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

特許第4970833号
(P4970833)

(45)発行日　平成24年7月11日(2012.7.11)　(24)登録日　平成24年4月13日(2012.4.13)

(51)Int.Cl.　　F I
H04W 4/06 (2009.01)　　H04Q 7/00 １２０
H04W 12/06 (2009.01)　　H04Q 7/00 １８３

請求項の数 6　外国語出願　(全 12 頁)

(21)出願番号　特願2006-113302 (P2006-113302)
(22)出願日　平成18年4月17日 (2006.4.17)
(65)公開番号　特開2007-6455 (P2007-6455A)
(43)公開日　平成19年1月11日 (2007.1.11)
審査請求日　平成21年4月8日 (2009.4.8)
(31)優先権主張番号　05008465.6
(32)優先日　平成17年4月19日 (2005.4.19)
(33)優先権主張国　欧州特許庁 (EP)

(73)特許権者　506130573
アヌープ　ナーハー
Ａｎｏｏｐ　Ｎａｈａｒ
ドイツ，４０８８５　ラーティンゲン，
ベックマンーシュトラーセ　７
(74)代理人　100061815
弁理士　矢野　敏雄
(74)代理人　100099483
弁理士　久野　琢也
(74)代理人　100128679
弁理士　星　公弘
(74)代理人　100135633
弁理士　二宮　浩康

最終頁に続く

(54)【発明の名称】広帯域データ伝送方法

(57)【特許請求の範囲】
【請求項１】
少なくとも１つの広帯域チャンネルを経由して、プロバイダサーバ（１０）からアノニマス広帯域端末（４０）にデータを伝送する方法であって、
少なくとも１つのモバイル無線電話網（６０）のチャンネルを経由して、広帯域データ伝送用の制御文を送信し、
少なくとも１つのモバイル無線電話端末（５０）が制御文の実行に用いられ、
モバイル無線電話端末（５０）とプロバイダサーバ（１０）との間の制御文に保護されたプロトコルが用いられ、
データ伝送の認証は、広帯域端末（４０）およびモバイル無線電話端末（５０）に伝送されるトークンの一致についての、手動作での確認によって実行される、
ことを特徴とする、広帯域データ伝送方法。
【請求項２】
最終ユーザの同定（本人確認）が明確にできる手段により、最終ユーザの基本登録が実現されることを特徴とする、請求項１に記載の広帯域データ伝送方法。
【請求項３】
アノニマス広帯域チャンネルを経由した、個人保護されたまたはプロテクトされたアプリケーションまたはコンテンツの表示および使用の前に、少なくとも１つのモバイル無線電話網（６０）のチャンネルを経由して、最終ユーザの同定（本人確認）がなされることを特徴とする、請求項２に記載の広帯域データ伝送方法。

【請求項４】
広帯域データ伝送により伝送されるべきデータが、最終ユーザにより、少なくとも１つのモバイル無線電話網（６０）のチャンネルを経由して選択されることを特徴とする、請求項２または３に記載の広帯域データ伝送方法。
【請求項５】
広帯域データ伝送により、データが最終ユーザによって複数の広帯域端末（４０）に伝送されることを特徴とする、請求項２～４のいずれか１項に記載の広帯域データ伝送方法。
【請求項６】
前記最終ユーザにより、前記複数の広帯域端末（４０）は、少なくとも１つのモバイル無線電話網（６０）のチャンネルを経由して選択されることを特徴とする、請求項５に記載の広帯域データ伝送方法。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、少なくとも１つの広帯域（ワイドバンド）チャンネルを経由して、データを伝送する方法に関するものである。
【背景技術】
【０００２】
前記広帯域（ワイドバンド）伝送は、たとえば、個人がインターネットにアクセスするとき、またはホームコンピュータを使うときに実現されている。
ホームコンピュータの大きな利点は、ユーザが自分の裁量で自由に構築（コンフィギュレート）でき、また必要なソフトウエアをあてがうことができることにある。
つまり、そのことにより、特別にそのユーザに適合したシステム構築が成し遂げられ、その結果、,多くの異ったアプリケーションが実行されることになる。
【０００３】
ホームコンピュータの他の利点は、例えば、インターネットへのの個人的アクセスにより、最終ユーザが同定（本人確認）され、法的に認証できることである。
このような認証に基き、最終ユーザは、例えば、インターネット上の有料ページやアプリケーションを利用することができる。
なお、これらの課金は、個人の電話料金請求と一緒に行われる。
【特許文献１】欧州特許出願ＥＰ１　４９９　１２７Ａ
【解決しようとする課題】
【０００４】
しかしながら、ホームコンピュータは携帯性（モビリティ）がないという欠点がある。
【０００５】
様々なモバイル（携帯）端末が上記の欠点を解決してくれる。
例えば、ラップトップコンピュータは、大きなディスプレイとキーボード、通常は十分なメモリ容量と必要な帯域幅（伝送容量）をもっているので、ホームコンピュータと同様にユーザフレンドリイである。
しかしながら、ラップトップコンピュータは、割と大きく重いので、最終ユーザは、しばしば、持ち運びをためらう。
【０００６】
端末のサイズや重さの点かから云えば、いわゆるハンドヘルドコンピュータが最適である。それは、非常に小さく、軽く、ハンディであり、最終ユーザは容易に持ち運びできるからである。
【０００７】
しかしながら、ハンドヘルドコンピュータは、それなりに、ディスプレイは小さく、キーボードは使いにくく、また、通常は、割に、記憶容量も小さい等、実用的でない。
その上、モバイルなので、モバイル無線電話網のモバイル無線電話チャンネルを経由し

