(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-171069
(P2004-171069A)
(43)公開日　平成16年6月17日(2004.6.17)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 15/00	G06F 15/00	330Z	5B085
G06F 13/00	G06F 13/00	520C	5K067
H04Q 7/38	H04B 7/26	109R	

審査請求 未請求　請求項の数 16　ＯＬ　（全 16 頁）

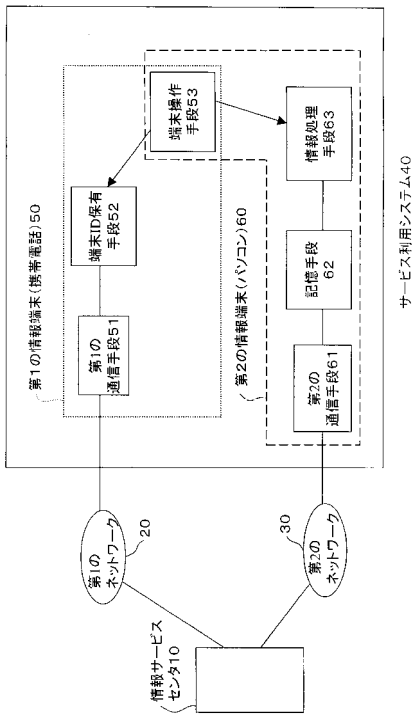
(21)出願番号　特願2002-332924(P2002-332924)
(22)出願日　平成14年11月15日(2002.11.15)

(71)出願人　000002945
オムロン株式会社
京都市下京区塩小路通堀川東入南不動堂町
８０１番地
(74)代理人　100083024
弁理士　高橋　昌久
(74)代理人　100103986
弁理士　花田　久丸
(72)発明者　安藤　丹一
京都市下京区塩小路通堀川東入南不動堂町
８０１番地　オムロン株式会社内

Ｆターム(参考)　5B085 AA08 AE03 AE04
5K067 AA32 BB04 BB21 DD04 DD17
DD29 EE02 EE12 EE16 FF04
HH22 HH32 HH36 KK13 KK15

(54)【発明の名称】認証済み情報提供システムおよび情報配信方法

(57)【要約】
【課題】真正な情報利用者からのアクセスであるかを情報利用者自身が簡便な手段で情報提供者に知らせ、情報提供者はそれに基づき認証を行ない、通信効率の比較的劣る通信システムを用いて認証が行なわれても、大容量の情報配信は通信効率の良い別の通信システムを経由して配信を受ける情報提供システムを構築することである。
【解決手段】複数のサービス利用システムから通信網経由で送られた端末ＩＤをサービス情報センタで認証後、当該サービス情報センタから当該サービス利用システムに特定のコンテンツ情報を配信する認証済み情報提供システムにおいて、前記サービス利用システムが、認証力の優れた端末ＩＤを持つ第１の情報端末と、当該第１の情報端末とは認証力が異なる第２の情報端末から構成されており、前記情報サービスセンタが前記第１の情報端末からの前記端末ＩＤを第１の通信ネットワーク経由で受信した後に認証し、認証完了後に前記第１のネットワークよりも通信効率の優れた第２の通信ネットワーク経由で前記第２の情報端末に前記コンテンツ情報を配信す



【特許請求の範囲】
【請求項１】
複数のサービス利用システムから通信網経由で送られた端末ＩＤを情報サービスセンタで認証後、当該情報サービスセンタから当該サービス利用システムに特定のコンテンツ情報を配信する認証済み情報提供システムにおいて、前記サービス利用システムが、認証力の優れた端末ＩＤを持つ第１の情報端末と、当該第１の情報端末とは認証力が異なる第２の情報端末から構成されており、前記情報サービスセンタが前記第１の情報端末からの前記端末ＩＤを第１の通信ネットワーク経由で受信した後に認証し、認証完了後に第２の通信ネットワーク経由で前記第２の情報端末に前記コンテンツ情報を配信するように構成されたことを特徴とする認証済み情報提供システム。
【請求項２】
前記第２の情報端末が、前記第１の情報端末よりも認証力が劣る情報端末であるが、通信効率が優れている前記第２の通信ネットワークに接続された情報端末であることを特徴とする請求項１記載の認証済み情報提供システム。
【請求項３】
前記第２の情報端末が、前記第１の情報端末よりも認証力が劣る情報端末であるが、通信速度が高速である前記第２の通信ネットワークに接続された情報端末であることを特徴とする請求項１記載の認証済み情報提供システム。
【請求項４】
前記第２の情報端末が、前記第１の情報端末よりも認証力が劣る情報端末であるが、通信コストが安価である前記第２の通信ネットワークに接続された情報端末であることを特徴とする請求項１記載の認証済み情報提供システム。
【請求項５】
前記第１の情報端末が携帯電話で、前記第１の通信ネットワークが携帯電話の通信ネットワークであり、かつ第２の通信ネットワークは少なくともインターネットを含む通信ネットワークであることを特徴とする請求項１記載の認証済み情報提供システム。
【請求項６】
前記第２の通信ネットワークはさらに、ホットスポットでの不特定多数が利用可能なＬＡＮ通信網を含むことを特徴とする請求項５記載の認証済み情報提供システム。
【請求項７】
前記サービス利用システムの、前記第１の情報端末は当該サービス利用システム外へ取り外し独立して機能することが可能なように構成されたことを特徴とする請求項１記載の認証済み情報提供システム。
【請求項８】
前記サービス利用システムでは、前記第１の情報端末から前記情報サービスセンタへ前記端末ＩＤが認証処理のために送信された後、第２の情報端末で前記情報サービスセンタからの前記コンテンツ情報を受信する際には、前記第１の情報端末が前記サービス利用システム外へ取り外されても、前記第２の情報端末は前記コンテンツ情報を受信出来るように構成されたことを特徴とする請求項７記載の認証済み情報提供システム。
【請求項９】
前記サービス利用システムが車両内に設けられ、前記第１の通信ネットワークが携帯電話の通信ネットワーク、前記第２の通信ネットワークがインターネットおよびホットスポットに設けられたＬＡＮ通信網で構成されたことを特徴とする請求項１記載の認証済み情報提供システム。
【請求項１０】
前記第２の情報端末が、パソコンあるいはＰＤＡであることを特徴とする請求項１記載の認証済み情報提供システム。
【請求項１１】
前記情報サービスセンタが、前記コンテンツ情報を前記サービス利用システムに送信するための前記サービス利用システムに対する課金機能を有することを特徴とする請求項１記

