

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2009-524301
(P2009-524301A)

(43) 公表日 平成21年6月25日(2009.6.25)

(51) Int.Cl.		F I			テーマコード (参考)
HO4W 4/24	(2009.01)	HO4Q	7/00	136	5K067
HO4W 12/06	(2009.01)	HO4Q	7/00	183	5K201
HO4M 11/00	(2006.01)	HO4M	11/00	303	

審査請求 有 予備審査請求 未請求 (全 33 頁)

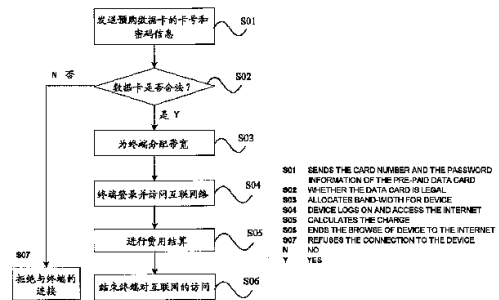
(21) 出願番号 特願2008-550610 (P2008-550610)
 (86) (22) 出願日 平成18年11月24日 (2006.11.24)
 (85) 翻訳文提出日 平成20年7月16日 (2008.7.16)
 (86) 国際出願番号 PCT/CN2006/003161
 (87) 国際公開番号 W02007/082444
 (87) 国際公開日 平成19年7月26日 (2007.7.26)
 (31) 優先権主張番号 200610033166.9
 (32) 優先日 平成18年1月18日 (2006.1.18)
 (33) 優先権主張国 中国 (CN)

(71) 出願人 504277388
 ▲ホア▼▲ウェイ▼技術有限公司
 中華人民共和國518129広東省深▲セ
 ン▼市龍岡区坂田華為本社ビル
 (74) 代理人 100064908
 弁理士 志賀 正武
 (74) 代理人 100089037
 弁理士 渡邊 隆
 (74) 代理人 100108453
 弁理士 村山 靖彦
 (74) 代理人 100110364
 弁理士 実広 信哉
 (72) 発明者 潘 海濤
 中華人民共和國518129広東省深▲セ
 ン▼市龍岡区坂田華為本社ビル
 最終頁に続く

(54) 【発明の名称】 プリペイドユーザによるインターネットへの無線アクセス方法

(57) 【要約】

プリペイドユーザのためのインターネットへの無線アクセスの方法は、以下のステップを有している。すなわち、ユーザ無線装置が無線通信ネットワークを通じてインターネットへログオンする場合、ユーザアカウント及びパスワード情報を無線通信ネットワークに送信するとともに(S01)、前記ユーザアカウント、パスワード及びプリペイド額の情報は無線通信ネットワークに保存される。前記無線通信ネットワークはユーザ無線装置に対して認証を行い(S02)、認証を通過した場合無線ユーザに帯域幅が割り当てられ(S03)、通過しなかった場合ユーザ無線装置に対する接続は拒否される(S07)。前記装置はインターネットにログオンしアクセスする(S04)。前記装置からログオフ要求情報を受信した場合、料金を計算し(S05)、プリペイド額から料金を差し引き、アクセスを終了させる(S06)。



【特許請求の範囲】**【請求項 1】**

インターネットに対するプリペイドユーザの無線アクセス方法であって、無線通信ネットワークを介してインターネットにログオンする場合、無線ユーザ端末により、ユーザアカウント番号及びパスワードに関する情報を無線通信ネットワークに送信するステップと、

前記無線通信ネットワークによって無線ユーザ端末の認証を行うステップと、

端末によってインターネットにログオンしかつ接続するステップと、

を具備し、

ユーザアカウント番号、パスワード及びプリペイド額に関する情報を、無線通信ネットワークにあらかじめ保持し、

前記無線ユーザ端末が認証を通過した場合、無線ユーザ端末に帯域幅を割り当て、そうでない場合、無線ユーザ端末の接続を拒否することを特徴とする無線アクセス方法。

【請求項 2】

前記無線ユーザ端末から切断要求メッセージを受信すると、無線通信ネットワークによって料金を計算し、プリペイド額から前記料金を差し引くステップと、

無線ユーザ端末をインターネットから切断するステップと、

を具備することを特徴とする請求項 1 に記載の無線アクセス方法。

【請求項 3】

前記ユーザアカウント番号及びパスワードに関する情報を無線通信ネットワークに送信するステップは、

無線通信ネットワークを介してインターネットへログオンする場合、ユーザアカウント番号及びパスワードに関する無線ユーザ端末の情報を、無線ユーザ端末から無線パケットゲートウェイへ送信するステップと、

ユーザアカウント番号及びパスワードに関する情報を、無線パケットゲートウェイから認証・認可・アカウントイング (A A A : Authentication Authorization and Accounting) システムへ送信するステップと、

を具備することを特徴とする請求項 1 に記載の無線アクセス方法。

【請求項 4】

前記無線ユーザ端末の認証を行うステップは、

ユーザアカウント番号及びパスワードに関する情報を、A A A システムによってデータベースから取得するステップと、

取得した情報に記録されているパスワードに関する情報が、無線ユーザ端末から送信されたパスワードに関する情報と一致するかどうかを判定するステップと、

一致した場合、無線ユーザ端末に帯域幅を割り当てるステップと、

一致しなかった場合、端末の接続を拒否するステップと、

を具備することを特徴とする請求項 3 に記載の無線アクセス方法。

【請求項 5】

無線ユーザ端末の認証を行うステップは、

無線ユーザ端末の認証を行うため、ユーザアカウント番号及びパスワードに関する情報を保持する認証要求メッセージを A A A システムから携帯電話インテリジェントネットワークへ送信するステップと、

ユーザアカウント番号に従って、ユーザアカウント番号及びパスワードに関する情報を、携帯電話インテリジェントネットワークによってデータベースから取得するステップと、

取得した情報に記録されているパスワードに関する情報を、A A A システムへ送信するステップと、

携帯電話インテリジェントネットワークから送信されたパスワードに関する情報が、A A A システムによって無線ユーザ端末から送信されたパスワードに関する情報と一致するかどうかを判定するステップと、

10

20

30

40

50

携帯電話インテリジェントネットワークから送信されたパスワードに関する情報が、送信されたパスワードに関する情報と一致した場合、無線ユーザ端末に帯域幅を割り当てるステップと、

一致しなかった場合、無線ユーザ端末の接続を拒否するステップと、
を具備することを特徴とする請求項 3 に記載の無線アクセス方法。

【請求項 6】

前記無線ユーザ端末の認証を行うステップは、

無線ユーザ端末の認証を行うため、ユーザアカウント番号及びパスワードに関する情報を保持する認証要求メッセージを、AAAシステムから携帯電話インテリジェントネットワークへ送信するステップと、

ユーザアカウント番号に従って、ユーザアカウント番号及びパスワードに関する情報を、データベースから携帯電話インテリジェントネットワークによって取得するステップと、

取得した情報に記録されているパスワードに関する情報が、無線ユーザ端末から送信されたパスワードに関する情報と一致するかどうかを判定するステップと、

インテリジェントネットワークが取得した情報に記録されているパスワードに関する情報が、無線ユーザ端末から送信されたパスワードに関する情報と一致した場合、

前記無線ユーザ端末が正規なものであることを示すメッセージを、携帯電話インテリジェントネットワークからAAAシステムへ送信するとともに、無線ユーザ端末に帯域幅を割り当てるステップと、

一致しなかった場合、無線ユーザ端末が不正であることを示すメッセージを、携帯電話インテリジェントネットワークからAAAシステムに送信するとともに、無線ユーザ端末の接続を拒否するステップと、

を具備することを特徴とする請求項 3 に記載の無線アクセス方法。

【請求項 7】

さらに前記無線ユーザ端末のSIMカードの認証を行うステップは、

無線ユーザ端末及びSIMカードの両方が認証を通過した場合、無線ユーザ端末に帯域幅を割り当てるステップと、

認証を通過しなかった場合、無線ユーザ端末を拒否するステップと、

を具備することを特徴とする請求項 3 に記載の無線アクセス方法。

【請求項 8】

前記無線ユーザ端末の認証を行うステップは、

ユーザアカウント番号に従って、データベースからユーザアカウント番号及びパスワードに関する情報をAAAシステムによって取得するステップと、

取得した情報に記録されているパスワードに関する情報が、無線ユーザ端末から送信されたパスワードに関する情報と一致するかどうかを判定するステップと、

一致した場合、AAAシステムによって無線ユーザ端末のSIMカード番号を得るステップと、

SIMカードの認証を行うため、SIMカード番号を運ぶ認証要求メッセージを携帯電話インテリジェントネットワークへ送信するステップと、

携帯電話インテリジェントネットワークによってSIMカードの情報に関するデータベースを問い合わせるステップと、

前記SIMカードが正規なものであるかどうかを判定するステップと

正規であった場合、SIMカードが正規であることを示すメッセージを、携帯電話インテリジェントネットワークからAAAシステムへ送信するとともに、無線ユーザ端末に帯域幅を割り当てるステップと、

不正であった場合、SIMカードが不正であることを示すメッセージを、携帯電話インテリジェントネットワークからAAAシステムへ送信するとともに、無線ユーザ端末の接続を拒否するステップと、

を具備することを特徴とする請求項 7 に記載の無線アクセス方法。

10

20

30

40

50

【請求項 9】

前記無線ユーザ端末の認証を行うステップは、

A A Aシステムによって無線ユーザ端末のS I Mカード番号を得るステップと、

無線ユーザ端末及びS I Mカードの認証を行うため、S I Mカード番号と同様にユーザアカウント番号及びパスワードを保持する認証要求メッセージを携帯電話インテリジェントネットワークへ送信するステップと、

ユーザアカウント番号に従って無線ユーザ端末の情報をデータベースから携帯電話インテリジェントネットワークによって取得するステップと、

取得した情報に記録されているパスワードに関する情報が、無線ユーザ端末から送信されたパスワードに関する情報と一致するかどうかを判定するステップと、

10

一致しなかった場合、無線ユーザ端末が不正であることを示すメッセージを携帯電話インテリジェントネットワークからA A Aシステムへ送信するとともに、無線ユーザ端末の接続を拒否するステップと、

一致した場合、携帯電話インテリジェントネットワークによってS I Mカードの情報に関するデータベースに問い合わせ、S I Mカードが正規なものであるかどうかを判定するステップと、

正規であった場合、無線ユーザ端末とS I Mカードの両方が正規であることを示すメッセージを、携帯電話インテリジェントネットワークからA A Aシステムへ送信するとともに、無線ユーザ端末に帯域幅を割り当てるステップと、

正規でなかった場合、S I Mカードが不正であることを示すメッセージを、携帯電話インテリジェントネットワークからA A Aシステムへ送信するとともに、無線ユーザ端末の接続を拒否するステップと、

20

を具備することを特徴とする請求項7に記載の無線アクセス方法。

【請求項 10】

前記無線ユーザ端末の認証を行うステップは、

A A Aシステムによってインターネットへアクセスするための要求メッセージからS I Mカード番号を得るステップと、

無線ユーザ端末及びS I Mカードの認証を行うため、S I Mカードと同様に、ユーザアカウント番号及びパスワードに関する情報を保持する認証要求メッセージを携帯電話インテリジェントネットワークへ送信するステップと、