なければデータを送信できない。
さらに、大容量のデータを送信するときは時間がかかる等の欠点がある。
【０００８】
必要とする携帯性（モビリティ）と使い易さの両方を保証するため、インターネットに誰でもがアクセス可能な広帯域端末が、続々と提供されている。
前記広帯域端末には、WEBブラウザが搭載され、IPアドレスを利用して、相手を認識し、同定（本人確認）できる。
前記広帯域端末を経由すれば、大容量のデータも短時間で送ることができる。
【０００９】
しかしながら、前記の公にアクセス可能な広帯域端末は、下記のような重大な欠点がある。
すなわち、前記広帯域端末は、最終ユーザによる、それに合ったソフトウエアのインストールまたはハードエアの構築（コンフィギレーション）という、限定された方法でしか、プリセットできない。
それ故、パブリックな前記広帯域端末では、大量なデータや著しく特殊な形式のデータを、取り扱うことができない場合がしばしばある。
【００１０】
他の欠点は、例えば、有料のインターネットページや有料のアプリケーションを利用することができないので、前記広帯域端末を使用している最終ユーザを同定し（本人確認）し認証することができないことである。
【発明の開示】
【課題を解決するための手段】
【００１１】
本発明の目的は、上記の欠点をとり除いたもので、少なくとも１つの広帯域チャンネルを経由してデータを伝送する方法であって、使い易く携帯性に優れたモバイル端末により、最終ユーザの本人確認と認証を保証することを特徴とする、広帯域データ伝送方法を提供することにある。
【００１２】
本発明は、上記目的を達成するためなされたもので、少なくとも１チャンネルのモバイル無線電話網を経由して広帯域データ伝送用の制御文（コントロールステートメント）が送信されることを特徴とする、少なくとも１つの広帯域チャンネルを利用したデータ伝送方法である。
【００１３】
広帯域チャンネルとモバイル無線電話チャンネルの併用は効果が大きく、各々のチャンネルを利用する長所を併せもつことができる。
すなわち、広帯域チャンネルを利用することで、大容量のデータを短時間で伝送ることができる。
一方、制御文は、送られるべき情報量が少ないので、モバイル無線電話網を使用して伝送することが可能である。
【００１４】
モバイル無線電話チャンネルの利用により、最終ユーザの同定（本人確認）と法的な認証が可能となる。
従って、基本的に、有料アプリケーションの利用料を最終ユーザのアカウントに付け替えることが可能になる。
【００１５】
本発明に係る方法の基本的なアイディアは、広帯域チャンネルとモバイル無線電話チャンネルの両方を使用して、セッション形式でデータ伝送できるコネクションを確立することにある。
そのことにより、セッションに関する制御機能、例えば「認証」、「アクセスコントロール」、「送信すべきデータの選択」等は、アプリケーションに基づいてまとめられたコ

ンテンツ、例えば、「画像」、「映画」、「音楽」、「メール」、「添付資料（アペンディクス）」等から厳密に分離される。

【００１６】

機能の実行に際し、「帯域幅」、「ディスプレイの寸法」、「キーボードの形状」等の仕様が、割合に低い要求でもかまわない「制御機能」は、モバイル無線電話チャンネルのみを経由して排他的に実行される。