載の認証済み情報提供システム。
【請求項１２】
前記情報サービスセンタで認証処理を行なう端末認証サーバと、前記コンテンツ情報を記憶するサービスデータ提供サーバとが、第２のＬＡＮまたは第３の通信ネットワークで結ばれていることを特徴とする請求項１記載の認証済み情報提供システム。
【請求項１３】
情報サービスセンタからコンテンツ情報を受信するサービス利用システムであって、認証力の優れた端末ＩＤを持つ第１の情報端末と、当該第１の情報端末とは認証力が異なる第２の情報端末から構成されており、前記情報サービスセンタへ前記第１の情報端末から前記端末ＩＤを第１の通信ネットワーク経由で送信して認証を受けた後に、前記第１の通信ネットワークよりも通信効率の優れた第２の通信ネットワーク経由で前記第２の情報端末で前記コンテンツ情報を受信するように構成されたことを特徴とするサービス利用システム。
【請求項１４】
前記サービス利用システムが車両内に設置され、前記第１の情報端末が携帯電話で、前記第１の通信ネットワークが携帯電話の通信ネットワークであり、かつ前記第２の情報端末がパソコンまたはＰＤＡで、前記第２の通信ネットワークがインターネットおよびホットスポットに設置されたＬＡＮ通信網で構成され前記コンテンツ情報を前記第２の情報端末で受信するように構成されたことを特徴とする請求項１３記載のサービス利用システム。
【請求項１５】
複数のサービス利用システムから通信網経由で送られた端末ＩＤを情報サービスセンタで認証後、当該情報サービスセンタから当該サービス利用システムに特定のコンテンツ情報を配信する認証済み情報配信方法において、前記情報サービスセンタで認証力の優れた端末ＩＤを持つ第１の情報端末から受信した前記端末ＩＤを認証するステップと、認証完了後に前記第１の通信ネットワークよりも通信効率の優れた第２の通信ネットワーク経由で、前記第１の情報端末とは認証力が異なる第２の情報端末に前記コンテンツ情報を配信するステップで構成されたことを特徴とする認証済み情報配信方法。
【請求項１６】
前記サービス利用システムが車両内に設置され、前記第１の情報端末が携帯電話で、前記第１の通信ネットワークが携帯電話の通信ネットワークであり、かつ前記第２の情報端末がパソコンまたはＰＤＡで、前記第２の通信ネットワークがインターネットおよびホットスポットに設置されたＬＡＮ通信網で構成され前記コンテンツ情報を前記第２の情報端末で受信するように構成されたことを特徴とする請求項１５記載の認証済み情報配信方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は情報利用者が携帯電話などの端末ＩＤ確認手段を持つ第１のネットワーク端末を用いて認証を受けた後に、情報サービスセンタ等の情報提供者がその認証データを流用して、端末の確認が確実に行えない第２のネットワーク端末へ情報提供を行なうことが出来る認証済み情報提供システムおよび情報配信方法に関する。具体的には情報利用者の携帯電話（第１のネットワーク端末）を用いて認証処理を行なうことで情報利用者本人であることを確認した後、情報サービスセンタから、携帯電話よりも通信速度、記憶容量の大きな別の端末（第２のネットワーク端末）へ効率よく情報をダウンロードする認証済み情報提供システムに関する。本認証済み情報提供システムを利用することにより、情報利用者は簡便に認証を受け、かつ通信効率のよい他の端末で速やかに情報提供を受けることができ、一方、情報提供者は利用者が誰であるかを携帯電話で確実に確認した後に、その本人確認が難しい端末に対しても安心して情報提供をすることが出来るために、確実に課金処理を行なうことが出来る利点を有する。
【０００２】
【従来の技術】

近年、無線ＬＡＮの部品コストの低下と、無線ＬＡＮインタネットアクセスポイントの構築コストの低下によって、ホットスポットと呼ばれる無線サービスが普及し始めている。このホットスポットとは、例えばレストランの駐車場等の不特定多数の自動車が出入りする場所で、レストランが客寄せを目的に顧客がレストラン提供の無線ＬＡＮを利用することにより何時でも自由にインターネット等にアクセスできるサービスである。この無線ＬＡＮは携帯電話の無線通信方式と比べて低い通信料金でサービスを提供できるという特徴がある。

【０００３】

しかしながら、一般に無線ＬＡＮにおいてはパソコンやＰＤＡに無線ＬＡＮカードをセットして利用者自身が設定を行う構成となっており、必ずしも真正な本人であることを確認することが出来ず、不正を行うことが可能な状態となっている。

この場合、情報利用者が無線ＬＡＮでインターネット接続サービスを提供することのみが目的の場合には問題は比較的少ないが、コンテンツサービスやプログラムのダウンロードを有料で受ける場合には、情報提供者にとっては確実に真正な本人に課金処理を行なうことが難しく、時として不正が行われて情報提供料が徴収できないというような大きな問題点を有している。

【０００４】

すなわち、情報提供者であるこれらのコンテンツデータの所有者あるいは著作権者は、一般に料金の徴収が適切に行えないサービス提供者にはコンテンツの提供を行わないことが多いため、情報利用者の満足するコンテンツを準備するためには、適切に料金が徴収できる仕組みが必要であるが、上述のように無線ＬＡＮのような利用者が端末の設定を容易に変更できるネットワークでは、簡便な操作で確実な認証を行うことは容易ではない。

【０００５】

【発明が解決しようとする課題】

そこで無線ＬＡＮのような環境において真正な情報利用者からのアクセスであるかを情報提供者が認証するためには、情報利用者に対して情報を受けるパソコンやＰＤＡ等の端末から、利用者ＩＤと十分に長い文字列のパスワードを入力することを要求しているが、情報利用者にとって操作が不便であるという問題点がある。

【０００６】

一方、情報利用者が保有する携帯電話の既存のサービスにおいては携帯電話そのものが課金の仕組みを有しており、端末ＩＤを使って端末の認証を行うことが可能であるため、それを利用した有料コンテンツサービスも行われている。携帯電話の有料コンテンツサービスにおいては、端末ＩＤは情報提供者から自動的に認識できるようになっているため、情報利用者は短いパスワードを入力するのみで、認証を受けることができ、簡便な操作でよいという特徴がある。すなわち携帯電話は認証力が優れている。しかしながら、一般に携帯電話の通信速度は無線ＬＡＮホットスポットと比較して大幅に低速で、携帯電話の利用料金はホットスポットで実施されている通信料金と比較して極めて高い通信料金となっているため、携帯電話を利用して音楽の配信や動画の配信を携帯電話に受けるには不向きである。また携帯電話の通信速度はＬＡＮホットスポット経由の通信速度と比べて格段に遅く、通信効率が悪い。しかも携帯電話の記憶容量はこれらの音楽や動画のデータ量と比較してはるかに小さく、より大ききデータ量である音楽や動画のデータ受信には向いていないという問題点がある。

【０００７】

一方、携帯電話を用いた課金システムについては、特開２００２－３１２７０９公報に、携帯電話を用いた課金システムが開示されている。このシステムでは、自動販売機は近距離にある携帯電話の発信電波を受信するための簡易受信機を内蔵し、携帯電話からの個人情報と購入商品情報を内蔵する発信機でホストコンピュータに無線で発信する。ホストコンピュータがその携帯電話の所持者を確認するとホストコンピュータから商品販売可能モードに設定する信号を受信後、利用者には商品販売を行ない、同時に課金処理を行なうように構成されている。すなわち本システムは、携帯電話の持つ本人確認（認証）用のＩＤ

を利用して、確実に課金処理を行なうものである。この場合、携帯電話、自動販売機、そしてホストコンピュータ間では、単に携帯電話のＩＤと販売商品（例えばコーラ）データという音楽や画像データとは比較にならない程に小さなデータを送るに過ぎず、また通信速度も殆ど問題にならない。これに反して上述のように情報利用者が情報提供者から音楽や画像データを情報提供者からダウンロードする場合には、通信速度が重要な問題となり、必ずしもこの携帯電話を用いた課金処理システムを、大容量のデータのダウンロードシステムには用いることが出来ない。