30

携帯電話インテリジェントネットワークによって、S I Mカードの情報に関するデータベースに問い合わせるステップと、

前記S I Mカードが正規なものであるかどうかを判定するステップと、

正規でなかった場合、S I Mカードが不正であることを示すメッセージを、携帯電話インテリジェントネットワークからA A Aシステムへ送信するとともに、無線ユーザ端末の接続を拒否するステップと、

正規であった場合、携帯電話インテリジェントネットワークによって、ユーザアカウント番号に従って、無線ユーザ端末の情報をデータベースから取得するとともに、取得した情報に記録されているパスワードに関する情報をA A Aシステムへ送信するステップと、

A A Aシステムによって、携帯電話インテリジェントネットワークから送信されたパスワードに関する情報が、無線ユーザ端末から送信されたパスワードに関する情報と一致するかどうかを判定するステップと、

40

一致した場合、無線ユーザ端末に帯域幅を割り当てるステップと、

一致しなかった場合、無線ユーザ端末の接続を拒否するステップと、

を具備することを特徴とする請求項7に記載の無線アクセス方法。

【請求項 11】

さらに前記無線ユーザ端末を認証する場合、無線ユーザ端末の正当性を認証するステップと、

適応性と有効期限について無線ユーザ端末を認証するステップと、

無線ユーザ端末が、正当性の認証を通過した場合、ステップ3が実行するステップと、

50

通過しなかった場合、端末の接続を拒否するステップと、

を具備することを特徴とする請求項 1 から請求項 10 のいずれか 1 項に記載の無線アクセス方法。

【請求項 12】

無線ユーザ端末を認証するステップと無線ユーザ端末に帯域幅を割り当てるステップの間には、

金額の保存に関する情報を設定するステップ

をさらに具備することを特徴とする請求項 1 から請求項 10 のいずれか 1 項に記載の無線アクセス方法。

【請求項 13】

金額の保存に関する情報の設定を行うステップは、

データカードの金額を保存するための要求を A A A システムから携帯電話インテリジェントネットワークへ送信するステップと、

前記要求に従ってユーザアカウント番号に対するプリペイド額を携帯電話インテリジェントネットワークによって保存するステップと、

プリペイド額が保存されたことを示すメッセージを A A A システムへ送信するステップと、

を具備することを特徴とする請求項 11 に記載の無線アクセス方法。

【請求項 14】

前記ユーザアカウントの残り金額が指定額より少ない又は等しいことを無線パケットゲートウェイから検出した場合、無線ユーザ端末によるインターネットサーフィンを終了させるステップ

をさらに具備することを特徴とする請求項 13 に記載の無線アクセス方法。

【請求項 15】

無線ユーザ端末を認証するステップと無線ユーザ端末に帯域幅を割り当てるステップの間は、

データカードの残り金額を A A A システムによって問い合わせるステップと、

前記金額から支払い可能なトラフィック量を計算するステップと、

支払い可能なトラフィック量に関する情報を無線パケットゲートウェイへ送信するステップと、

無線パケットゲートウェイによって、前記端末へ送信されたトラフィック量を計算するステップと、

トラフィック量が、支払い可能なトラフィック量より多い又は等しい場合、無線ユーザ端末によるインターネットサーフィンを終了させるステップと、

を具備することを特徴とする請求項 1 から請求項 10 のいずれか 1 項に記載の無線アクセス方法。

【請求項 16】

無線ユーザ端末を切断した時に、無線ユーザ端末へ送信されたトラフィック量に従ってプリペイド額から接続料金を差し引くステップ

をさらに具備することを特徴とする請求項 1 から請求項 10 のいずれか 1 項に記載の無線アクセス方法。

【請求項 17】

プリペイド額から接続料金を差し引くステップは、

無線パケットゲートウェイによって、無線ユーザ端末に送信されたトラフィック量を計算するステップと、

前記トラフィック量を A A A システムへ送信し、A A A システムによってトラフィック量に従ってプリペイド額から接続料金を差し引くステップと、

を具備することを特徴とする請求項 16 に記載の無線アクセス方法。

【請求項 18】

プリペイド額から接続料金を差し引くステップは、

10

20

30

40

50

無線パケットゲートウェイによって無線ユーザ端末へ送信されたトラフィック量を計算し、AAAシステムへトラフィック量を送信するステップと、

AAAシステムによって前記トラフィック量から接続料金を計算し、プリペイド額から接続料金を差し引くための要求を、携帯電話インテリジェントネットワークへ送信するステップと、

携帯電話インテリジェントネットワークによって、プリペイド額から接続料金を差し引くステップと、

を具備することを特徴とする請求項16に記載の無線アクセス方法。

【発明の詳細な説明】

【技術分野】

10

【0001】

本発明はネットワーク技術の分野、特にプリペイドユーザによるインターネットへの無線アクセスの方法に関連するものである。

【0002】

本願は、発明の名称を“データカードを使用したインターネットへの無線アクセス方法”として2006年1月18日に中国特許庁へ提出された、中国特許出願第200610033166.9号に基づき優先権を主張し、その内容は引用によってそのままここに組み込まれる。

【背景技術】

【0003】

20

社会の発展につれて、社会生活、経済、科学研究、国家防衛など、様々な情報が常に更新されるとともに、正確な情報が行き交い様々な分野でますます使われている。個人又は集団の発展は、他の成功を頼りにしなければならない。したがって情報を完全に取得する方法は、重要な問題の1つとなる。そこに、情報を取得するための様々な手段が存在する。とりわけ、現在、人々にとってネットワークは、便利で迅速にかつ詳細な方法で情報を取得するには最良であり、テレビや新聞といったメディアよりもポピュラーである。現在、ユーザの多くは、広いカバレッジ及び高帯域幅で利点のある有線ブロードバンドネットワークを通して情報を取得する。しかし、有線ブロードバンドネットワークは、固定した場所によるPCからアクセスのみが可能である。その結果、ユーザはインターネットサーフィンをするため、固定した場所にPCを持ち運ばなければならない、非常に不便である。同様に、ユーザは、有線ブロードバンドネットワークに比べてログオンできる場所がより自由な無線ローカルエリアネットワークを通して、情報を取得する。しかし、これもカバレッジが狭いことがユーザにとって不便の原因になっている。社会経済の迅速な発展の結果としての携帯端末の高い普及率と同様に、無線ネットワークの持続的な進歩の結果としての広いカバレッジと他のネットワークを通じた携帯性の点から、無線ネットワークの重要な長所により、様々な分野の人々にとって、携帯端末又は無線ネットワークカード（携帯端末のSIMカードを通して無線ネットワークにアクセスするために、携帯端末又はPCに挿入することができる）によって、無線ネットワークを通して情報を取得することが、最善の選択になる。

30

【0004】

40

しかし、先行技術では、携帯端末又は無線ネットワークカードを使って、ユーザがインターネットサーフィンする場合、以下の欠点が生じる。

【発明の開示】

【発明が解決しようとする課題】

【0005】

現在、携帯端末又は無線ネットワークカードを通して、インターネットにアクセスするためにユーザがダイヤルアップする場合、ネットワークシステムは、ユーザが使用しているSIMカードのみを検証し、一定のセキュリティ情報によってユーザの身元を認証しない。ユーザがSIMカードを使用してアクセスすることが通常の状態であるかぎり（たとえば、SIMカードの番号に料金を支払う必要がない）、ユーザはインターネットにアクセ

50

スすることができる。したがって、発生する全ての料金は、アクセスに使用したSIMカードのアカウントから差し引かれる。さらに、ユーザAが携帯端末又は無線ネットワークカードを紛失し、ユーザBがユーザAの携帯端末又は無線ネットワークカードを入手した場合、身元確認が要求されないため、ユーザBはその携帯端末又は無線ネットワークカードを使って直接インターネットサーフィンすることができる。したがって、発生する全ての料金はユーザAが支払うことになり、その結果、携帯端末の正規ユーザに多大な損害と不都合をもたらしてしまう。

【課題を解決するための手段】

【0006】

本発明は、プリペイドユーザがインターネットに無線アクセスするための方法を提供する。他のユーザによるインターネットへの不正アクセスによって、携帯端末の正規ユーザに不合理な料金が発生することを防ぐため、本発明は、データカードに設定されたユーザアカウント番号及びパスワードに関する情報を通してユーザの身元認証を可能にする。

10

【0007】

本発明の一実施形態は、プリペイドユーザによるインターネットへの無線アクセスの方法を提供し、以下のステップを有している。

【0008】

無線通信ネットワークを介してインターネットにログオンする場合、無線ユーザ端末は、ユーザアカウント番号及びパスワードに関する情報を無線通信ネットワークへ送信する。このとき、ユーザアカウント番号、パスワード、プリペイド額に関する情報は、無線通信ネットワークにあらかじめ保持されている。

20

【0009】

無線通信ネットワークは無線ユーザ端末を認証し、無線ユーザ端末が認証を通過した場合無線ユーザ端末に帯域幅が割り当てられ、そうでない場合無線ユーザ端末の接続は拒否される。

【0010】

端末によってインターネットにログオンし、インターネットサーフィンを行う。

【0011】

さらなる利点として、本発明は以下のステップを有する。

【0012】

無線ユーザ端末からの切断メッセージを受信すると、無線通信ネットワークは料金を計算し、プリペイド額から前記料金を差し引く。

30

【0013】

ユーザ携帯端末をインターネットから切断する。

【0014】

ユーザアカウント番号及びパスワードに関する情報を無線通信ネットワークへ送信するステップは、以下のステップを有している。無線通信ネットワークを介してインターネットにログインする場合、ユーザアカウント番号及びパスワードについて無線ユーザ端末の情報を、無線ユーザ端末から無線パケットゲートウェイへ送信する。

【0015】

無線パケットゲートウェイは、ユーザアカウント番号及びパスワードについての情報を、認証・認可・アカウントリング(AAA: Authentication Authorization and Accounting)システムへ送信する。

40

【0016】

好ましくは、無線ユーザ端末の認証は、以下のステップを有している。

【0017】

AAAシステムは、ユーザアカウント番号に従ってデータベースから、ユーザアカウント番号及びパスワードに関する情報を取得するとともに、取得した情報に記録されたパスワードに関する情報が、無線ユーザ端末から送信されたパスワードに関する情報と一致するかどうかを判定し、一致した場合無線ユーザ端末に帯域幅が割り当てられ、一致しない

50

場合端末接続は拒否される。

【0018】

好ましくは、無線ユーザ端末の認証は、以下のステップを有している。

【0019】

ユーザアカウント番号及びパスワードに関する情報を所持する、無線ユーザ端末について認証を行うため、認証要求メッセージがAAAシステムから携帯電話インテリジェントネットワークへ送信される。

【0020】

ユーザアカウント番号に従ってデータベースから、ユーザアカウント番号及びパスワードに関する情報が、携帯電話インテリジェントネットワークによって取得されるとともに、取得された情報に記録されたパスワードに関する情報がAAAシステムへ送信される。