一方、「伝送速度」、「ディスプレイの寸法」等に対して高度な要求が必要な「データの伝送」については、広帯域アクセスチャンネル経由で実行される。

【００１７】

このようにして、パーソナルモバイル無線データサービスとアノニマス広帯域データアクセスの相乗効果により、例えば、最終ユーザが、自分の個人データに対し、最適なアクセスを行うことができる。

既存のインターネットの使用は、モバイルの使用と同様なセキュリティと個人保護（パーソナリゼーション）をもたらしてくれる。

また、「同定（本人確認）」、「法的な認証」、および「モバイル使用の管理」といった既知の有益情報も広帯域網内でアクセス可能になる。

【００１８】

少なくとも１つの広帯域端末を、広帯域データの伝送に用いることが望ましい。

例えばモバイル電話のようなモバイル無線電話端末が、制御文の送信に使われることが望ましい。

このようにして、「安全なディスプレイ」、「機密および個人的利用」または「プロテクトされたユーザプログラムの利用」、あるいは「アノニマス広帯域チャンネル経由のコンテンツの利用」等が、モバイル端末からのセッション制御およびコンテンツ制御によって実現される。そこでは、モバイル電話は、いわば、広帯域アクセス用リモート制御としての役割を果たしている。

【００１９】

本発明の方法によれば、最終ユーザの基本登録および／または同定（本人確認）は、制御文の伝送に使用される少なくとも１つのモバイル無線電話チャンンネルを経由して、実際の広帯域データ伝送が始まる前の各時間に実行される。

最も簡単な方法は、モバイル無線電話網のオペレータ（運用管理者）により既に得られているモバイル電話の認証(情報)を利用することである。

【００２０】

さらにIPアドレス（それは、一時的ではあるが、明確に、モバイル電話、つまり最終ユーザに割り当てられいる）を利用して、モバイル無線電話網オペレータは、最終ユーザのＭＳＩＳＤＮの割り当てフォームから、安全に本人確認を決定することができる。

【００２１】

さらにまた、アプリケーションソフトウエアを使用したＳＩＭカードによるアクセスもＡＰＩによって可能であり本人確認に用いられる。

最終的には、特別な法的暫定プロセスの範囲内で、いわゆるＰＫＩシステムに対するセーフ鍵（秘密鍵）方式がモバイル電話に提供され、最終ユーザの同定（本人確認）に使用される。

【００２２】

簡易なＷＡＰシステムに基づき、ユーザネーム及びパスワードを用いて最終ユーザの認証を履行するのは、上記と同じような簡易な方法ではあるが、セキュリティが低いので、有効な方法ではない。

【００２３】

リアルな広帯域データが伝送される前に、最終ユーザは、少なくとも１つのモバイル無線電話チャンネル経由で、広帯域データ伝送が行われることに同意することが望ましい。

このようにすれば、本発明に係る方法の安全性を高めることができる。

【００２４】

また、広帯域伝送により送信されるデータは、最終ユーザによって、少なくとも１つの無線電話チャンネルを利用して選択されることが望ましい。

このようにして、最終ユーザのコントロール下で、広帯域データ伝送のすべてが管理されることが望ましい。

【００２５】

さらに、本発明の大きな利点は、広帯域データ伝送により、広帯域端末を使用している多くのパートナーに同時にデータを送ることが出来ることである。

広帯域データ伝送に参加したいパートナーは、最終ユーザによって、少なくとも１つのモバイル無線電話チャンネル経由で選択されることが望ましい。

このようにすることにより、最終ユーザは、この件にかかるやり方についてもまた、管理権限を持つことができる。

【００２６】

本発明に係る方法は、下記のステップから構成されることが望ましい。

（ａ）本発明に係る方法を実行するプロバイダにより、最終ユーザの基本的な登録がなされ、前記プロバイダによる最終ユーザの同定（本人確認）を明確に行ない、

（ｂ）第１の広帯域端末と前記プロバイダのサーバとの間に広帯域コネクションを確立し、それにより、最終ユーザの同定（本人確認）を行ない，

（ｃ）前記プロバイダのサーバと同定（本人確認）された最終ユーザのモバイル無線電話端末との間に、モバイル無線電話コネクションを確立し、

（ｄ）前記モバイル無線電話コネクションを利用して、広帯域データ伝送を実行することについて、最終ユーザから確認をとり、

（ｅ）ポジティブな確認が得られた場合には、データ伝送を開始する。

【００２７】

上記のポジティブな確認が取れた場合は、前記プロバイダのサーバは、第１の広帯域端末と他の広帯域端末との間に、ルータを通して、自動的に広帯域コネクションを確立することが望ましい。