【０００８】

さらに上述の携帯電話を用いた課金システムでは、課金のための認証処理と商品販売の課金処理とが同時に行なう必要がある。しかしながら上述のように携帯電話を用いて認証後に、音楽や画像情報を得る場合には、どのような高速な通信回線を用いようともかなりのダウンロードに時間を要するために、時として予め本人であるとの認証を携帯電話で行ない、情報入手のためのダウンロードはある程度の時間経過後に行ないたいという必要性が生ずる。例えばホットスポットがレストランの駐車場であり、情報利用者（例えばレストランの客）がそのレストランで食事中に、車に載置されたコンピュータに音楽データをダウンロードする場合、携帯電話は利用者本人がレストラン内へ持参する場合には、上述の自動販売機の課金システムは使用することが出来ない。

【０００９】

本発明の第１の目的は、真正な情報利用者からのアクセスであるかを情報利用者自身が簡便な手段で情報提供者に知らせ、情報提供者はそれに基づき認証を行なう情報提供システムを提供することである。

【００１０】

本発明の第２の目的は、認証力はあるが通信効率の比較的劣る通信システムを用いて認証が行なわれても、大容量の情報配信は通信効率の良い別の通信システムを経由して配信を受ける情報提供システムを提供することである。

【００１１】

本発明の第３の目的は、大容量のコンテンツ情報を受信する際には、認証を受けるために用いた情報機器は、そのコンテンツ情報の受信とは独立して使用することが出来る情報提供システムを提供することである。

【００１２】

さらに本発明の第４の目的は、ホットスポットでの効率的なデータ通信を可能にすることを目的とする。

【００１３】

【課題を解決するための手段】

本発明はかかる課題を解決するため、複数のサービス利用システムから通信網経由で送られた端末ＩＤを情報サービスセンタで認証後、当該情報サービスセンタから当該サービス利用システムに特定のコンテンツ情報を配信する認証済み情報提供システムにおいて、前記サービス利用システムが、認証力の優れた端末ＩＤを持つ第１の情報端末と、当該第１の情報端末とは認証力が異なる第２の情報端末から構成されており、前記情報サービスセンタが前記第１の情報端末からの前記端末ＩＤを第１の通信ネットワーク経由で受信した後に認証し、認証完了後に第２の通信ネットワーク経由で前記第２の情報端末に前記コンテンツ情報を配信するように構成されたことを特徴とする認証済み情報提供システムを提案する。

【００１４】

このように構成することで、改ざんできない端末ＩＤを持つ第１の情報端末、すなわち認証力が優れた第１の情報端末で認証を行ない、その後に前記第１の情報端末よりも認証力は劣るが、通信効率が優れている通信ネットワーク、あるいは通信速度が高速である通信ネットワークに接続された第２の情報端末に、前記大容量のコンテンツ情報を送信することが可能となる。なおここで言う通信効率が優れているとは、例えば通信速度が速いこと、あるいは通信コストが安い等の広い概念を意味する。

【００１５】
また前記第１の情報端末が携帯電話で、前記第１の通信ネットワークが携帯電話の通信ネットワークであり、かつ第２の通信ネットワークは少なくともインターネットを含む通信ネットワークであるために、システムの構成として普遍性があり特に別段の装置、あるいはシステムを必要とはせずにシステムを構成することが出来る。
【００１６】
前記第２の通信ネットワークはさらに、ホットスポットでの不特定多数が利用可能なＬＡＮ通信網を含むことを特徴とする。従って近年多くの場所ですでに稼動しているホットスポットでの効率的な通信に応用することが可能となる。
【００１７】
なお前記サービス利用システムの、前記第１の情報端末は当該サービス利用システム外へ取り外し独立して機能することが可能なように構成する。また前記サービス利用システムでは、前記第１の情報端末から前記情報サービスセンタへ前記端末ＩＤが認証処理のために送信された後、第２の情報端末で前記情報サービスセンタからの前記コンテンツ情報を受信する際には、前記第１の情報端末が前記サービス利用システム外へ取り外されても、前記第２の情報端末は前記コンテンツ情報を受信出来るように構成する。このように構成することで、大容量のコンテンツ情報を例えばレストランの駐車場でダウンロードし、その間は携帯電話をシステムから取り外して、例えばレストラン内の食事中に通常の携帯電話として独立して使用可能となる。
【００１８】
本発明に係る認証済み情報提供システムでは、サービス利用システムが車両内に設けられ、前記第１の通信ネットワークが携帯電話の通信ネットワーク、前記第２の通信ネットワークがインターネットおよびホットスポットに設けられたＬＡＮ通信網で構成されたことを特徴とするために、自動車内からの大容量コンテンツのダウンロードが可能となる。
【００１９】
この場合前記第２の情報端末が、パソコンあるいはＰＤＡであり、携帯端末のホットスポットでの活用が可能となる。そして前記情報サービスセンタが、前記コンテンツ情報を前記サービス利用システムに送信するための前記サービス利用システムに対する課金機能を有するため、有償コンテンツ情報に対しても、ＩＤの偽造等の不正行為から防御することが出来る。
【００２０】
さらに前記情報サービスセンタで認証処理を行なう端末認証サーバと、前記コンテンツ情報を記憶するサービスデータ提供サーバとが、第２のＬＡＮまたは第３の通信ネットワークで結ばれていることにより、認証処理とコンテンツ情報配信とを別の場所、あるいは別のビジネスとして行なうことが可能となる。
【００２１】
さらに本発明では情報サービスセンタからコンテンツ情報を受信するサービス利用システムであって、改ざんできない端末ＩＤを持つ第１の情報端末と、当該第１の情報端末よりも通信効率のよい第２の情報端末から構成されており、前記情報サービスセンタへ前記第１の情報端末から前記端末ＩＤを第１の通信ネットワーク経由で送信して認証を受けた後に、前記第１の通信ネットワークよりも通信効率の優れた第２の通信ネットワーク経由で前記第２の情報端末で前記コンテンツ情報を受信するように構成されたことを特徴とするサービス利用システム、およびその為の認証済み情報配信方法を提案する。
【００２２】
【発明の実施の形態】
以下、本発明を図に示した実施例を用いて詳細に説明する。但し、この実施例に記載されている構成部品の寸法、材質、形状、その相対配置などは特に特定的な記載がない限り、この発明の範囲をそれのみに限定する趣旨ではなく、単なる説明例にすぎない。
【００２３】
図１に本発明の認証済み情報提供システムの概念図を示す。本システムにおいては情報提

供者である情報サービスセンタ１０は第１のネットワーク２０と第２のネットワーク３０を使用してサービス利用システム４０から構成されており、情報提供者である情報サービスセンタ１０は情報利用者の情報利用システム４０に対して情報提供サービスを行なう。第１のネットワーク２０は端末ＩＤを確実に認証する手段をもつネットワークであり、第１の通信手段を用いて利用者の確実な認証を行う。例えば情報利用者の有する携帯電話の通信回線網である。第２のネットワーク３０は端末ＩＤを確実に認証すること以外の点で、第１のネットワーク２０よりも優れている通信方式である。例えばレストランの駐車場に設置されたホットスポットに設けられたレストラン提供のＬＡＮシステム経由のインターネット網である。一般に携帯電話は通話毎に課金が行なわれるので、そのＩＤ等を用いて確実に課金処理を行うために、他の情報端末に比べて認証力が強い。