【0021】

AAAシステムは、携帯電話インテリジェントネットワークから送信されたパスワードに関する情報が、無線ユーザ端末から送信されたパスワードに関する情報と一致するかどうかを判定し、一致した場合無線ユーザ端末に帯域幅を割り当てる。

【0022】

一致しなかった場合無線ユーザ端末の接続は拒否される。

【0023】

さらに有利な点として、本発明では、端末切断の際、無線ユーザ端末に送信されたトラフィック量に従ってプリペイド額から接続料金を差し引くステップを有している。

【0024】

以上まとめると、本発明の具体例において、無線ユーザ端末はデータカードを使用して無線ネットワークにログオンするとともに、先行技術において無線ユーザがインターネットにアクセスする方法を拡充するものである。加えて、インターネットサーフィンの料金は、携帯端末のSIMカードに関係なくデータカードから直接差し引かれる。したがって、たとえユーザが携帯端末を紛失したとしても、そのユーザは他のユーザによるインターネットへの不正アクセスによる不合理な料金を負担することはない。さらに、携帯端末が利用できない場合でも、接続料金は携帯端末のSIMカードに関係ないため、他の携帯端末によってインターネットサーフィンすることができるため、ユーザに大きな利便性をもたらす。加えて、それぞれのデータカードにパスワードが設定されるので、たとえデータカードを紛失したとしても、他のユーザは認証を通過することができないので、データカードのプリペイド額を消費されることはない。データカードの所有者は、データカードのユーザネームに対応するパスワードを通じてネットワークにログオンできるので、データカードの紛失による損害を受けることはなく、ユーザは接続料金に関してのセキュリティが保障される。

【発明を実施するための最良の形態】

【0025】

図1は、本発明によるデータカードを使ったインターネットサーフィンのための典型的な方法を図示したフローチャートである。

【0026】

図2は、本発明の一実施形態によるデータカードの認証を行うAAAシステムを図示したフローチャートである。

【0027】

図3は、本発明の一実施形態によるデータカードの認証を行う携帯電話インテリジェントネットワーク(CIN: Cellphone Intelligent Network)を図示したフローチャートである。

【0028】

図4は、本発明の一実施形態によるデータカードとSIMカードの認証フローチャートである。

【0029】

図5は、本発明の他の実施形態によるデータカードとSIMカードの認証フローチャートである。

【0030】

図6は、本発明の他の実施形態によるデータカードとSIMカードの認証フローチャートである。

【0031】

本発明の原理、特徴及び効果をより理解するため、さらに詳細な技術的解決手段について添付図面及び実施形態を参照する。

【0032】

本発明の実施形態では、認証・認可・アカウントिंग(AAA: Authentication Authorization and Accounting)システム又は携帯電話インテリジェントネットワーク(CIN: Cellphone Intelligent Network)は、ある一定のプリペイド額を含んだデータカードを発行し、ユーザアカウント番号及びパスワードをそれぞれのデータカードに設定する。ユーザは、前記データカードをいつでも購入できるとともに、その有効期限が切れるまではデータカードを使ってインターネットサーフィンを行うことができる。インターネットにアクセスする場合、データカードを発行するAAAシステム又はCINによる認証のため、ユーザは端末を通じて、データカードのユーザアカウント番号及びパスワードを入力する必要がある。これにより、不正アクセスによる正規ユーザへの料金発生を防ぐことができる。図1からわかるように、本発明によるデータカードを使ったインターネットサーフィンの方法は、以下のステップを有している。

10

20

【0033】

S01: 無線通信ネットワークを介してインターネットへログオンする過程で、端末は、パケットデータサービングノード(PDSN: Packet Data Serving Node)/ゲートウェイGPRSサポートノード(GGSN: Gateway GPRS Support Node)を介して、事前に購入したデータカードのユーザアカウント番号及びパスワードに関する情報をAAAシステムに送信する。このデータカードは、無線通信ネットワーク内のAAAシステム又はCINによって発行されたもので、プリペイド額に関する情報を含んでいる。

【0034】

ユーザは、ある一定のプリペイド額を含むデータカードを購入し、これを使ってインターネットサーフィンを行う。したがって、前記データカードは、先行技術においてユーザがインターネットにアクセスする方法を拡充するものである。

30

【0035】

S02: 無線通信ネットワーク内のAAAシステムは、データカードのユーザアカウント番号及びパスワードに関する情報を受信した時に、ユーザアカウント番号に対応するデータカードがAAAシステムによって発行されたものであるかどうかを判定する。そうである場合AAAシステムはデータカードの認証を行い、そうでない場合はCINがデータカードの認証を行う。データカードが認証を通過した場合S03が実行され、そうでない場合端末の接続は拒否される。

【0036】

データカードごとに1つのパスワードが設定されるため、たとえデータカードを紛失したとしても、データカードの所有者でない他のユーザが認証を通過することはできず、データカードのプリペイド額を消費されることはない。一方、データカードの所有者がそのデータカードのユーザアカウント番号及びパスワードを変更しないかぎり、そのユーザアカウント番号及びパスワードを使ってネットワークにログオンできる。したがって、接続料金についてのセキュリティは保障され、ユーザがデータカードの紛失による被害を受けることもない。加えて、ユーザが携帯端末によってネットワークへのログオンを要求した場合には、ネットワークにログオン要求を送信するSIMカードが認証される。したがって、携帯端末を紛失したとしても、不正ユーザによってインターネットへのアクセスに使用されることはないので、携帯端末ユーザのリスクを軽減する。

40

【0037】

50

S 0 3 : A A Aシステムは、端末に割り当てる帯域幅を指示するメッセージをP D S N / G G S Nへ送信するとともに、P D S N / G G S Nは、指示メッセージを受信した時に、対応する帯域幅を端末に割り当てる。

【 0 0 3 8 】

S 0 4 : 端末は、インターネットにログオンし接続される。

【 0 0 3 9 】

S 0 5 : 端末からの切断要求メッセージを受けた時に、P D S N / G G S Nは端末へ送信されたトラフィック量とA A Aシステムへ送信されたトラフィック量を計算する。すなわち、まずA A Aシステムは、トラフィック量から料金を計算する。そして、データカードを発行したA A Aシステム又はC I Nは、データカードのプリペイド額からその料金を差し引く。この後、A A Aシステムはインターネットから端末を切断するように指示するメッセージをP D S N / G G S Nへ送信する。

【 0 0 4 0 】

インターネットサーフィンの料金は、携帯端末のS I Mカードには関係なく、データカードから直接差し引かれる。したがって、たとえユーザが携帯端末を紛失しても、他のユーザによるインターネットへの不正アクセスによって不合理な料金をそのユーザが負担する必要はなく、接続料金についてのセキュリティが保証される。さらに、接続料金は携帯端末のS I Mカードには関係ないので、ユーザの携帯端末が利用できない場合でも、そのユーザは他の携帯端末によってインターネットサーフィンを行うことができ、ユーザに多大な利便性をもたらす。

【 0 0 4 1 】

S 0 6 : P D S N / G G S Nは端末をインターネットから切断し、その端末によるインターネットサーフィンを終了させる。

【 0 0 4 2 】

前記の実施形態のうちS 0 1は、詳細には以下のステップを通して実行される。

【 0 0 4 3 】

S 1 1 : ユーザは、携帯端末クライアント又はP C端末クライアントを通じてダイヤルアップによって、データカードのユーザアカウント番号(たとえば“ 1 2 3 ”)及びパスワード(たとえば、“ 1 3 5 ”)を入力するとともに、インターネットへのアクセス要求を無線基地局へ送信する。ユーザによってダイヤルアップに使われたクライアントが携帯端末クライアントである場合、そのユーザは、データカードのユーザアカウント番号及びパスワードを直接入力し、その後インターネットへのアクセス要求を送信する。ユーザによってダイヤルアップに使われたクライアントがP C端末クライアントである場合、無線ネットワークカードがあらかじめP C端末に挿入されているときに限って、ユーザはデータカードのユーザアカウント番号及びパスワードを入力し、その後インターネットへの接続要求を送信することができる。

【 0 0 4 4 】

S 1 2 : 無線基地局は、受信したデータカードのユーザアカウント番号“ 1 2 3 ”及びパスワード“ 1 3 5 ”を、P D S N / G G S Nのような無線パケットゲートウェイへ送信し、データカードの認証を要求する。

【 0 0 4 5 】

S 1 3 : P D S N / G G S Nは、R a d i u s (ユーザサービスによる遠隔認証ダイヤル: Remote Authentication Dial In user Service) / D i a m e t e r (R a d i u sに代わる次世代A A A)プロトコルの下、アクセス要求メッセージを介して、データカードのユーザアカウント番号“ 1 2 3 ”及びパスワード“ 1 3 5 ”を、A A Aシステムへ送信して、データカードの認証と認可をA A Aシステムに要求する。

【 0 0 4 6 】

S 0 2では、A A Aシステムによるデータカードの認証は、詳細には以下のステップを通して実行される。

【 0 0 4 7 】

10

20

30

40

50

S 2 1 1 : A A Aシステムは、ユーザアカウント番号が“ 1 2 3 ”であるということや、同様にパスワード、有効期限、適用性（たとえば、そのカードが、現ネットワークを通じて、又は現在地において、インターネットサーフィンに使用できるかどうか）、カードの残り金額、といったデータカードの情報をデータベースから取得するとともに、取得された情報中のパスワードが、P D S N / G G S Nから送信されたパスワード“ 1 3 5 ”と一致しているかどうかを判定し、そうである場合S 0 3が実行され、そうでない場合端末の接続は拒否される。

【 0 0 4 8 】

A A Aシステムによるデータカードの認証は、図 2 に示した流れで実行される。図 2 からわかるとおり、本発明の一実施形態においてA A Aシステムによるデータカードの認証過程は、以下のステップを有している。

10

【 0 0 4 9 】

S 2 2 1 : A A Aシステムは、データカードのユーザアカウント番号“ 1 2 3 ”及びパスワード“ 1 3 5 ”をC I Nへ送信し、データカードが正規なものかどうかの確認をC I Nに要求する。

【 0 0 5 0 】

S 2 2 2 : C I Nは、ユーザアカウント番号が“ 1 2 3 ”であるということや、パスワード、有効期限、適用性（たとえば、そのカードが、現ネットワークを通じて、又は現在地において、インターネットサーフィンに使用できるかどうか）、カードの残り金額といったデータカードの情報をデータベースから取得するとともに、取得した情報中に記録されているデータカードのパスワードをA A Aシステムに送信する。

20

【 0 0 5 1 】

S 2 2 3 : A A Aシステムは、C I Nから送信されたパスワードが、P D S N / G G S Nから送信されたパスワード“ 1 3 5 ”と一致するかどうかを判定し、一致した場合S 0 3が実行され、そうでない場合端末接続が拒否される。

【 0 0 5 2 】

図 3 からわかるとおり、本発明の一実施形態によるC I Nによるデータカードの認証過程は、以下のステップを有している。

【 0 0 5 3 】

S 2 3 1 : A A Aシステムは、データカードのユーザアカウント番号“ 1 2 3 ”及びパスワード“ 1 3 5 ”をC I Nへ送信し、データカードが正規なものかどうかの確認をC I Nに要求する。

