣＳＮ上に流れてしまう。このことから、ＷｉＭＡＸの無線通信システムでは、ＭＳ１０とＡＡＡサーバ５０だけが、ｔｒｕｅ－ｉｄｅｎｔｉｔｙを使用し、他のノードはｐｓｅｕｄｏ－ｉｄｅｎｔｉｔｙを使用することとしている。このため、ＡＳＮ－ＧＷ３０からＨＡ４０に通知されるＮＡＩは、ｐｓｅｕｄｏ－ｉｄｅｎｔｉｔｙとなる。なお、ｐｓｅｕｄｏ－ｉｄｅｎｔｉｔｙとｔｒｕｅ－ｉｄｅｎｔｉｔｙとの対応表も、ＭＳ１０とＡＡＡサーバ５０だけがもつことになる。
【００２１】
次に、ＨＡ４０は、ステップ４１０において、ＡＡＡサーバ５０に対し、ＡＡＡプロト

コル（例えば、ＲＡＤＩＵＳ（Remote Access Dial In User Service）プロトコル）を用いて、ＭＳ１０のＰｓｅｕｄｏ－Ｉｄｅｎｔｉｔｙを含む、ＭＳ１０に対する認証結果を要求するＡｃｃｅｓｓ　Ｒｅｑｕｅｓｔメッセージを送信する。

【００２２】

次に、ＡＡＡサーバ５０は、ステップ４１１において、ＨＡ４０に対し、Ａｃｃｅｓｓ　Ｒｅｑｕｅｓｔメッセージに対する応答として、ＡＡＡプロトコルを用いて、ＭＳ１０に対する認証結果を通知するＡｃｃｅｓｓ　Ａｃｃｅｐｔメッセージを送信する。

【００２３】

これにより、ＨＡ４０は、ＭＳ１０に対する認証結果を確認する。

【００２４】

次に、ＨＡ４０は、ステップ４１２において、ＡＳＮ－ＧＷ３０に対し、ＲＲＱメッセージに対する応答として、Ｍｏｂｉｌｅ　ＩＰを用いて、ＭＳ１０のＣＳＮへの接続を許可することを通知するＲＲＰ（Registration Response）メッセージを送信する。

【００２５】

その後、ＡＳＮ－ＧＷ３０は、ステップ４１３において、ＢＳ２０を介してＭＳ１０に対し、ＤＨＣＰ　Ｄｉｓｃｏｖｅｒメッセージに対する応答として、ＤＨＣＰを用いて、ＭＳ１０に割り当てるＩＰアドレスの候補を通知するＤＨＣＰ　Ｏｆｆｅｒメッセージを送信する。

【００２６】

これにより、ＭＳ１０は、ＩＰアドレスを取得し、セッション確立のための処理を開始する。

【００２７】

このように、ＷｉＭＡＸの無線通信システムにおいては、ＭＳ１０は、自己のユーザ識別情報として、Ｔｒｕｅ－Ｉｄｅｎｔｉｔｙ、Ｐｓｅｕｄｏ－Ｉｄｅｎｔｉｔｙ、およびＭＡＣアドレスの３つを使用している。

【００２８】

また、ＢＳ２０およびＡＳＮ－ＧＷ３０は、ＭＳ１０のユーザ識別情報として、Ｐｓｅｕｄｏ－ＩｄｅｎｔｉｔｙおよびＭＡＣアドレスの２つを使用可能である。

【００２９】

また、ＨＡ４０は、ＭＳ１０のユーザ識別情報として、Ｐｓｅｕｄｏ－Ｉｄｅｎｔｉｔｙの１つのみを使用可能である。

【００３０】

また、ＡＡＡサーバ５０は、ＭＳ１０のユーザ識別情報として、Ｔｒｕｅ－Ｉｄｅｎｔｉｔｙ、Ｐｓｅｕｄｏ－Ｉｄｅｎｔｉｔｙ、およびＭＡＣアドレスの３つを使用可能である。

【特許文献１】特開２００８－３５２４８号公報

【特許文献２】特開２００８－９２５７７号公報

【発明の開示】

【発明が解決しようとする課題】

【００３１】

ところで、ＭＳ１０、ＢＳ２０、ＡＳＮ－ＧＷ３０、ＨＡ４０、およびＡＡＡサーバ５０の各ノードは、ＭＳ１０のユーザに対して実行する保守機能を備えている。保守機能の一例を以下に示す。