【００２４】

さらにサービス利用システム４０は、第１の情報端末５０と第２の情報端末６０で構成されている。例えば第１の情報端末５０とは携帯電話であり、第２の情報端末６０とはパソコンや、車内に設置されたインターネット接続が可能なパソコン機能端末である。第１の情報端末５０は、第１のネットワーク２０と接続する第１の通信手段５１と第１のネットワークにおいて端末ＩＤを認証する端末ＩＤ保有手段５２、端末操作手段５３の一部から構成されている。第２の情報端末６０は、第２のネットワーク３０と接続する第２の通信手段６１、第２のネットワーク３０から受信したサービス情報を記憶する記憶手段６２、サービス情報を処理するする情報処理手段６３、利用者がサービスを受けるための操作を行う端末操作手段５３の一部から構成される。従ってサービス利用システム４０は、概念的に情報利用者の携帯電話とパソコン等のインターネット利用端末から構成されている。

【００２５】

次に、第１のネットワークが携帯電話ネットワークであり、第２のネットワークが無線ＬＡＮのホットスポット経由のインターネットである場合について、実施例の詳細を説明する。

【００２６】

図２にサービス利用システム４０の実施例の構成を示す。サービス利用システム４０は、第１の情報端末５０である携帯電話、第２の情報端末６０である例えばパソコンあるいはパソコン機能端末で構成されており、携帯電話はこの実施例では市販されている携帯電話アダプタ７０を介して第２の情報端末であるパソコンに接続されている。第２の情報端末６０は、一般的なラップトップパソコンまたは車内設置のパソコン機能端末の構成であり詳述は省略するが、図１の概念図で示した６１に相当する第２のネットワークである無線ＬＡＮとのインタフェース手段である無線ＬＡＮインタフェース１６１、図１の概念図で示した記憶手段６２に相当するハードディスク１１６２Ａとハードディスクインターフェース１６２Ａ、その他ＣＰＵ１６３、ＲＯＭ１６４、ＲＡＭ１６５、操作手段１６６、電源管理部１６７、シリアルインタフェース１６８、携帯電話と直接接続を行なうコネクタ１６３から構成されている。

【００２７】

オプションとして電源管理部１６７を加えた構成とすることで、サービス利用時に電源のオンオフを自動的に行って、より低消費電力の実現することが可能である。車両など、消費電力の制約が厳しい利用形態においては、この電源管理部を加えた構成とすることが望ましい。

【００２８】

図３に他の実施例によるサービス利用システム４０Ａが示されており、第１の情報端末である携帯電話５０用のアダプタと携帯電話保持機構１６９Ａを内蔵する第２の情報端末６０Ａの実施例を示す。図３の構成では、携帯電話をサービス利用システムに直接接続できるため、サービス利用システム４０Ａの設置が容易であったり、利用者の利用開始のための準備作業が簡便になったりする。設置場所が車両の場合のように、携帯電話が移動したり落下したりする恐れがあるときには、サービス利用システムは携帯電話を物理的に保持する構成となっていることが望ましい。

【００２９】
図４に例えばコンテンツサービスを提供する情報サービスセンタ１０の構成を示す。この実施例では情報サービスセンタ１０は、第１の通信方式である携帯電話ネットワーク２０とは携帯電話ネットワーク接続装置１１を介して接続される。情報サービスセンタ１０はさらに、第２の通信方式である無線ＬＡＮのホットスポットに設けられた無線ＬＡＮ接続装置３０Ａ経由のインターネット３０Ｂに接続するために、インターネットネットワーク接続装置１２を介して接続される。
【００３０】
無線ＬＡＮホットスポットはインターネット３０Ｂに接続されているため、情報サービスセンタ１０はインターネット経由で無線ＬＡＮホットスポットと接続できる。サービス利用システム４０が無線ＬＡＮホットスポットのサービス提供範囲にあると、情報サービスセンタ１０はサービス利用システム４０と接続し通信を行うことができる。
【００３１】
この実施例ではサービス利用システム４０は第１の通信端末である携帯電話５０と接続されているため、情報サービスセンタ１０は携帯電話ネットワーク２０を介してサービス利用システム４０と接続し通信を行うことができる。
【００３２】
携帯電話ネットワーク接続装置１１とインターネットネットワーク接続装置１２を介して、情報サービスセンタ１０内のＬＡＮ１３は携帯電話ネットワーク２０およびインターネット３０Ｂに接続される。
【００３３】
サービスデータ提供サーバ１４の負荷が重い場合には、図４の構成のようにサービスデータ提供サーバを複数台設置し、それらの複数台へのサーバに負荷を振り分けるのに負荷分散装置１５（ロードバランサと呼ばれる場合もある）を利用する構成としてもよい。サービスデータ提供サーバ１４の負荷が軽い場合には、負荷分散装置１５は省略してサーバ１台で処理する構成としてもよい。あるいは、端末をグループ分けしてグループごとに異なるサーバに接続するように運用して、負荷分散装置１５を省略した構成とすることも可能である。
【００３４】
端末認証サーバ１６はＬＡＮ１３を介してサービスデータ提供サーバ１４と通信を行うことができる。他の類似の実施例として、情報サービスセンタ１０内の端末認証サーバ１６とサービスデータ提供サーバは、ＬＡＮ１３で接続することなく、第３の通信網を経由しても、またインターネットを経由して接続してもよいし、また端末認証サーバ１６とサービスデータ提供サーバ１４を１台のサーバ装置で実施するような構成としてもよい。
【００３５】
図５は、ホットスポットに駐車した自動車内で情報サービスセンタ１０から情報提供を提供する場合の実施例を示す。サービス利用システム１０が車両内に設置された場合には、以下に示すようなサービスを提供することができ、本発明に係る認証済み情報提供システムの効果が発揮される。
【００３６】
サービス提供者のサービス内容として、例えば１００Ｍｂｙｔｅ～数Ｇｂｙｔｅのコンテンツデータを配信するコンテンツサービスを想定するが、特にこれに限定しない。本発明に係る認証済み情報提供システムでは、認証は携帯電話のネットワーク経由（第１のネットワーク）、コンテンツの配信はインターネットおよびＬＡＮ経由（第２のネットワーク）で行なわれる。これに反して従来は、このようなコンテンツサービスは、車両においては主に携帯電話を経由してしか通信を行うことができなかったため、主にコスト面の制約から大容量のコンテンツサービスは行われていないのが現状であった。すなわちこれまでは、無線ＬＡＮホットスポットのサービスエリア内に車が停車した状態においては、高速通信が実現できるが、利用端末の特定が困難であるためコンテンツ提供者がコンテンツの提供を拒否したり、利用者が認証手順を操作することが複雑なため利用を簡便に行えない