そして、そのコネクションを経由して第１の広帯域端末にデータを伝送する。

【発明を実施するための最良の形態】

【００２８】

次に、図面に基づき、本発明に係る方法を具体的に説明する。

図１は概略図であり、本発明に係る方法の実施に使用する、種々の機器を示している。

図１において、１０はサーバ、２０はルータ、３０は管理サーバ、４０はアノニマス広帯域端末、５０は最終ユーザのモバイル端末、６０はモバイル端末が使用されるモバイル無線電話網である。

本発明に係る方法により、広帯域端末に伝送されるべきデータは、サーバ１０に記憶される。データが伝送される前に、送られるべきデータが準備される。

データの準備は、アプリケーションにより特化され、また、他のパラメータにも依存する。

例えば、広帯域端末へビデオストリームデータを伝送する場合であるか、またはテクニカルデータを伝送する場合であるかの違いにより、さらには、画像の解像度その他種々のパラメータにより、伝送に使用するバンド幅（帯域幅）は異なる。

【００２９】

発明の下地を作る技術と方法は、有益なものであるが、ここで詳細を述べることは省略する。

本発明に係る方法により伝送されるべき多くの異種データがある場合は、これらデータの目録をつくるとか予めデータを整えておくといった、最終ユーザが利用し易い方法を講じれば非常に便利である。

このような方法をとれば、最終ユーザは、モバイル端末５０を用いて伝送すべきデータを具体的に選択することができるという利点がある。

【００３０】

ルータ２０は、本発明に係る方法のインテリジェント配信センタの役割をする。ルータ２０は、アノニマス広帯域端末４０とサーバ１０との間に設置される。
もし、前もって、アノニマス広帯域端末４０に対する、通信文セッションが管理サーバ３０上で認証されている場合は(詳細は、後述する)、ルータはプロキシサーバのように働き、要求されたデータに対するアクセスのみを許す。
ルータ２０は、サーバ１０から伝送されたデータのみを、それ以上処理することなく、アノニマス広帯域端末４０に伝送する。
この目的のために、結局、アノニマス広帯域端末４０とサーバ１０との間に安全なコネクションが確立され、また再び遮断されなくてはならない。
ルータ２０は伝送レベル上（ネットワーク層）の経路のみを定める。
ルータ２０の他の構成機器への接続は、それぞれのアプリケーションにより異なる。

【００３１】

ルータ２０とサーバ１０との接続は、安全に広帯域方式で行われる。
もっとも確実な方法として、インターネット接続が安全に保護されているＶＰＮがサードサーバーへの接続に用いられる。
ＶＰＮとは、「仮想プライベートネットワーク」という意味である。
有り難いことに、ＶＰＮは、インターネットのようなオープンで保護されていないネット上においても、安全な専用線として構築することができる。
このＶＰＮ上では、無関係なパートナーからのモニタリングやアクセスを拒否して、通信が保護される。

【００３２】

上記のことは、ＶＰＮサーバを経由する、データトラフィックについて、いわゆる「トンネリング」手法をとることにより実現される。（「トンネリング」とは、ルータ間に外から見えないトンネルを作るように経路をつくり、パケットをカプセル化してトンネル内を通す手法）。
トンネリングの構築により、同時にデータの暗号化も行われるので、認証が安全に実施される。

【００３３】

さらに高度の安全性が要求される場合は、専用線の使用も考えられる。
サーバ１０による履行の場合は、ローカルエリアネットワーク、すなわちＬＡＮで構築でき、また簡易な方法では、同一のコンピュータにソフトをインストールするだけで実現できる。

【００３４】

管理サーバ３０と最終ユーザのモバイル端末５０との間では、データ通信接続が維持される。
セッション制御および伝送すべきデータの制御は、前記端末５０による二つの異なった通信によって行われる。
セッション制御のために、本発明に係る方法の実施を行う間、管理サーバは全てのアクセスおよびセッションを管理する。
このため、初期化アクセスの要求毎に、管理サーバ３０は、セッションに属し、かつ、アノニマス広帯域端末４０とモバイル端末５０の両方に適用できるようにつくられている両義のトークンを発生する。
もし、両方のトークンが、モバイル端末５０上で、手動作で、確実に確認されたら、セッションは認証を許可する。