・信号モニタリング機能

指定ユーザに関連する信号を記録する機能。例えば、ＨＡ４０は、Ｍｏｂｉｌｅ　ＩＰおよびＡＡＡプロトコルを用いて転送された信号のうち、指定ユーザに関連する信号を記録する。

・接続規制機能

指定ユーザの接続要求を拒否（Reject）する機能。例えば、ＨＡ４０は、指定ユーザのＣＳＮへの接続を要求するＲＲＱメッセージに対する応答として、ＲＲＰメッセージでエ

ラーを返す。
・輻輳規制除外機能
一般ユーザからの接続要求を破棄する状態でも、指定ユーザのみＲＲＱメッセージによる接続要求を受付ける機能。例えば、ＨＡ４０は、ＨＡ輻輳状態でも、指定ユーザのみ接続要求を受付ける。
・通信傍受機能
指定ユーザの通信データを記録する機能。例えば、ＨＡ４０は、Ｍｏｂｉｌｅ　ＩＰを用いて転送される通信データを通すトンネルを生成した後に、このトンネルを介してＭＳ１０とＣＳＮ間を実際に転送される通信データを記録する。
【００３２】
ただし、ユーザごとに、そのユーザに対して実行する保守機能は異なっている。例えば、あるユーザに対しては、上述した４つの保守機能を全て実行するが、別のユーザに対しては、上述した４つの保守機能のうち輻輳規制除外機能のみを実行する等である。
【００３３】
したがって、各ノードは、保守機能を実行するには、まず、自己に接続されるユーザを指定して、そのユーザに対する保守機能の実行要否を判断する必要がある。
【００３４】
ＭＳ１０およびＡＡＡ５０は、ｔｒｕｅ－ｉｄｅｎｔｉｔｙを使用してユーザ管理を行うことができるので、ユーザ指定を行うのに問題はない。
【００３５】
また、ＢＳ２０およびＡＳＮ－ＧＷ３０は、ｔｒｕｅ－ｉｄｅｎｔｉｔｙを知らないものの、ＮＡＩとは別にＭＡＣアドレスでもユーザ管理を行っているため、ユーザ指定を行うことができる。
【００３６】
しかし、ＨＡ４０は、ユーザ管理をｐｓｅｕｄｏ－ｉｄｅｎｔｉｔｙでしか行うことができない。
【００３７】
個々のセッションは、ｐｓｅｕｄｏ－ｉｄｅｎｔｉｔｙの一意性が保障されているので、セッション確立後であれば、ＨＡ４０は、そのセッションからユーザ指定を行うことが可能である。しかし、ｐｓｅｕｄｏ－ｉｄｅｎｔｉｔｙは、ＥＡＰによる認証シーケンスにおいてＭＳ１０により乱数生成される場合があるため、ＨＡ４０は、セッション確立前に、ユーザを指定できず、保守機能の実行要否を判断できないという課題がある。
【００３８】
また、ＨＡ４０は、他ノードが保持するｐｓｅｕｄｏ－ｉｄｅｎｔｉｔｙとｔｒｕｅ－ｉｄｅｎｔｉｔｙとの対応表がないと、Ｍｏｂｉｌｅ　ＩＰセッションのユーザを指定できず、保守機能の実行要否を判断できないという課題がある。
【００３９】
そこで、本発明の目的は、上述した課題のいずれかを解決することができる通信システム、接続装置、情報通知方法、プログラムを提供することにある。
【課題を解決するための手段】
【００４０】
本発明の通信システムは、
端末と、前記端末の移動を管理するサーバ装置と、前記端末を前記サーバ装置と接続する接続装置と、を有してなる通信システムであって、
前記接続装置は、
前記端末のＭＡＣアドレスを記録するとともに、前記端末に対する保守機能の実行要否を表す保守機能実行要否情報を該端末のＭＡＣアドレスと対応付けて記録し、
前記端末のＭＡＣアドレスと対応付けられた保守機能実行要否情報を含むメッセージを、Ｍｏｂｉｌｅ　ＩＰを用いて前記サーバ装置に送信する。
【００４１】