といった問題点があったため、大容量コンテンツサービスは行われていなかった。
【００３７】
なお本発明に係る図５に示す実施例においては、利用者は携帯電話をサービス利用システムを認証を受ける段階では無線ＬＡＮホットスポットのサービスエリア内である必要はないので、携帯電話のサービスエリア内にいればよく、ほとんどの場所で認証を受けることができる。すなわち必ずしもＬＡＮエリアで認証を受ける必要は無く、車がＬＡＮエリアに到着する前に認証処理は予め完了しておくことが可能である。
【００３８】
携帯電話を接続した状態で、情報サービスセンタ１０の認証を受けると、サービス利用システム４０内の第２の情報端末（例えばパソコン、あるいは車内設置のパソコン機能端末）にはサービスＩＤが受信され記録されている。従って認証が終了した後は、携帯電話を介した通信が引き続き可能である必要はない。このため、以下の効果が得られる。
（１）コンテンツデータのダウンロード中やコンテンツを利用するときには携帯電話の操作を行う必要はない。
（２）サービスＩＤを複数回利用可能とすれば、１回の認証のための操作によって複数回サービスを受けることができ、利用者の操作は大幅に削減できる。
（３）ホットスポットのサービスエリアが屋内や地下にあり、携帯電話の通信が行えない場所であってもサービスの提供を受けることができる。
（４）ホットスポットのサービスを受けるときに、携帯電話がサービス利用システムに接続されている必要はない。従って、例えば大容量のコンテンツを第２のネットワークでダウンロードしているときに、携帯電話を取り外して持って歩くことができる。より具体的な例としては、レストランやショッピングセンタが提供する無線ＬＡＮホットスポットに到着した後、食事やショッピングをしている間にコンテンツデータのダウンロードが完了し、その間において携帯電話は取り外して手元に置いておけることになる。
（５）認証の証拠として得られるサービスＩＤはサービス利用システム４０内に記録されている。従って、サービス利用システムの重要情報を外部から隠蔽して保護するだけで改ざんや不正利用を防止することができる。
【００３９】
次に図６に端末認証サーバとサービスデータ提供サーバの連携について示す。端末認証サーバ１６は携帯電話ネットワーク３０を介してサービス利用システム４０と通信を行い、ホットスポットのＬＡＮを介してサービスデータ提供サーバ１４とコンテンツ配信のための通信を行う。
【００４０】
サービスデータ提供サーバ１４は無線ＬＡＮホットスポットのサービスエリア内にあるサービス利用システム４０とインターネットを介して通信を行う。
【００４１】
ここで各装置、システム間のデータの流れを図の中央部に示す。
（１）サービス利用システム４０は端末ＩＤを含むサービス要求情報を携帯電話ネットワーク１１を介して端末認証サーバ１６に送る。
（２）端末認証サーバ１６は、サービス利用システム４０から送られてきた端末ＩＤを使って端末ＩＤデータベース１６Ａを検索し、当該端末ＩＤに対するサービスの内容を知る。
（３）端末認証サーバ１６は、サービスデータ提供サーバ１４に端末ＩＤを送る。
（４）サービスデータ提供サーバ１４はサービスＩＤを発行し端末認証サーバ１６に送る。
（５）端末認証サーバ１６は携帯電話ネットワーク１１でサービス利用システム４０にサービスＩＤを送る。
（６）サービス利用システム４０はサービスＩＤを記録する。
（７）例えば車両がレストランの駐車場内に設けられた無線ＬＡＮのサービスエリアにおいて、サービス利用システム４０がサービスＩＤを含むサービス要求をサービスデータ提

供サーバ１４に送る。
（８）サービスデータ提供サーバ１４はサービスＩＤをチェックして正規のものであれば、相当するサービスデータをサービス利用システムに送信する。
（９）サービス利用システム４０は後のサービスに必要となるデータを分類して記憶装置に記憶する。
【００４２】
以上のように端末認証サーバ１６とサービスデータ提供サーバ１４が連携して、サービス利用システム４０に対してサービスを実施することによって、利用者の認証からサービスデータの配信までの一連の処理の流れを実現することができる。
【００４３】
なおサービスＩＤはサービスデータ提供サーバ１４からの情報に基づいて端末認証サーバ１６で発行するような構成としてもよい。また端末ＩＤデータベース１６Ａと、サービスデータデータベース１４Ａは端末認証サーバ１６やサービスデータ提供サーバ１４と分離した装置に置くような構成としてもよいし、いずれかのサーバに置く構成としても良いし、全てを１台のサーバ装置に置くような構成としてもよい。
【００４４】
図７（Ａ）－図７（Ｃ）はサービス利用システム４０内の処理についての処理フローチャートである。図７（Ａ）は端末認証時のフローチャートで、図７（Ｂ）はサービスデータ受信時、図７（Ｃ）は提供時のフローチャートである。
【００４５】
まず図７（Ａ）で端末認証処理について説明する。
ＳＴ７Ａ－１：利用者がサービス利用システム４０の操作手段を用いて、認証が必要な操作を行うと、サービス利用システム４０は携帯電話ネットワーク２０を介して情報サービスセンタ１０に接続し認証の要求を行う。
ＳＴ７Ａ－２：このとき、携帯電話ネットワーク２０を介して情報サービスセンタ１０へ端末ＩＤが送信される。
ＳＴ７Ａ－３：上記の端末の動きに対応して情報サービスセンタ１０からサービスＩＤがサービス利用システム４０へ送られてくるのでそれを受信する。
ＳＴ７Ａ－４：情報サービスセンタ１０からサービスＩＤが送られてこない場合には端末はサービスを中断する。
ＳＴ７Ａ－５：サービスＩＤが送られて来た場合には、サービス利用システム４０でサービスＩＤを記録する。
【００４６】
つぎに図７（Ｂ）でサービスデータ受信処理について説明する。
ＳＴ７Ｂ－１：例えばレストランの無線ＬＡＮからインターネット経由で情報サービスセンタ１０のサービスデータ提供サーバ１４に端末ＩＤとサービスＩＤを含むサービスデータ要求情報を送り、サービスデータ（音楽、画像データ）の送信を求める。
ＳＴ７Ｂ－２：サービスデータが無い場合にはサービスを中断する。
ＳＴ７Ｂ－３：サービスデータがある場合には情報サービスセンタ１０からサービスデータを受信する。
ＳＴ７Ｂ－４：受信したサービスデータから後に利用するデータを分類する。
ＳＴ７Ｂ－５：分類したサービスデータを記録する。
【００４７】
さらに図７（Ｃ）でサービスデータ受信処理について説明する。
ＳＴ７Ｃ－１：利用者が図１に示す端末操作手段５３を使って、端末サービスの開始を要求する。
ＳＴ７Ｃ－２：　サービス利用システム４０の記憶装置に６２サービスデータが記録されているか確認する。
ＳＴ７Ｃ－３：サービスデータが無い場合にはサービスを中断する。
ＳＴ７Ｃ－４：サービスデータがある場合には、記憶手段６２からサービスデータを読み