30

【 0 0 5 4 】

S 2 3 2 : C I Nは、ユーザアカウント番号が“ 1 2 3 ”であるということや、パスワード、有効期限、適用性（たとえば、そのカードが、現ネットワークを通じて、又は現在地において、インターネットサーフィンに使用できるかどうか）、そのカードの残り金額といった、データカードの情報をデータベースから取得するとともに、取得した情報中のパスワードが、A A Aシステムから送信されたパスワード“ 1 3 5 ”と一致するかどうかを判定し、一致した場合S 2 3 3が実行され、そうでない場合端末接続は拒否される。

【 0 0 5 5 】

S 2 3 3 : C I Nは、そのデータカードが正規なものかどうかを示す認証の結果を、Q U E R Y _ U S E R I N F O _ A C C _ R E S Pメッセージを通してA A Aシステムに送信し、その後S 0 3が実行される。

40

【 0 0 5 6 】

前記実施形態のS 0 2では、ユーザによってダイヤルアップに使用されたクライアントが携帯端末クライアントである場合、携帯端末の正当性を保障するため、データカードを認証した時に、携帯端末のS I Mカードに関しても同様に実行される。データカードとS I Mカードの両方が認証を通過した場合、S 0 3が実行される。データカードとS I Mカードのいずれかでも認証を通過しなかった場合、携帯端末の接続は拒否される。データカードがA A Aシステムによって発行されるケースでは、図 4 に示したとおり、本発明の一

50

実施の形態によるデータカードとSIMカードの両方の認証過程は、以下のステップを有している。

【0057】

S241:AAAシステムは、パスワード、有効期限、適用性(たとえば、そのカードが、現ネットワークを通じて、又は現在地において、インターネットサーフィンに使用できるかどうか)、カードの残りプリペイド額、ユーザアカウント番号が“123”である、といったデータカードの情報をデータベースから取得するとともに、取得した情報中のパスワードが、PDSN/GGSNから送信されたパスワード“135”と一致するかどうかを判定し、一致した場合S242が実行され、そうでない場合携帯端末の接続は拒否される。

10

【0058】

S242:AAAシステムは、PDSN/GGSNから送信されたユーザアカウント番号及びパスワードに関する情報から、携帯端末のSIMカードのユーザアカウント番号を得るとともに、様々なシステム間の情報を交換するための専用プロトコルによるQUERY__USERINFO__ACCメッセージを通じてSIMカード番号をCINへ送信し、SIMカードの認証を行うようにCINへ要求する。

【0059】

S243:CINは、SIMカード番号によるSIMカードの情報についてデータベースに問い合わせるとともに、SIMカードの認証を行う。SIMカード番号が認証を通過したならばS244が実行され、そうでない場合CINはSIMカードが不正であることを示すメッセージを送信し、携帯端末の接続は拒否される。

20

【0060】

S244:CINは、データカードとSIMカードの両方が正規であることを示すメッセージをAAAシステムへ送信するとともに、S03が実行される。

【0061】

CINによってデータカードが発行されるケースでは、図5に示したとおり、本発明の他の実施形態によるデータカードとSIMカードの両方の認証の流れは以下のステップを有している。

【0062】

S251:AAAシステムは、データカードが正規であるかどうかの確認をCINに要求するため、データカードのユーザアカウント番号“123”及びパスワード“135”をCINへ送信するとともに、PDSN/GGSNから送信されたユーザアカウント番号及びパスワードに関する情報より携帯端末のSIMカード番号を得る。そして、SIMカードの認証を実行するようCINに要求するため、様々なシステム間の情報を交換するための専用プロトコルによるQUERY__USERINFO__ACCメッセージを通じて、CINへSIMカード番号を送信する

30

【0063】

S252:CINは、ユーザアカウント番号が“123”であるということや、パスワード、有効期限、適用性(たとえば、そのカードが、現ネットワークを通じて、又は現在地において、インターネットサーフィンに使用できるかどうか)、カードの残り金額といったデータカードの情報をデータベースから取得するとともに、取得した情報中のパスワードがPDSN/GGSNから送信されたパスワード“135”と一致するかどうかを判定し、一致すればS253が実行され、そうでなければ携帯端末の接続は拒否される。

40

【0064】

S253:CINは、SIMカード番号によるSIMカードの情報についてデータベースに問い合わせるとともに、SIMカードの認証を行う。SIMカード番号が認証を通過した場合はS254が実行され、そうでない場合は携帯端末の接続は拒否される。

【0065】

S254:CINはデータカードとSIMカードの両方が正規であることを示すメッセージをAAAシステムに送信するとともに、S03が実行される。

50

【 0 0 6 6 】

図 5 に図示した実施形態では、S I Mカードが最初に認証されるか、又はデータカードとS I Mカードが同時に認証される。データカードとS I Mカードのいずれかでも認証を通過しなかった場合、ユーザは携帯端末を通じてインターネットサーフィンを行うことはできない。

【 0 0 6 7 】

C I Nによってデータカードが発行されるケースでは、図 6 に示したとおり、本発明の他の実施形態によるデータカードとS I Mカードの両方の認証の流れは、以下のステップを有している。

【 0 0 6 8 】

S 2 6 1 : A A Aシステムは、データカードが正規かどうかの確認をC I Nに要求するため、データカードのユーザアカウント番号“ 1 2 3 ”及びパスワード“ 1 3 5 ”をC I Nへ送信するとともに、P D S N / G G S Nから送信されたユーザアカウント番号及びパスワードに関する情報から携帯端末のS I Mカード番号を得て、C I NにS I Mカードの認証を行うように要求するため、様々なシステム間の情報を交換するための専用プロトコルによるQ U E R Y _ U S E R I N F O _ A C Cメッセージを通じて、S I Mカード番号をC I Nへ送る。

【 0 0 6 9 】

S 2 6 2 : C I Nは、S I Mカード番号によるS I Mカードの情報についてデータベースに問い合わせるとともに、S I Mカードの認証を行う。S I Mカード番号が認証を通過した場合S 2 6 3 が実行され、そうでなければ携帯端末の接続は拒否される。

【 0 0 7 0 】

S 2 6 3 : C I Nは、ユーザアカウント番号が“ 1 2 3 ”であるということや、パスワード、有効期限、適用性（たとえば、そのカードが、現ネットワークを通じて、又は現在地において、インターネットサーフィンに使用できるかどうか）、カードの残り金額、といったデータカードの情報をデータベースから取得するとともに、取得した情報中のデータカードのパスワードをA A Aシステムへ送信する。

【 0 0 7 1 】

S 2 6 4 : A A Aシステムは、C I Nから送信されたパスワードが、P D S N / G G S Nから送信されたパスワード“ 1 3 5 ”と一致するかどうかを判定し、一致した場合S 0 3 が実行され、そうでない場合携帯端末の接続は拒否される。

【 0 0 7 2 】

データカードのパスワードを認証するとき、A A Aシステム又はC I Nは、データベースから直接又は間接的に得られたデータカードの情報によって、適用性、有効期限、カードの残り金額など、といったカードの情報を含む、データカードの正当性についての認証を実行する。データカードが認証を通過した場合、前記認証過程に従ってS 0 3 が実行される、又はさらにS I Mカードも認証される。そうでない場合、A A Aシステムは端末接続を拒否するか、又はC I Nが、データカードが不正であることを示す認証結果をA A Aシステムへ送信するとともに、A A Aシステムは端末接続を拒否する。図 2 及び図 6 に示した認証過程において、データカードの正当性がA A Aシステムによる認証を必要とする場合、S 2 2 2 及びS 2 6 3 において、C I Nは同様にデータカードの正当性に関する情報をA A Aシステムに送信する。

【 0 0 7 3 】

前記の実施形態において、S 0 2 とS 0 3 の間、データカードを発行したA A Aシステム又はC I Nは、データカードに保存されたある一定の金額に関して情報を設定する。データカードがA A Aシステムによって発行された場合、A A Aシステムは、ある一定の金額を直接データカードに保存する。データカードがC I Nによって発行された場合、A A AシステムはA U T H _ P P _ A C Cメッセージを介してデータカードにある一定額を保存するための要求をC I Nへ送信する。C I Nはその要求に従って対応する額を保存するとともに、ある金額の保存が成功したことを示すメッセージをA A Aシステムに返信する

10

20

30

40

50

。

【0074】

さらに、前記の実施形態では、S02とS03の間、AAAシステムはデータカードの残り金額に関する問い合わせ、かつそのプリペイド額によって支払うことのできるトラフィック量を計算するとともに、そのデータカードで支払い可能なトラフィック量に関する情報をPDSN/GGSNに送信する。S04とS05の間、PDSN/GGSNは端末に送信されたトラフィック量を計算する。トラフィック量が、データカードの金額で支払うことのできるトラフィック量より多い又は等しい場合、PDSN/GGSNは端末を切断し、端末によるインターネットサーフィンを終了させる。一方で、S04とS05の間、PDSN/GGSNは、端末に送信されたトラフィック量をリアルタイムに計算すると

10

【0075】

前記の実施形態において、S05は以下のように実行される。

【0076】

ユーザが、クライアント端末を通じて切断要求をPDSN/GGSNに送信した場合、PDSN/GGSNは、端末に送信されたトラフィック量を計算するとともに、そのトラフィック量をAAAシステムに送信する。データカードがAAAシステムによって発行された場合、AAAシステムはPDSN/GGSNから送信されたトラフィック量に従って接続料金を計算するとともに、データカードのプリペイド額から接続料金を差し引き、インターネットからの端末の切断を指示するメッセージをPDSN/GGSNへ送信する。データカードがCINによって発行された場合、AAAシステムはPDSN/GGSNから送信されたトラフィック量に従って接続料金を計算するとともに、データカードの金額から接続料金を差し引く要求をCINへ送信する。

20

CINはデータカードのプリペイド額から相当する接続料金を差し引き、料金が差し引かれたことを示すメッセージをAAAシステムへ返信する。そして、AAAシステムはイン

30

。

【0077】

S05において接続料金を差し引く過程から、データカードがAAAシステムによって発行された場合、AAAシステムは接続料金をデータカードから直接差し引く。先行技術において接続料金を差し引く過程と比較すると、AAAシステムはサービス料金を計算するとともに、サービス料金を差し引くようCINに要求し、CINは対応するサービス料金を差し引き、サービス料金が差し引かれたことを示すメッセージを返信することによって、システム間の対話を減少し、サービス手続きを単純化する結果、ネットワーク上の負荷を緩和し、ユーザがインターネットにアクセスする時間を節約し、ユーザに利便性をも

40

【0078】

本発明は、本発明の一実施形態によって記載されるとともに図示された。前記実施形態は単なる実施例に過ぎず限定するものではなく、本発明はそれらに限定されてはならないこと、特許請求の範囲によって定義される本発明の趣旨及び範囲から逸脱しない限り、前記記載及び図面の記載から様々な改良や変化が可能であることは、当業者に自明である。