本発明の接続装置は、
端末を、該端末の移動を管理するサーバ装置と接続する接続装置であって、
前記端末のＭＡＣアドレスを記録するとともに、前記端末に対する保守機能の実行要否を表す保守機能実行要否情報を該端末のＭＡＣアドレスと対応付けて記録する記録部と、
前記端末のＭＡＣアドレスと対応付けられた保守機能実行要否情報をメッセージに含める制御部と、
前記メッセージを、Ｍｏｂｉｌｅ　ＩＰを用いて前記サーバ装置に送信する送信部と、を有する。

【００４２】
本発明の情報通知方法は、
端末を、該端末の移動を管理するサーバ装置と接続する接続装置による情報通知方法であって、
前記端末のＭＡＣアドレスを記録するとともに、前記端末に対する保守機能の実行要否を表す保守機能実行要否情報を該端末のＭＡＣアドレスと対応付けて記録する記録ステップと、
前記端末のＭＡＣアドレスと対応付けられた保守機能実行要否情報をメッセージに含める制御ステップと、
前記メッセージを、Ｍｏｂｉｌｅ　ＩＰを用いて前記サーバ装置に送信する送信ステップと、を有する。

【００４３】
本発明のプログラムは、
端末を、該端末の移動を管理するサーバ装置と接続する接続装置に、
前記端末のＭＡＣアドレスを記録するとともに、前記端末に対する保守機能の実行要否を表す保守機能実行要否情報を該端末のＭＡＣアドレスと対応付けて記録する記録手順と、
前記端末のＭＡＣアドレスと対応付けられた保守機能実行要否情報をメッセージに含める制御手順と、
前記メッセージを、Ｍｏｂｉｌｅ　ＩＰを用いて前記サーバ装置に送信する送信手順と、を実行させる。

【発明の効果】

【００４４】
本発明の通信システムによれば、接続装置は、サーバ装置に対し、端末のＭＡＣアドレスに対応する保守機能実行要否情報を含むメッセージを、Ｍｏｂｉｌｅ　ＩＰを用いて送信する。

【００４５】
したがって、サーバ装置は、メッセージの受信以降に、保守機能実行要否情報を確認可能となるため、疑似のＮＡＩと真のＮＡＩとの対応表を持たなくても、保守機能の実行要否を判断できるという効果が得られる。

【発明を実施するための最良の形態】

【００４６】
以下に、本発明を実施するための最良の形態について図面を参照して説明する。

【００４７】
なお、以下で説明する実施形態では、本発明の通信システムが、ＷｉＭＡＸの無線通信システムである場合を例に挙げて説明するが、本発明はこれに限定されず、他の通信方式の無線通信システム、有線通信システム、有線無線混在通信システムであってもよい。

【００４８】
本実施形態の無線通信システムは、図３の無線通信システムの構成要素のうち、ＡＳＮ－ＧＷ３０をＡＳＮ－ＧＷ３０Ａに変更し、図４のデバイス／ユーザ認証シーケンス内の処理のうち、ＲＲＱメッセージに係るステップ４０９をステップ４０９Ａに変更したものである。

【００４９】
そこで、以下では、ＲＲＱメッセージに係る処理を行うＡＳＮ－ＧＷ３０Ａを中心に説明する。
【００５０】
図１は、本実施形態におけるＡＳＮ－ＧＷ３０Ａの構成を示すブロック図である。なお、図１は、ＲＲＱメッセージに係る処理を行う部分の構成のみを示している。
【００５１】
図１に示すように、本実施形態におけるＡＳＮ－ＧＷ３０Ａは、記録部３１と、制御部３２と、送信部３３と、を有している。
【００５２】
記録部３１は、対応表３１１と保守管理機能リスト３１２とを記録する。
【００５３】
対応表３１１には、デバイス／ユーザ認証シーケンスの前の不図示のＭＳ－ＰｒｅＡｔｔａｃｈｍｅｎｔシーケンスにおいて取得されるＭＳ１０のＭＡＣアドレスと、デバイス／ユーザ認証シーケンスにおいて取得されるＭＳ１０のｐｓｅｕｄｏ－ｉｄｅｎｔｉｔｙと、が対応付けられて記録される。
【００５４】
保守管理機能リスト３１２には、ＨＡ４０がＭＳ１０に対して実行する保守機能の実行要否を表す保守機能実行要否情報が、ＭＳ１０のＭＡＣアドレスと対応付けられて、ＭＡＣアドレスごと（ユーザごと）に記録される。例えば、記録部３１は、ＭＡＣアドレスごとに、表１に示すような保守管理機能リスト３１２を記録することになる。
【００５５】
【表１】