出す。
ＳＴ７Ｃ－５：サービスデータを使って情報処理手段６３からサービスを取り出す。例えば音楽のコンテンツ配信を受けた場合は、プレーヤへ音楽データを送り音楽として聴くことが出来る。
【００４８】
図８には端末認証サーバ１６での処理フローチャートが示されている。
ＳＴ８－１：サービス利用システム４０が情報サービスセンタ１０の端末認証サーバ１６に接続を要求してくる。
ＳＴ８－２：接続を許可する。
ＳＴ８－３：サービス利用システム４０から端末ＩＤを含む認証要求情報が送られる。
ＳＴ８－４：端末ＩＤで端末ＩＤデータベース１６Ａを検索してサービス内容を知る。
ＳＴ８－５：端末ＩＤの登録が無い場合にはサービスを中断し、サービス利用システム４０にサービス中断を通知する（ＳＴ８－１０）。
ＳＴ８－６：端末ＩＤの登録がある場合には、端末ＩＤをサービスデータ提供サーバ１４に送信する。
ＳＴ８－７：サービスデータ提供サーバ１４からの応答を確認する。
ＳＴ８－８：サービスＩＤが送信されない場合にはサービスを中断し端末にサービス中断を通知する（ＳＴ８－１０）。
ＳＴ８－９：サービスＩＤが送られてきた場合には端末にサービスＩＤを送信する。
【００４９】
図９（Ａ）および図９（Ｂ）には、図４に示す情報サービスセンタ１０内のサービスデータ提供サーバ１４のフローチャートを示す。図９（Ａ）は端末認証時のフローチャート、図９（Ｂ）はサービスデータ提供時のフローチャートである。
【００５０】
図９（Ａ）に示す端末認証時には、サービスデータ提供サーバ１４は以下の動作を行う。
ＳＴ９Ａ－１：端末認証サーバ１６から端末ＩＤを受信する。
ＳＴ９Ａ－２：サービスデータベース１４Ａを検索し、端末ＩＤの登録が無ければサービスを中断し認証サーバに中断を通知する（ＳＴ９Ａ－５）。
ＳＴ９Ａ－３：端末ＩＤの登録が有る場合にはサービスＩＤを発行し記録する。
ＳＴ９Ａ－４：発行したサービスＩＤを認証サーバ１６に送信する。
【００５１】
図９（Ｂ）に示すサービスデータ提供時、サービスデータ提供サーバ１４は以下の動作を行う。
ＳＴ９Ｂ－１：サービス利用システム４０から端末ＩＤとサービスＩＤを受信する。
ＳＴ９Ｂ－２：サービスデータデータベース１４Ａを検索し、端末ＩＤの登録があるかを確認する。端末ＩＤの登録が無い場合には、サービスを中断し端末に中断を通知する（ＳＴ９Ｂ－６）。
ＳＴ９Ｂ－３：端末ＩＤの登録がある場合には、サービスＩＤの確認を行う。サービスデータの登録が無ければ、サービスを中断し端末に中断を通知する（ＳＴ９Ｂ－６）。
ＳＴ９Ｂ－４：サービスデータの登録があれば、サービスデータデータベース１４Ａからサービスデータを読み出す。
ＳＴ９Ｂ－５：サービスデータをインターネット経由でサービス利用システム４０に送信する。
【００５２】
次に図１０に端末ＩＤデータベースの実施例の構成を示す。この実施例では端末ＩＤデータベースは端末ＩＤから、当該ＩＤの端末に対してサービスデータを保持しているサーバを特定できる文字列を検索する。例えば端末ＩＤは７桁の数字とする。またデータサーバを特定できる文字列として、例えば＜サーバ名＞：＜格納場所名＞とする。格納場所名は例えば端末ＩＤの前に小文字のｔをつけたものとする。
【００５３】

図１０の例では端末ＩＤ０００００１に対して文字列ＤａｔａＳｅｒｖｅｒ００１：／ｔ０００００１が対応しており、サーバがＤａｔａＳｅｒｖｅｒ００１で特定でき、場所が文字列ｔ０００００１で特定できる。このようにして複数台のデータサーバを利用することもできるが、本実施例ではデータサーバを１台とする。端末認証サーバは端末ＩＤデータベースを検索することでサービスデータ提供サーバを特定して、当該端末へのサービスＩＤを要求することができる。

次に図１１にサービスデータデータベースの実施例の構成を示す。この実施例では、データベースのデータはファイルシステムのディレクトリ構造で実現している。各サービスデータ提供サーバはサービスデータデータベースを参照して、端末へのサービスデータを提供する。

【００５４】

【発明の効果】

以上記載の如く本発明によれば、利用者は携帯電話をサービス利用システムと接続して操作手段によって、サービスの要求を出し、必要な場合には比較的短いパスワードを入力するのみで、データ配信サービスを受けることができる。さらに、受信したデータによるサービスを受ける場合には認証を行う必要は無いため、極めて容易な操作でサービスを開始することができる。さらにデータ配信サービスは、通信効率が良い第２の通信ネットワークを経由して行われるので、高速かつ通信コストを安くすることが可能となる。

【００５５】

また本発明考案を高音質の楽曲データや動画像のコンテンツデータ配信に利用することを考えれば、効果は明らかである。

【図面の簡単な説明】

【図１】図１は本発明の認証済み情報提供システムの概念図である。

【図２】図２はサービス利用システム４０の実施例の構成図である。

【図３】図３は他のサービス利用システム４０Ａの実施例の構成図である。

【図４】図４はコンテンツサービスを提供する情報サービスセンタの構成図である。

【図５】図５は、ホットスポットに駐車した自動車内で情報サービスセンタから情報提供を提供する場合の実施例についての概念図である。

【図６】図６は端末認証サーバとサービスデータ提供サーバの連携に関する概念図である。

【図７】図７（Ａ）－図７（Ｃ）はサービス利用システム内での処理に関するフローチャートである。

【図８】図８は端末認証サーバ内での処理に関するフローチャートである。

【図９】図９（Ａ）、図９（Ｂ）はサービスデータ提供サーバ内での処理に関するフローチャートである。

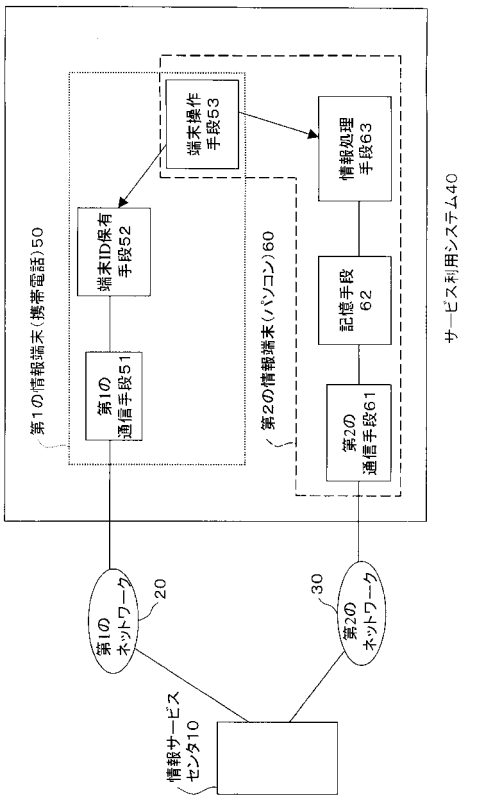
【図１０】図１０は端末ＩＤデータベースの構成図の一例である。

【図１１】図１１はサービスデータデータベースの構成図の一例である。

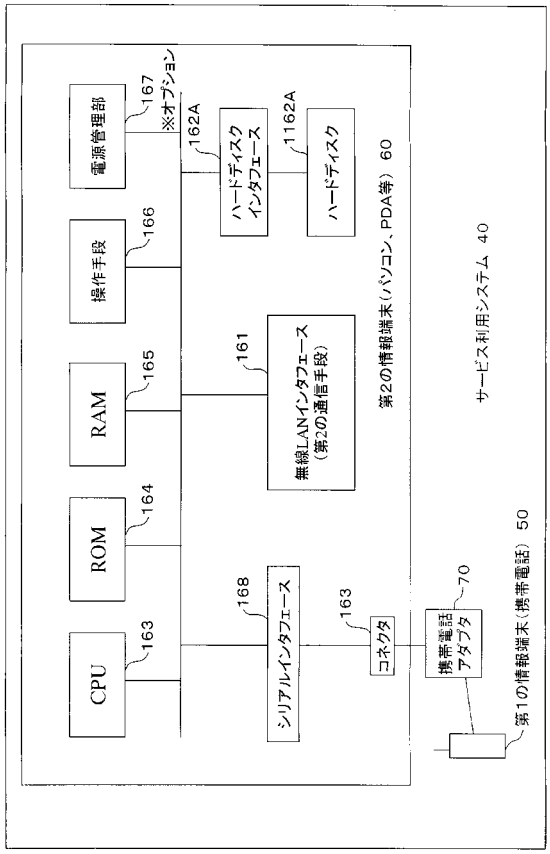
【符号の説明】

１０　情報サービスセンタ
２０　第１のネットワーク
３０　第２のネットワーク
４０　サービス利用システム
５０　第１の情報端末（携帯電話）
５１　第１の通信手段
５２　端末ＩＤ保有手段
５３　端末操作手段
６０　第２の情報端末（パソコン）
６１　第２の通信手段
６２　記憶手段
６３　情報処理手段