【図面の簡単な説明】

【0079】

【図1】図1は、本発明によるデータカードを使ったインターネットサーフィンのための典型的な方法を図示したフローチャートである。

50

【図2】図2は、本発明の一実施形態によるデータカードの認証を行うAAAシステムを図示したフローチャートである。

【図3】図3は、本発明の一実施形態によるデータカードの認証を行う携帯電話インテリジェントネットワーク(CIN: Cellphone Intelligent Network)を図示したフローチャートである。

【図4】図4は、本発明の一実施形態によるデータカードとSIMカードの認証フローチャートである。

【図5】図5は、本発明の他の実施形態によるデータカードとSIMカードの認証フローチャートである。

【図6】図6は、本発明の他の実施形態によるデータカードとSIMカードの認証フローチャートである。

10

【符号の説明】

【0080】

S01 ユーザアカウント及びパスワード情報を無線通信ネットワークに送信するステップ

S02 無線通信ネットワークがユーザ無線装置に対して認証を行うステップ

S03 ユーザ無線装置に帯域幅を割り当てるステップ

S04 ユーザ無線装置がインターネットにログオンしアクセスするステップ

S05 ユーザ無線装置からのログオフ要求に対して、料金を計算するステップ

S06 端末によるインターネットサーフィンを終了させるステップ

20

S07 ユーザ無線装置に対する接続を拒否するステップ

S221 データカードの認証を要求するメッセージを送信するステップ

S222 データカードのパスワードに関する情報を送信するステップ

S223 データカードが正規であるかどうかを判定するステップ

S241 SIMカードの認証を要求するメッセージを送信するステップ

S242 データカードのパスワードに関する情報を送信するステップ

S243 SIMカードが正規であるかどうかを判定するステップ

S244 データカード及びSIMカードが正規であることを示すメッセージを送信するステップ

S251 SIMカード及びデータカードの認証を要求するメッセージ送信するステップ

30

S252 データカードが正規であるかどうかを判定するステップ

S253 SIMカードが正規であるかどうかを判定するステップ

S254 データカード及びSIMカードが正規であることを示すメッセージを送信するステップ

S261 SIMカード及びデータカードの認証を要求するメッセージを送信するステップ

S262 SIMカードが正規であるかどうかを判定するステップ

S263 データカードのパスワードに関する情報を送信するステップ

S264 データカードが正規であるかどうかを判定するステップ

40

【 図 1 】

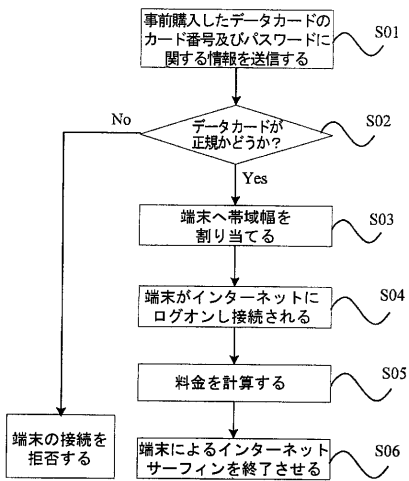


Fig. 1

【 図 2 】

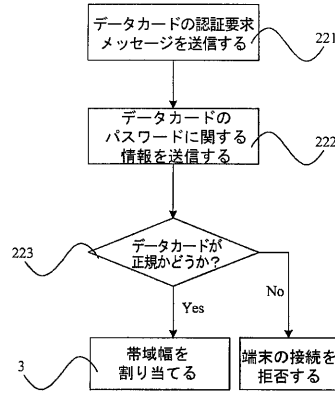


Fig. 2

【 図 3 】

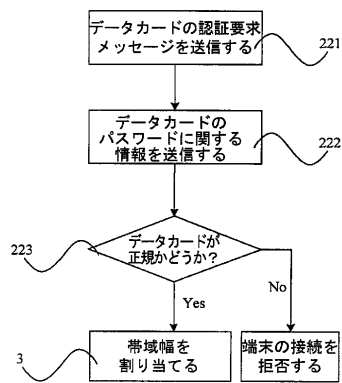


Fig. 3

【 図 4 】

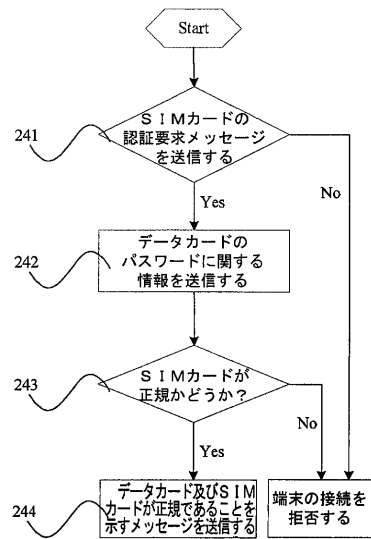


Fig. 4

【 図 5 】

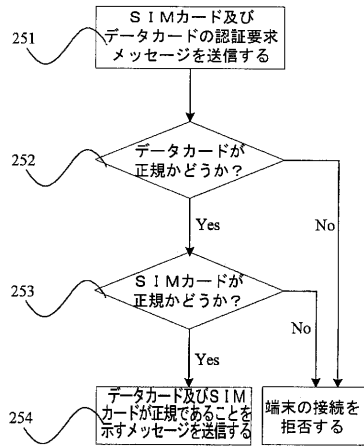


Fig. 5

【 図 6 】

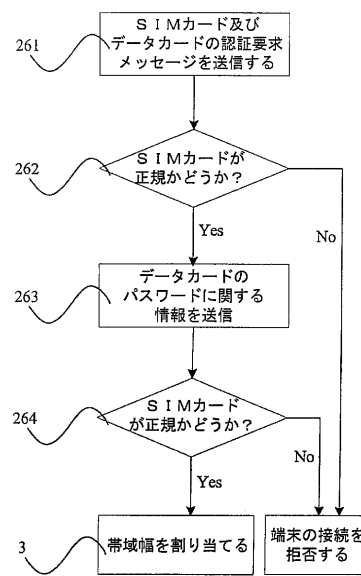


Fig. 6

【 手続 補正書 】

【 提出日 】 平成20年7月22日 (2008.7.22)

【 手続 補正 1 】

【 補正対象書類名 】 特許請求の範囲

【 補正対象項目名 】 全文

【 補正方法 】 変更

【 補正の内容 】

【 特許請求の範囲 】

【 請求項 1 】

インターネットに対するプリペイドユーザの無線アクセス方法であって、
無線ユーザ端末が無線通信ネットワークを介してインターネットにログオンする場合、無線ユーザ端末から送信されたユーザアカウント番号及びパスワードに関する情報を無線通信ネットワークによって受信するステップと、

前記無線通信ネットワークによって無線ユーザ端末の認証を行うステップと、
 を具備し、

ユーザアカウント番号、パスワード及びプリペイド額に関する情報を、無線通信ネットワークにあらかじめ保持し、

前記無線ユーザ端末が認証を通過した場合、無線ユーザ端末に帯域幅を割り当て、そうでない場合、無線ユーザ端末の接続を拒否することを特徴とする無線アクセス方法。

【 請求項 2 】

前記無線ユーザ端末から切断要求メッセージを受信すると、無線通信ネットワークによって料金を計算し、プリペイド額から前記料金を差し引くステップと、
 を具備することを特徴とする請求項 1 に記載の無線アクセス方法。

【 請求項 3 】

前記無線ユーザ端末によって送信されたユーザアカウント番号及びパスワードに関する情

報を受信するステップは、無線ユーザ端末が無線通信ネットワークを介してインターネットへログオンする場合、無線ユーザ端末から送信されたユーザアカウント番号及びパスワードに関する情報を、無線通信ネットワーク内の無線パケットゲートウェイによって受信するステップと、

ユーザアカウント番号及びパスワードに関する情報を、無線パケットゲートウェイから認証・認可・アカウントイング（AAA：Authentication Authorization and Accounting）システムへ送信するステップと、

を具備することを特徴とする請求項 1 に記載の無線アクセス方法。

【請求項 4】

前記無線ユーザ端末の認証を行うステップは、

ユーザアカウント番号及びパスワードに関する情報を、AAAシステムによってデータベースから取得するステップと、

取得した情報に記録されているパスワードに関する情報が、無線ユーザ端末から送信されたパスワードに関する情報と一致するかどうかを判定するステップと、

一致した場合、無線ユーザ端末に帯域幅を割り当てるステップと、

一致しなかった場合、端末の接続を拒否するステップと、

を具備することを特徴とする請求項 3 に記載の無線アクセス方法。

【請求項 5】

無線ユーザ端末の認証を行うステップは、

無線ユーザ端末の認証を行うため、ユーザアカウント番号及びパスワードに関する情報を保持する認証要求メッセージをAAAシステムから携帯電話インテリジェントネットワークへ送信するステップと、

ユーザアカウント番号に従って、ユーザアカウント番号及びパスワードに関する情報を、携帯電話インテリジェントネットワークによってデータベースから取得するステップと、

取得した情報に記録されているパスワードに関する情報を、AAAシステムへ送信するステップと、

携帯電話インテリジェントネットワークから送信されたパスワードに関する情報が、AAAシステムによって無線ユーザ端末から送信されたパスワードに関する情報と一致するかどうかを判定するステップと、

携帯電話インテリジェントネットワークから送信されたパスワードに関する情報が、送信されたパスワードに関する情報と一致した場合、無線ユーザ端末に帯域幅を割り当てるステップと、

一致しなかった場合、無線ユーザ端末の接続を拒否するステップと、

を具備することを特徴とする請求項 3 に記載の無線アクセス方法。

【請求項 6】

前記無線ユーザ端末の認証を行うステップは、

無線ユーザ端末の認証を行うため、ユーザアカウント番号及びパスワードに関する情報を保持する認証要求メッセージを、AAAシステムから携帯電話インテリジェントネットワークへ送信するステップと、

ユーザアカウント番号に従って、ユーザアカウント番号及びパスワードに関する情報を、データベースから携帯電話インテリジェントネットワークによって取得するステップと、

取得した情報に記録されているパスワードに関する情報が、無線ユーザ端末から送信されたパスワードに関する情報と一致するかどうかを判定するステップと、

インテリジェントネットワークが取得した情報に記録されているパスワードに関する情報が、無線ユーザ端末から送信されたパスワードに関する情報と一致した場合、

前記無線ユーザ端末が正規なものであることを示すメッセージを、携帯電話インテリジェントネットワークからAAAシステムへ送信するとともに、無線ユーザ端末に帯域幅を割り当てるステップと、

一致しなかった場合、無線ユーザ端末が不正であることを示すメッセージを、携帯電話インテリジェントネットワークからAAAシステムに送信するとともに、無線ユーザ端末の接続を拒否するステップと、

を具備することを特徴とする請求項3に記載の無線アクセス方法。

【請求項7】

さらに前記無線ユーザ端末のSIMカードの認証を行うステップは、無線ユーザ端末及びSIMカードの両方が認証を通過した場合、無線ユーザ端末に帯域幅を割り当てるステップと、