| 保守機能一覧 | 保守機能実行要否情報 |
|---|---|
| 信号モニタリング機能 | 実行しない |
| 接続規制機能 | 実行しない |
| 輻輳規制除外機能 | 実行する |
| 通信傍受機能 | 実行しない |
| ： | ： |

【００５６】
ここで、ＡＡＡサーバ５０は、ＭＳ１０に対するデバイス／ユーザ認証を行うものであり、一般的に、全ユーザの詳細情報を持っている。そのため、ＡＡＡサーバ５０の構成を、ユーザごとに保守管理機能リストを持つ構成とすることは比較的容易である。
【００５７】
これに対して、ＡＳＮ－ＧＷ３０Ａは、一般的に、全ユーザの詳細情報を持たず、ユーザごとに保守管理機能リストを持つ構成とすることは困難である。
【００５８】
そのため、ＡＳＮ－ＧＷ３０Ａは、特定のユーザ（オペレータが任意に選択し、詳細情報を登録したユーザ）のみ保守管理機能リスト３１２を持ち、その他のユーザにはデフォルトの保守管理機能リストを適用してもよい。
【００５９】
または、ＡＡＡサーバ５０でユーザごとの保守管理機能リストを作成し、ＡＳＮ－ＧＷ３０Ａは、事前にＡＡＡサーバ５０から保守管理機能リストを送信してもらい、これを保守管理機能リスト３１２としてもよい。
【００６０】
制御部３２は、対応表３１１からＭＳ１０のｐｓｅｕｄｏ－ｉｄｅｎｔｉｔｙおよびＭＡＣアドレスを抽出する。
【００６１】

また、制御部３２は、上記で抽出されたＭＡＣアドレスに対応する保守機能実行要否情報を保守管理機能リスト３１２から抽出する。

【００６２】

さらに、制御部３２は、ＲＲＱメッセージにＥｘｔｅｎｓｉｏｎフィールドを追加し、そのＥｘｔｅｎｓｉｏｎフィールドに、上記で抽出された保守機能実行要否情報を含める。

【００６３】

送信部３３は、制御部３２によりＥｘｔｅｎｓｉｏｎフィールドに保守機能実行要否情報を含めたＲＲＱメッセージを、Ｍｏｂｉｌｅ　ＩＰを用いてＨＡ４０に送信する。

【００６４】

以下、本実施形態におけるデバイス／ユーザ認証シーケンスについて、図２を参照して説明する。なお、図２において、図４と同様のステップには同様の符号を付す。

【００６５】

図２に示すように、まず、図４と同様のステップ４０１～４０８の処理が行われる。

【００６６】

次に、ステップ４０９Ａにおいて、ＡＳＮ－ＧＷ３０Ａは、ステップ４０８でＤＨＣＰ　Ｄｉｓｃｏｖｅｒメッセージを送信してきたＭＳ１０のｐｓｅｕｄｏ－ｉｄｅｎｔｉｔｙおよびＭＡＣアドレスを対応表３１１から抽出する。続いて、ＡＳＮ－ＧＷ３０Ａは、上記で抽出されたＭＡＣアドレスに対応する保守機能実行要否情報を保守管理機能リスト３１２から抽出する。続いて、ＡＳＮ－ＧＷ３０Ａは、ＲＲＱメッセージのＥｘｔｅｎｓｉｏｎフィールドに上記で抽出された保守機能実行要否情報を含め、そのＲＲＱメッセージを、Ｍｏｂｉｌｅ　ＩＰを用いてＨＡ４０に送信する。