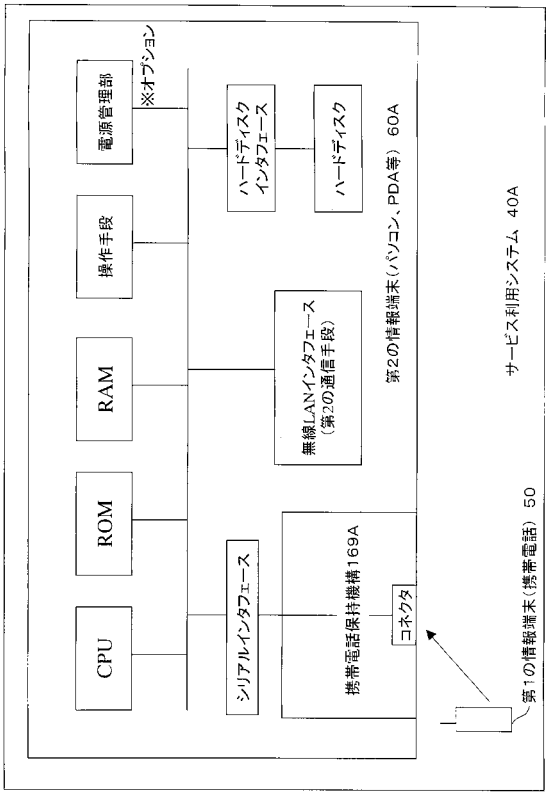
【図１】


第1の情報端末（携帯電話）50
第1の通信手段51
端末ID保有手段52
端末操作手段53
第2の情報端末（パソコン）60
第2の通信手段61
記憶手段62
情報処理手段63
サービス利用システム40
第1のネットワーク
20
30
第2のネットワーク
情報サービスセンタ10

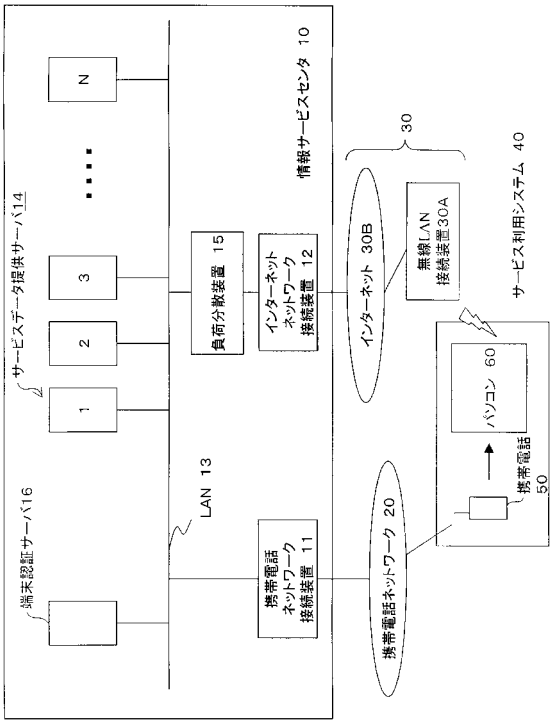
【図２】


CPU
163
ROM
164
RAM
165
操作手段
166
電源管理部
167
※オプション
ハードディスクインタフェース
162A
ハードディスク
1162A
無線LANインタフェース（第2の通信手段）
161
シリアルインタフェース
168
コネクタ
163
携帯電話アダプタ
70
第2の情報端末（パソコン、PDA等）60
サービス利用システム 40
第1の情報端末（携帯電話）50

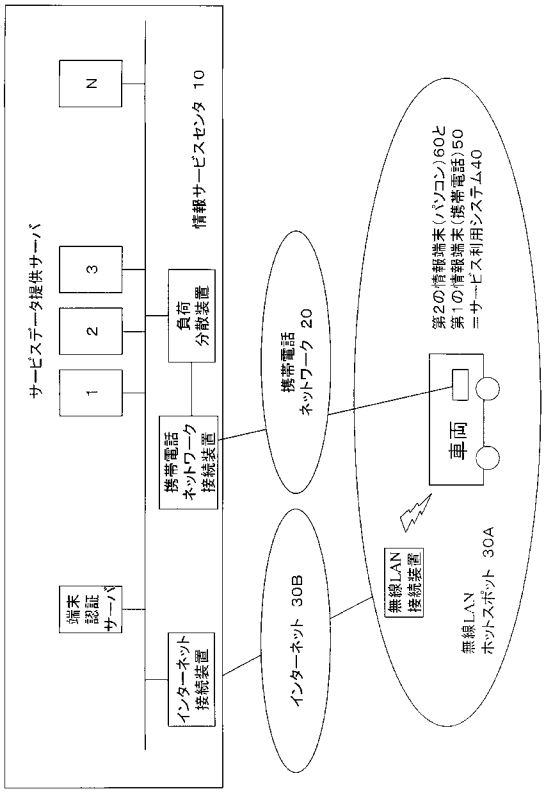
【図３】


CPU
ROM
RAM
操作手段
電源管理部
※オプション
ハードディスクインタフェース
ハードディスク
無線LANインタフェース（第2の通信手段）
シリアルインタフェース
携帯電話保持機構169A
コネクタ
第2の情報端末（パソコン、PDA等） 60A
サービス利用システム 40A
第1の情報端末（携帯電話） 50

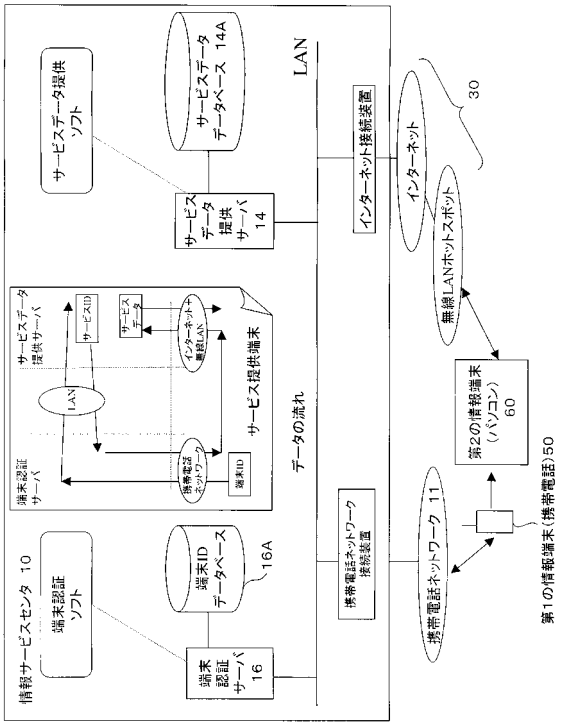
【図４】


端末認証サーバ16
サービスデータ提供サーバ14
1
2
3
N
LAN 13
携帯電話ネットワーク接続装置 11
負荷分散装置 15
インターネットネットワーク接続装置 12
情報サービスセンタ 10
インターネット 30B
30
無線LAN接続装置30A
携帯電話ネットワーク 20
パソコン 60
携帯電話
50
サービス利用システム 40