認証を通過しなかった場合、無線ユーザ端末を拒否するステップと、

を具備することを特徴とする請求項3に記載の無線アクセス方法。

【請求項8】

前記無線ユーザ端末の認証を行うステップは、

ユーザアカウント番号に従って、データベースからユーザアカウント番号及びパスワードに関する情報をAAAシステムによって取得するステップと、

取得した情報に記録されているパスワードに関する情報が、無線ユーザ端末から送信されたパスワードに関する情報と一致するかどうかを判定するステップと、

一致した場合、AAAシステムによって無線ユーザ端末のSIMカード番号を得るステップと、

SIMカードの認証を行うため、SIMカード番号を運ぶ認証要求メッセージを携帯電話インテリジェントネットワークへ送信するステップと、

携帯電話インテリジェントネットワークによってSIMカードの情報に関するデータベースを問い合わせるステップと、

前記SIMカードが正規なものであるかどうかを判定するステップと

正規であった場合、SIMカードが正規であることを示すメッセージを、携帯電話インテリジェントネットワークからAAAシステムへ送信するとともに、無線ユーザ端末に帯域幅を割り当てるステップと、

不正であった場合、SIMカードが不正であることを示すメッセージを、携帯電話インテリジェントネットワークからAAAシステムへ送信するとともに、無線ユーザ端末の接続を拒否するステップと、

を具備することを特徴とする請求項7に記載の無線アクセス方法。

【請求項9】

前記無線ユーザ端末の認証を行うステップは、

AAAシステムによって無線ユーザ端末のSIMカード番号を得るステップと、

無線ユーザ端末及びSIMカードの認証を行うため、SIMカード番号と同様にユーザアカウント番号及びパスワードを保持する認証要求メッセージを携帯電話インテリジェントネットワークへ送信するステップと、

ユーザアカウント番号に従って無線ユーザ端末の情報をデータベースから携帯電話インテリジェントネットワークによって取得するステップと、

取得した情報に記録されているパスワードに関する情報が、無線ユーザ端末から送信されたパスワードに関する情報と一致するかどうかを判定するステップと、

一致しなかった場合、無線ユーザ端末が不正であることを示すメッセージを携帯電話インテリジェントネットワークからAAAシステムへ送信するとともに、無線ユーザ端末の接続を拒否するステップと、

一致した場合、携帯電話インテリジェントネットワークによってSIMカードの情報に関するデータベースに問い合わせ、SIMカードが正規なものであるかどうかを判定するステップと、

正規であった場合、無線ユーザ端末とSIMカードの両方が正規であることを示すメッセージを、携帯電話インテリジェントネットワークからAAAシステムへ送信するとともに、無線ユーザ端末に帯域幅を割り当てるステップと、

正規でなかった場合、SIMカードが不正であることを示すメッセージを、携帯電話イ

ンテリジェントネットワークから A A A システムへ送信するとともに、無線ユーザ端末の接続を拒否するステップと、

を具備することを特徴とする請求項 7 に記載の無線アクセス方法。

【請求項 1 0】

前記無線ユーザ端末の認証を行うステップは、

A A A システムによってインターネットへアクセスするための要求メッセージから S I M カード番号を得るステップと、

無線ユーザ端末及び S I M カードの認証を行うため、S I M カードと同様に、ユーザアカウント番号及びパスワードに関する情報を保持する認証要求メッセージを携帯電話インテリジェントネットワークへ送信するステップと、

携帯電話インテリジェントネットワークによって、S I M カードの情報に関するデータベースに問い合わせるステップと、

前記 S I M カードが正規なものであるかどうかを判定するステップと、

正規でなかった場合、S I M カードが不正であることを示すメッセージを、携帯電話インテリジェントネットワークから A A A システムへ送信するとともに、無線ユーザ端末の接続を拒否するステップと、

正規であった場合、携帯電話インテリジェントネットワークによって、ユーザアカウント番号に従って、無線ユーザ端末の情報をデータベースから取得するとともに、取得した情報に記録されているパスワードに関する情報を A A A システムへ送信するステップと、

A A A システムによって、携帯電話インテリジェントネットワークから送信されたパスワードに関する情報が、無線ユーザ端末から送信されたパスワードに関する情報と一致するかどうかを判定するステップと、

一致した場合、無線ユーザ端末に帯域幅を割り当てるステップと、

一致しなかった場合、無線ユーザ端末の接続を拒否するステップと、

を具備することを特徴とする請求項 7 に記載の無線アクセス方法。

【請求項 1 1】

さらに前記無線ユーザ端末を認証する場合、無線ユーザ端末の正当性を認証するステップと、

適応性と有効期限について無線ユーザ端末を認証するステップと、

無線ユーザ端末が、正当性の認証を通過した場合、端末によってインターネットにログインし、インターネットサーフィンを行うステップが実行するステップと、通過しなかった場合、端末の接続を拒否するステップと、

を具備することを特徴とする請求項 3 に記載の無線アクセス方法。

【請求項 1 2】

無線ユーザ端末を認証するステップと無線ユーザ端末に帯域幅を割り当てるステップの間には、

金額の保存に関する情報を設定するステップ

をさらに具備することを特徴とする請求項 3 に記載の無線アクセス方法。

【請求項 1 3】

金額の保存に関する情報の設定を行うステップは、

データカードの金額を保存するための要求を A A A システムから携帯電話インテリジェントネットワークへ送信するステップと、

前記要求に従ってユーザアカウント番号に対するプリペイド額を携帯電話インテリジェントネットワークによって保存するステップと、

プリペイド額が保存されたことを示すメッセージを A A A システムへ送信するステップと、

を具備することを特徴とする請求項 1 2 に記載の無線アクセス方法。

【請求項 1 4】

前記ユーザアカウントの残り金額が指定額より少ない又は等しいことを無線パケットゲートウェイから検出した場合、無線ユーザ端末によるインターネットサーフィンを終了さ

せるステップ

をさらに具備することを特徴とする請求項 1 3 に記載の無線アクセス方法。

【請求項 1 5】

無線ユーザ端末を認証するステップと無線ユーザ端末に帯域幅を割り当てるステップの間は、

データカードの残り金額を A A A システムによって問い合わせるステップと、

前記金額から支払い可能なトラフィック量を計算するステップと、

支払い可能なトラフィック量に関する情報を無線パケットゲートウェイへ送信するステップと、

無線パケットゲートウェイによって、前記端末へ送信されたトラフィック量を計算するステップと、

トラフィック量が、支払い可能なトラフィック量より多い又は等しい場合、無線ユーザ端末によるインターネットサーフィンを終了させるステップと、

を具備することを特徴とする請求項 1 から請求項 1 0 のいずれか 1 項に記載の無線アクセス方法。

【請求項 1 6】

無線ユーザ端末を切断した時に、無線ユーザ端末へ送信されたトラフィック量に従ってプリペイド額から接続料金を差し引くステップ

をさらに具備することを特徴とする請求項 3 に記載の無線アクセス方法。

【請求項 1 7】

プリペイド額から接続料金を差し引くステップは、

無線パケットゲートウェイによって、無線ユーザ端末に送信されたトラフィック量を計算するステップと、

前記トラフィック量を A A A システムへ送信し、A A A システムによってトラフィック量に従ってプリペイド額から接続料金を差し引くステップと、

を具備することを特徴とする請求項 1 6 に記載の無線アクセス方法。

【請求項 1 8】

プリペイド額から接続料金を差し引くステップは、

無線パケットゲートウェイによって無線ユーザ端末へ送信されたトラフィック量を計算し、A A A システムへトラフィック量を送信するステップと、

A A A システムによって前記トラフィック量から接続料金を計算し、プリペイド額から接続料金を差し引くための要求を、携帯電話インテリジェントネットワークへ送信するステップと、

携帯電話インテリジェントネットワークによって、プリペイド額から接続料金を差し引くステップと、

を具備することを特徴とする請求項 1 6 に記載の無線アクセス方法。

【請求項 1 9】

プリペイドユーザがインターネットに無線アクセスするためのシステムであって、

無線ユーザ端末が無線通信ネットワークを介してインターネットにログオンする場合、無線ユーザ端末から送信されたユーザアカウント番号およびパスワードに関する情報を受信するために構成された無線通信ネットワークを具備し、

ユーザアカウント番号、情報およびプリペイド額に関する情報は、無線通信ネットワークにあらかじめ保持され、無線ユーザ端末を認証するとともに、無線ユーザ端末が認証を通過した場合、無線ユーザ端末に帯域幅を割り当てる、またはそうでない場合、無線ユーザ端末の接続を拒否することを特徴とする無線アクセスシステム。

【請求項 2 0】

無線パケットゲートウェイ、認証・認可・アカウントティング (A A A : Authentication Authorization and Accounting) システムおよびデータベースをさらに具備し、

無線ユーザ端末が無線通信ネットワークを介してインターネットにログオンする場合、無線パケットゲートウェイは、無線ユーザ端末から送信されたユーザアカウント番号および

パスワードに関する情報を受信するために構成され、

A A Aシステムは、無線ユーザ端末を認証するために構成されるとともに、無線ユーザ端末が認証を通過した場合、無線ユーザ端末に帯域幅を割り当てるか、またはそうでない場合、無線ユーザ端末の接続を拒否するとともに、

ユーザアカウント番号、パスワードおよびプリペイド額はデータベースに保持されることを特徴とする請求項 19 記載の無線アクセスシステム。

【請求項 21】

A A Aシステムは、ユーザアカウント番号およびパスワードに関する情報をユーザアカウント番号に従ってデータベースから取得するためにさらに構成され、取得された情報に記録されたパスワードに関する情報が、無線ユーザ端末から送信されたパスワードに関する情報と一致するかどうか判定するとともに、一致した場合、無線ユーザ端末に帯域幅が割り当てられるか、またはそうでない場合、端末の接続は拒否されることを特徴とする請求項 20 に記載の無線アクセスシステム。

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】0003

【補正方法】変更

【補正の内容】

【0003】

社会の発展につれて、社会生活、経済、科学研究、国家防衛など、様々な情報が常に更新されるとともに、正確な情報が行き交い様々な分野でますます使われている。個人又は集団の発展は、他の成功を頼りにしなければならない。したがって情報を完全に取得する方法は、重要な問題の1つとなる。そこに、情報を取得するための様々な手段が存在する。とりわけ、現在、人々にとってネットワークは、便利で迅速にかつ詳細な方法で情報を取得するには最良であり、テレビや新聞といったメディアよりもポピュラーである。現在、ユーザの多くは、広いカバレッジ及び高帯域幅で利点のある有線ブロードバンドネットワークを通して情報を取得する。しかし、有線ブロードバンドネットワークは、固定した場所によるPCからアクセスのみが可能である。その結果、ユーザはインターネットサーフィンをするため、固定した場所にPCを持ち運ばなければならず、非常に不便である。同様に、ユーザは、有線ブロードバンドネットワークに比べてログオンできる場所がより自由な無線ローカルエリアネットワークを通して、情報を取得する。しかし、これもカバレッジが狭いことがユーザにとって不便の原因になっている。社会経済の迅速な発展の結果としての携帯端末の高い普及率と同様に、無線ネットワークの持続的な進歩の結果としての広いカバレッジと他のネットワークを通じた携帯性の点から、無線ネットワークの重要な長所により、様々な分野の人々にとって、携帯端末又は無線ネットワークカード（PCは携帯端末に挿入されるか、またはPCは携帯端末のSIMカードを通して無線ネットワークに接続される）によって、無線ネットワークを通して情報を取得することが、最善の選択になる。