【００６７】

その後、図４と同様のステップ４１０～４１３の処理が行われる。

【００６８】

上述したように本実施形態においては、ＡＳＮ－ＧＷ３０Ａは、ＨＡ４０に対し、セッションを確立しようとしているＭＳ１０に対する保守機能の実行要否を表す保守機能実行要否情報を、Ｍｏｂｉｌｅ　ＩＰを用いてＲＲＱメッセージにより通知する。

【００６９】

そのため、ＨＡ４０は、ＲＲＱメッセージの受信以降に、ＭＳ１０が確立しようとしているセッションに必要な保守機能実行要否情報を確認可能となる。

【００７０】

よって、ＨＡ４０は、ｐｓｅｕｄｏ－ｉｄｅｎｔｉｔｙ以外のユーザ識別情報や、ｐｓｅｕｄｏ－ｉｄｅｎｔｉｔｙとｔｒｕｅ－ｉｄｅｎｔｉｔｙとの対応表を持たなくても、セッション確立前に、保守機能の実行要否を判断できる。

【００７１】

なお、本実施形態においては、Ｐｒｏｘｙ　Ｍｏｂｉｌｅ　ＩＰｖ４を適用した場合のデバイス／ユーザ認証シーケンスについて説明したが、本発明はこれに限定されず、その他のデバイス／ユーザ認証シーケンス（例えば、Ｃｌｉｅｎｔ　Ｍｏｂｉｌｅ　ＩＰｖ４を適用したもの）を適用してもよい。

【００７２】

また、本実施形態においては、ＨＡ４０と対向する接続装置がＡＳＮ－ＧＷ３０Ａである場合について説明したが、本発明はこれに限定されない。例えば、本発明をＷｉＭＡＸ以外のネットワークに適用する場合、ＨＡ４０と対向する接続装置は、必ずしもＡＳＮ－ＧＷ３０Ａではなく、ＦＡ（Foreign-Agent）となる場合もある。この場合、本発明の接続装置をＦＡに適用し、図１に示したＡＳＮ－ＧＷ３０Ａと同様の機能をＦＡに設ければよい。

【００７３】

なお、本発明のＡＳＮ－ＧＷ３０Ａにて行われる方法は、コンピュータに実行させるためのプログラムに適用してもよい。また、そのプログラムを記憶媒体に格納することも可

能であり、ネットワークを介して外部に提供することも可能である。

【図面の簡単な説明】

【００７４】

【図１】本発明の一実施形態の無線通信システムにおけるＡＳＮ－ＧＷの構成を示すブロック図である。

【図２】本発明の一実施形態の無線通信システムにおけるデバイス／ユーザ認証シーケンスを説明するシーケンス図である。

【図３】無線通信システムの全体構成を示す図である。

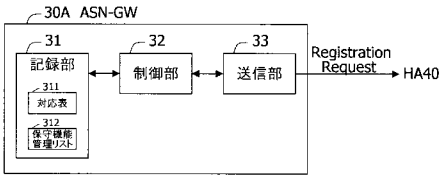
【図４】関連する無線通信システムにおけるデバイス／ユーザ認証シーケンスを説明するシーケンス図である。