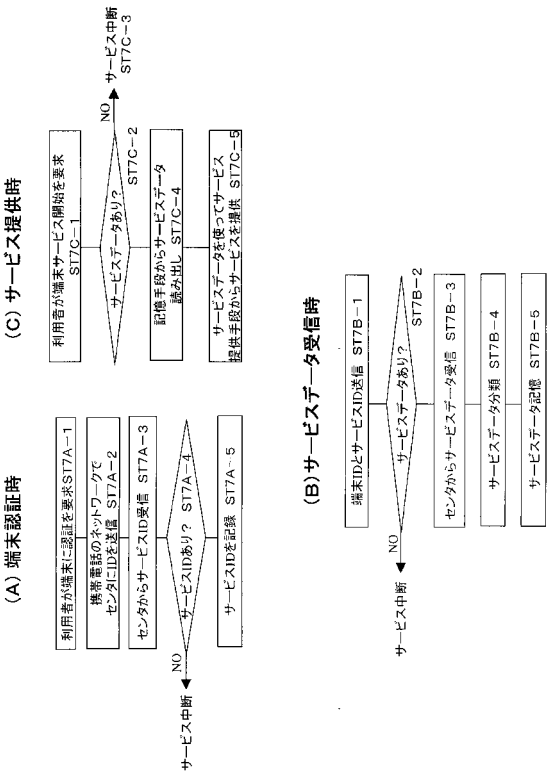
【図５】


サービスデータ提供サーバ
1
2
3
N
端末認証サーバ
インターネット接続装置
携帯電話ネットワーク接続装置
負荷分散装置
情報サービスセンタ 10
インターネット 30B
携帯電話ネットワーク 20
無線LAN接続装置
車両
無線LANホットスポット 30A
第2の情報端末（パソコン）60と
第1の情報端末（携帯電話）50
＝サービス利用システム40

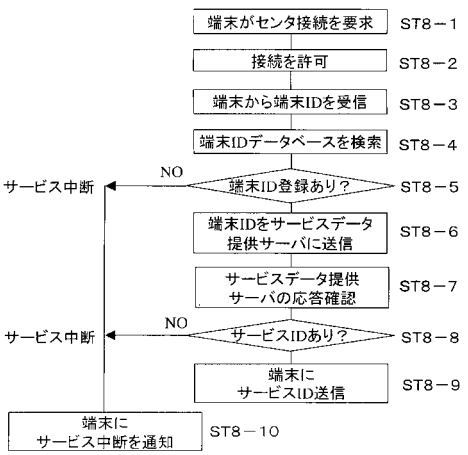
【図６】


サービスデータ提供ソフト
サービスデータデータベース 14A
LAN
サービスデータ提供サーバ 14
インターネット接続装置
インターネット
30
サービスデータ提供サーバ
端末認証サーバ
サービスID
サービスデータ
インターネット＋無線LAN
携帯電話ネットワーク
端末ID
サービス提供端末
無線LANホットスポット
データの流れ
情報サービスセンタ 10
端末認証ソフト
端末IDデータベース
16A
端末認証サーバ 16
携帯電話ネットワーク接続装置
携帯電話ネットワーク 11
第2の情報端末（パソコン）60
第1の情報端末（携帯電話）50

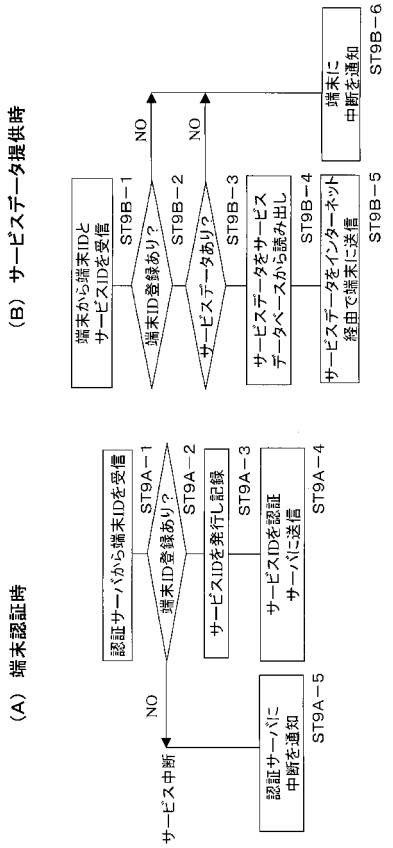
【図７】


(A) 端末認証時
利用者が端末に認証を要求 ST7A－1
携帯電話のネットワークでセンタにIDを送信 ST7A－2
センタからサービスID受信 ST7A－3
サービスIDあり？ ST7A－4
NO
サービス中断
サービスID記録 ST7A－5
(C) サービス提供時
利用者が端末サービス開始を要求 ST7C－1
サービスデータあり？ ST7C－2
NO
サービス中断 ST7C－3
記憶手段からサービスデータ読み出し ST7C－4
サービスデータを使ってサービス提供手段からサービスを提供 ST7C－5
(B) サービスデータ受信時
端末IDとサービスID送信 ST7B－1
サービスデータあり？ ST7B－2
NO
サービス中断
センタからサービスデータ受信 ST7B－3
サービスデータ分類 ST7B－4
サービスデータ記憶 ST7B－5

【図８】


端末がセンタ接続を要求 ST8－1
接続を許可 ST8－2
端末から端末IDを受信 ST8－3
端末IDデータベースを検索 ST8－4
NO
サービス中断
端末ID登録あり？ ST8－5
端末IDをサービスデータ提供サーバに送信 ST8－6
サービスデータ提供サーバの応答確認 ST8－7
NO
サービス中断
サービスIDあり？ ST8－8
端末にサービスID送信 ST8－9
端末にサービス中断を通知 ST8－10

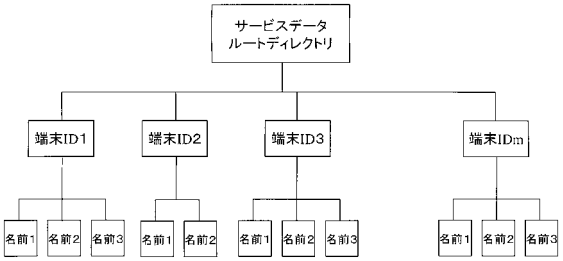
【図９】



【図１０】

端末ID	データサーバID
0000001	DataServer001:/t000001/
0000002	DataServer001:/t000002/
0000003	DataServer001:/t000003/
0000004	
N	サーバ名:/端末ID/

【図１１】



フロントページの続き

【要約の続き】
るように構成する。
【選択図】　図１