【手続補正 3】

【補正対象書類名】図面

【補正対象項目名】図1

【補正方法】変更

【補正の内容】

【図 1】

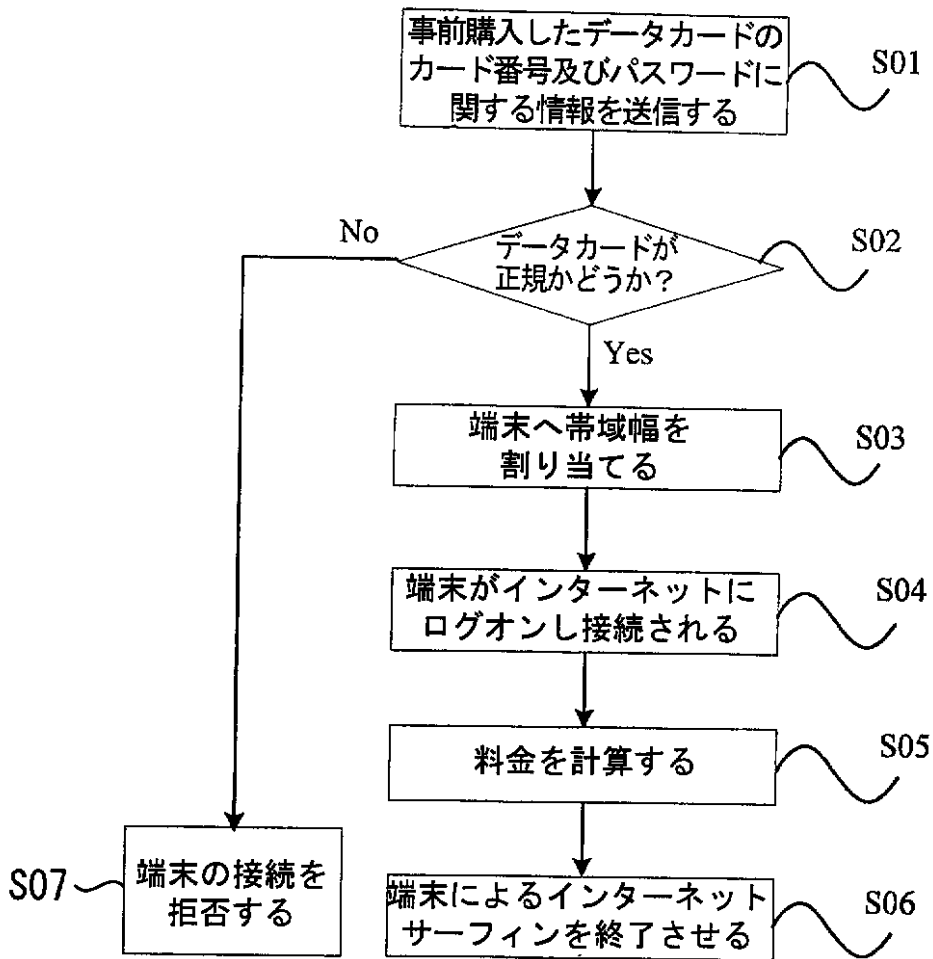


Fig. 1

- 【手続補正 4】
- 【補正対象書類名】 図面
- 【補正対象項目名】 図 2
- 【補正方法】 変更
- 【補正の内容】

【図2】

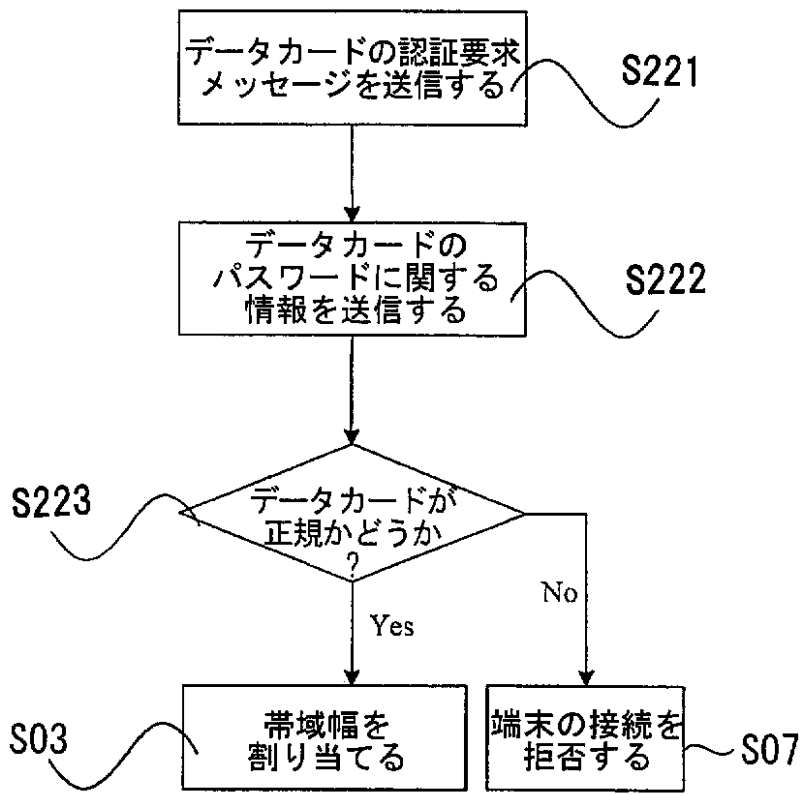


Fig. 2

【手続補正5】

【補正対象書類名】図面

【補正対象項目名】図3

【補正方法】変更

【補正の内容】

【図3】

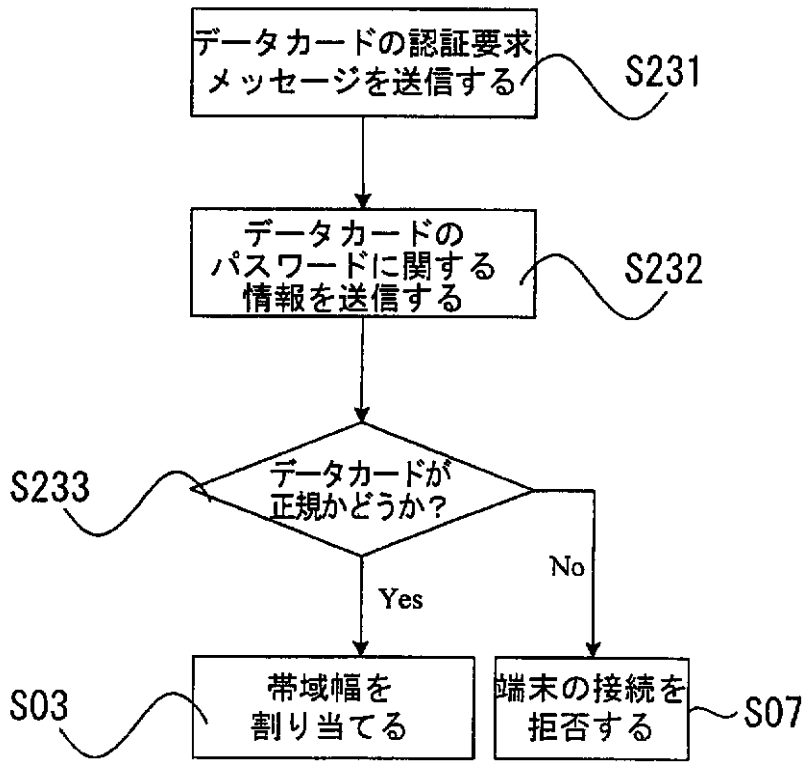


Fig. 3

【手続補正6】

【補正対象書類名】図面

【補正対象項目名】図4

【補正方法】変更

【補正の内容】

【図4】

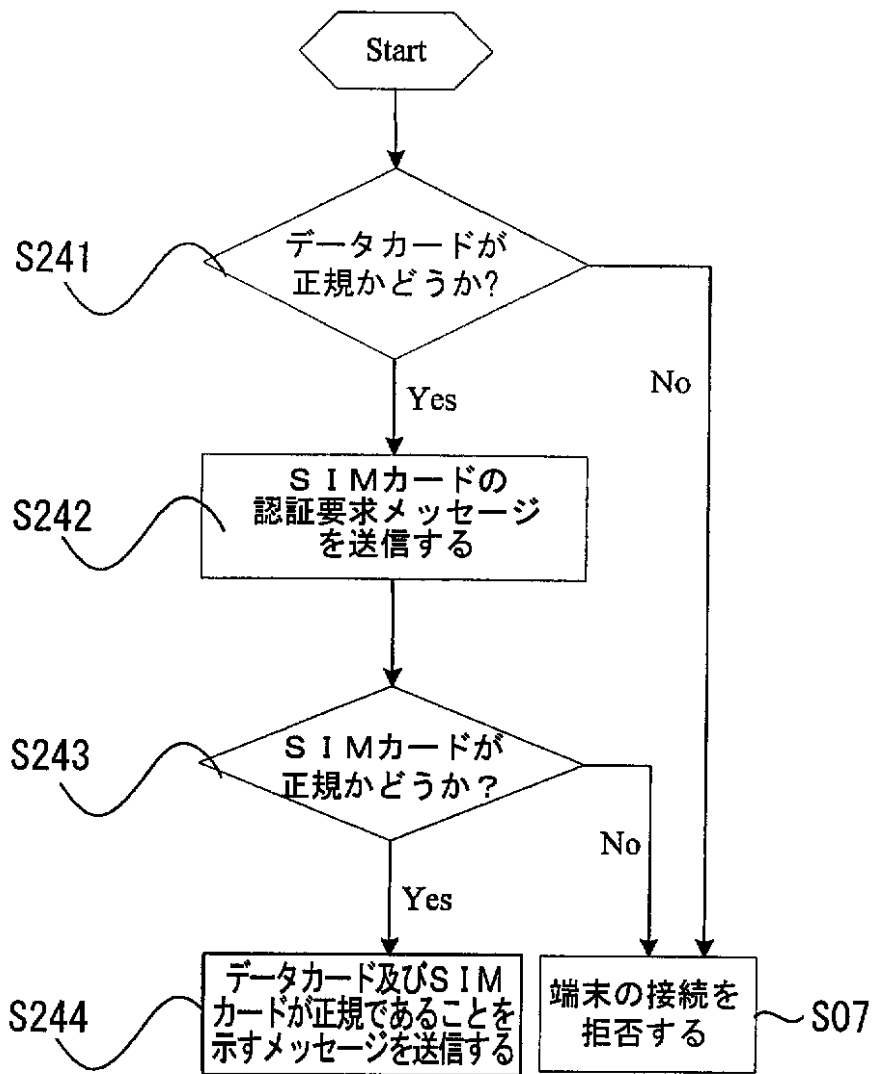


Fig. 4

【手続補正7】

【補正対象書類名】図面

【補正対象項目名】図5

【補正方法】変更

【補正の内容】

【 図 5 】

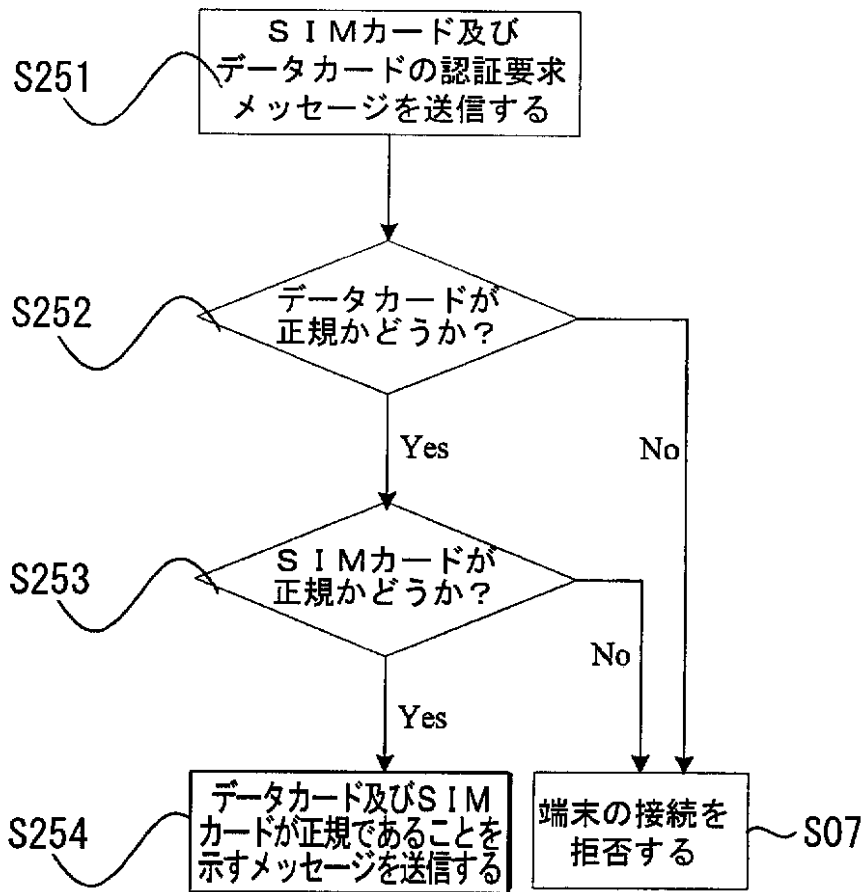


Fig. 5

【 手続補正 8 】

【 補正対象書類名 】 図面

【 補正対象項目名 】 図 6

【 補正方法 】 変更

【 補正の内容 】

【 図 6 】

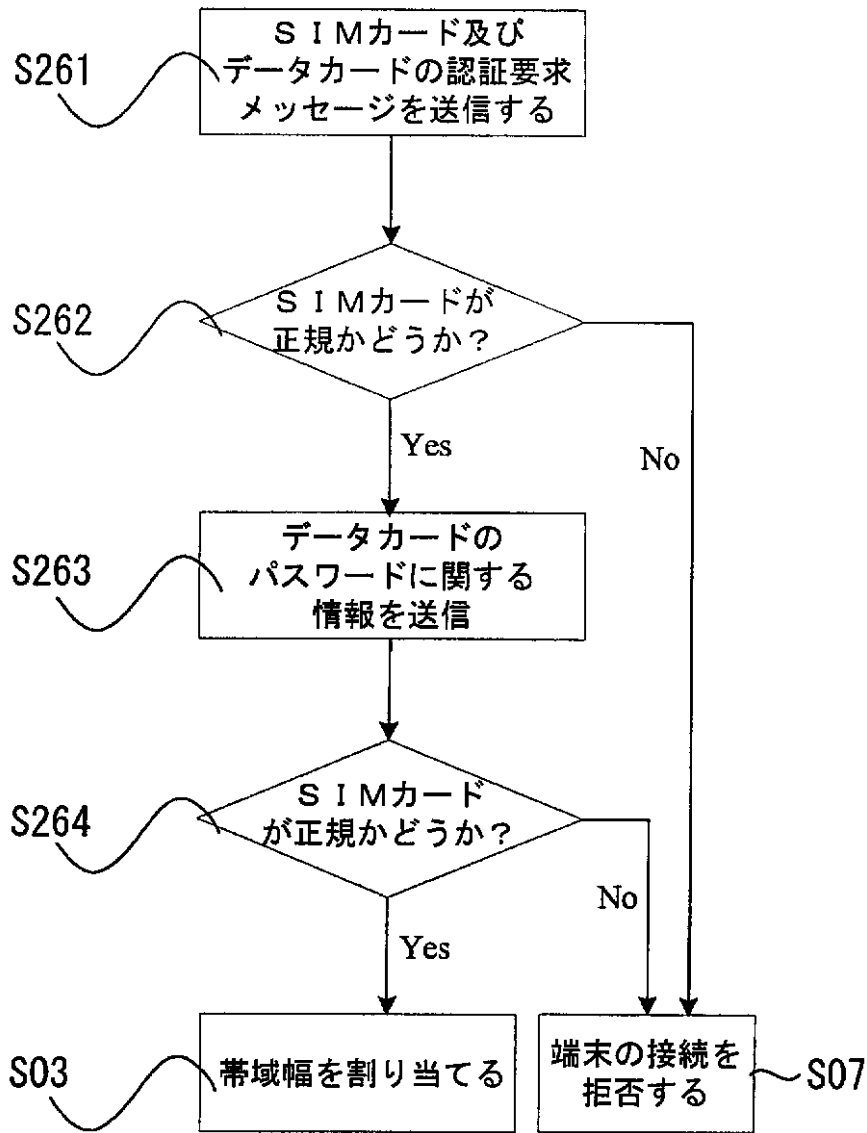


Fig. 6


【 国际调查报告 】

INTERNATIONAL SEARCH REPORT		International application No. PCT/CN2006/003161
A. CLASSIFICATION OF SUBJECT MATTER		
H04L9/32(2007.01)i		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols)		
IPC: H04L,H04B,H04Q		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
WPI,EPODOC,PAJ,CPRS,CNKI:WIRELESS,MOBILE,LOGON,ACCOUNT,PASSWORD,PREPAID,AUTHENTI+,AUTHORI+,IDENTIF+,COST,MONEY		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim
X	US2004225887A1(DOUGLAS R. O'NEIL ET-AL) 11.Nov.2004 (11.11.2004) Description paragraph 4 line 13-14, paragraph 42,43, 47,67,69, figures 2,3	1, 2, 16
A		3-15,17,18
A	WO2004111809A1(BRILLOIN TELEFON AB L M ET-AL)23.Dec.2004 (23.12.2004) The whole document	1-18
A	CN1323500A(AT MOBILE COM CORP) 21.Nov.2001 (21.11.2001) The whole document	1-18
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
<p>* Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"B" earlier application or patent but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&"document member of the same patent family</p>		
Date of the actual completion of the international search 10.Feb.2007(10.02.2007)		Date of mailing of the international search report 08 · MAR 2007 (03 · 2007)
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R. China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451		Authorized officer SUN Wenhan Telephone No. 86-10-62084497

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2006/003161

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US2004225887A1	11.11.2004	None	
WO2004111809A1	23.12.2004	AU2003239059 A1	04.01.2005
		CN1788244 A	14.06.2006
		EP1634133 A1	15.03.2006
		US2006094403 A1	04.05.2006