【符号の説明】

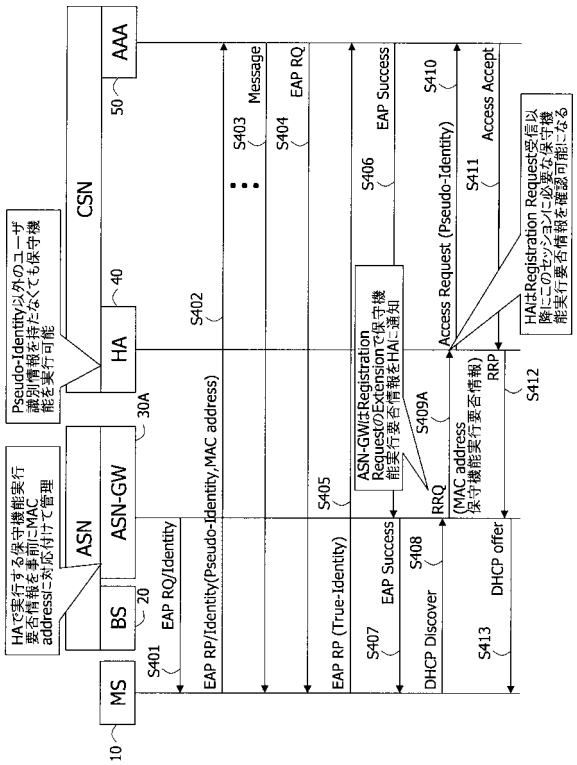
【００７５】

１０　　ＭＳ
２０　　ＢＳ
３０，３０Ａ　　ＡＳＮ－ＧＷ
３１　　記録部
３２　　制御部
３３　　送信部
３１１　　対応表
３１２　　保守機能管理リスト
４０　　ＨＡ
５０　　ＡＡＡサーバ

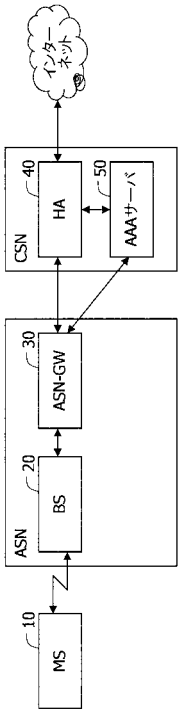
【図１】



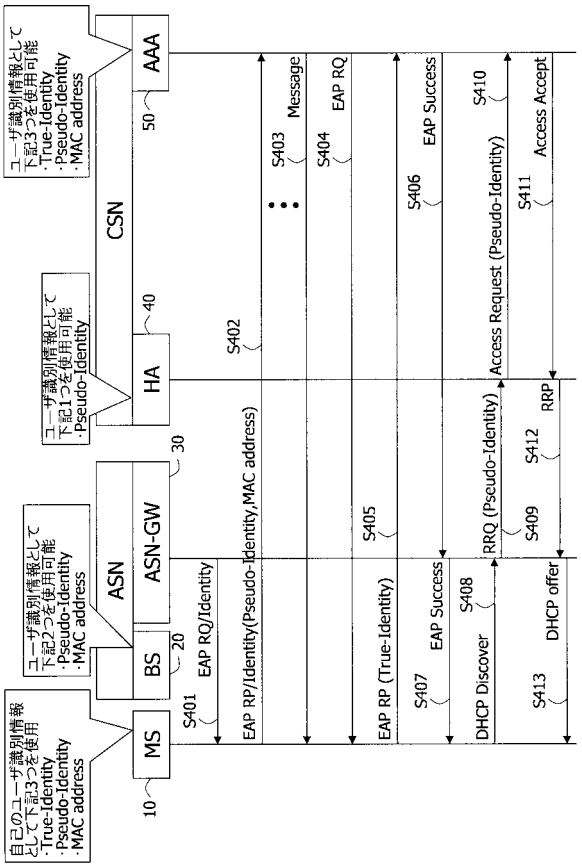

【図２】



【図３】


インターネット
CSN
40
HA
50
AAAサーバ
ASN
30
ASN-GW
20
BS
10
MS

【図４】


自己のユーザ識別情報として下記3つを使用
・True-Identity
・Pseudo-Identity
・MAC address
ユーザ識別情報として下記2つを使用可能
・Pseudo-Identity
・MAC address
ユーザ識別情報として下記1つを使用可能
・Pseudo-Identity
ユーザ識別情報として下記3つを使用可能
・True-Identity
・Pseudo-Identity
・MAC address
MS
10
BS
20
ASN
ASN-GW
30
HA
40
CSN
AAA
50
S401
EAP RQ/Identity
EAP RP/Identity(Pseudo-Identity,MAC address)
S402
S403
Message
EAP RQ
S404
EAP RP (True-Identity)
S405
S406
EAP Success
S407
EAP Success
DHCP Discover
S408
RRQ (Pseudo-Identity)
Access Request (Pseudo-Identity)
S410
S409
S412
RRP
S411
Access Accept
S413
DHCP offer

フロントページの続き

(56)参考文献 特開２００６－８０９３０（ＪＰ，Ａ）
国際公開第２００７／１１７４６１（WO，Ａ２）
国際公開第２００８／０８０４２０（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｗ　４／００ － ９９／００
Ｈ０４Ｂ　７／２６