CN1323500A	21.11.2001	AU5923499 A	01.05.2000
		BRPI9914559 A	26.06.2001
		CA2347020 A1	20.04.2000
		EP1121825 A1	08.08.2001
		JP2002528016T	27.08.2002
		US6393269 B1	21.05.2002
		US2002111153 A1	15.08.2002
		WO0022871 A1	20.04.2000
		KR20010085921 A	07.09.2001

国际检索报告		国际申请号 PCT/CN2006/003161
A. 主题的分类 H04L9/32(2007.01)i 按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类		
B. 检索领域 检索的最低限度文献(标明分类系统和分类号) IPC: H04L,H04B,H04Q 包含在检索领域中的除最低限度文献以外的检索文献		
在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用)) WPI,EPODOC,PAJ, CPRS,CNKI: 无线, 移动, 登录, 帐号, 账号, 密码, 预付, 鉴权, 认证, 费, 款 WIRELESS,MOBILE,LOGON,ACCOUNT,PASSWORD,PREPAID,AUTHENTI+,AUTHORI+,IDENTIF+,COST,MON EY		
C. 相关文件		
类型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	US2004225887A1(DOUGLAS R. O'NEIL ET-AL) 11.11 月 2004 (11.11.2004) 说明书第 4 段第 13-14 行, 第 42、43、47 段, 第 67、69 段, 附图 2、3	1, 2, 16
A		3-15,17,18
A	WO2004111809A1(艾利森电话股份有限公司)23.12 月 2004 (23.12.2004) 全文	1-18
A	CN1323500A(奥本维夫技术公司) 21.11 月 2001 (21.11.2001) 全文	1-18
<input type="checkbox"/> 其余文件在 C 栏的续页中列出。 <input checked="" type="checkbox"/> 见同族专利附件。		
* 引用文件的具体类型: "A" 认为不特别相关的表示了现有技术一般状态的文件 "E" 在国际申请日的当天或之后公布的在先申请或专利 "L" 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 "O" 涉及口头公开、使用、展览或其他方式公开的文件 "P" 公布日先于国际申请日但迟于所要求的优先权日的文件 "T" 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 "X" 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 "Y" 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 "&" 同族专利的文件		
国际检索实际完成的日期 10.2 月 2007 (10.02.2007)		国际检索报告邮寄日期 08.03.2007 (08.03.2007)
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号: (86-10)62019451		受权官员 孙文涵 电话号码: (86-10)62084497 

国际检索报告 关于同族专利的信息		国际申请号 PCT/CN2006/003161	
检索报告中引用的 专利文件	公布日期	同族专利	公布日期
US2004225887A1	11.11.2004	无	
WO2004111809A1	23.12.2004	AU2003239059 A1	04.01.2005
		CN1788244 A	14.06.2006
		EP1634133 A1	15.03.2006
		US2006094403 A1	04.05.2006
CN1323500A	21.11.2001	AU5923499 A	01.05.2000
		BRPI9914559 A	26.06.2001
		CA2347020 A1	20.04.2000
		EP1121825 A1	08.08.2001
		JP2002528016T	27.08.2002
		US6393269 B1	21.05.2002
		US2002111153 A1	15.08.2002
		WO0022871 A1	20.04.2000
		KR20010085921 A	07.09.2001

フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), EP(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW

Fターム(参考) 5K067 AA30 DD17 DD53 EE02 EE16 HH22 HH23 KK15
5K201 AA09 BC23 BD10 CB13 EA05 EA07 FA07