【００３５】

ある場合には、特別のアノニマス広帯域端末４０のため、あるいはセッションの時間間隔のために、ルータ２０が、所望のデータにアクセスすることを指令される。
管理コンピュータ(サーバ)３０は、それ自体または同じモバイル端末上で、同時に種々のセッションを管理することができる。
管理サーバ３０は、全てのセッション情報、例えば、「開始」、「終了」、「要求して

いるアノニマス広帯域端末のアドレス」、「要求されたデータ」、「モバイル端末による認証」等の情報が提供され、その結果、インボイスに関連する最も重要な情報を提供することができる。

【００３６】

セッションのコントロールとは別に、管理サーバ３０は、伝送すべき制御文（コントロールステートメント）を受信することができる。

制御文、例えば、「伝送されるべきデータ」、「伝送されるべきデータの指令」等は、メニューから選択されることが望ましい。

しかしながら、伝送されるべきデータに関する制御文は、管理サーバ３０自体によっては処理されず、結局、ルータ２０を通してサーバ１０に送られ、そこで処理される。

伝送すべきデータに関する制御文は、高度にアプリケーションに特化されているので、その機能についての詳細は、ここで説明することはできない。

送信すべきデータを制御するための特殊なロジックチャンネルが、モバイル端末５０とサーバ１０との間に設置されている管理サーバ３０を通して構築される。

上記ロジックチャネルにより、アプリケーションの仕様に従って、専用のプロトコルが実行される。

【００３７】

アノニマス広帯域端末４０は、技術的にまたはアプリケーション仕様に沿って、割合、自由に設計することができる。

しかしながら、大事なことは（基本的条件は）、データが明確な方法で利用できように作られ、アノニマス広帯域端末４０で、確実に相手を同定し、本人確認ができるということである。

“アノニマス”という言葉は、ここでは次のような意味である。

前記広帯域端末４０が、ソフトウエアまたはハードウエアのコンフィギュレーションによる限定された方法のみにより、プリセットされている、という意味である。

【００３８】

アノニマス広帯域端末４０は、ＷＥＢブラウザにより、公にインターネットにアクセスでき、ＩＰアドレスを通して同定とアドレス確認ができる。

他の利用機器として、ＦＡＸマシンも使えるが、ＤＶＢ（デジタルＴＶ放送）受信機またはビデオストリーミングサーバも使用できる。

それらの装置を利用して、本発明の方法により、モバイル端末５０を経由して、安全に本人確認およびアドレス確認ができる。

【００３９】

モバイル端末５０を利用した広帯域セッションの実務上の管理のため、本発明に係る方法は、モバイル端末５０上で、アプリケーションソフトウエアを実行させることができる。

このアプリケーションソフトウエアは、最終ユーザに対するプライマリユーザインターフェイスを意味している。

アプリケーションソフトウエアは、広帯域チャンネルを経由して管理サーバ３０へ伝送された現在のセッション要求を、最終ユーザへ知らせる。

前記要求は、モバイル端末により排除あるいは受理される。

このようにして、各要求は、管理サーバ３０により発生されたトークンにより認識される。

アノニマス広帯域端末４０により、トークンが比較された後、最終ユーザはモバイル端末上でセッションを確認または拒否することができる。

【００４０】

いくつかのセッション要求が個々に、そして平行して、モバイル端末５０によって、取り扱われる。

それにより、例えば、簡易な方法で、閉されたユーザググループに対して、ｗｅｂキャスティング（放送）が実現できる。

モバイル無線電話網を介して、モバイル端末５０は、例えばＧＰＲＳ，ＵＭＴＳなどで

使用されるパケットを、管理サーバ３０へ伝送するように、コネクションをスイッチさせなくてはならない。
このコネクションが安全に認証されるということが重要である。
このためには、幾つかの方法が考えられる。
最も簡単な方法は、モバイル無線電話網のオペレータ（運用管理者）により既に得られている、モバイル電話による認証を利用することである。
さらにＩＰアドレスは、一時的ではあるが確実にモバイル電話つまり最終ユーザに割り当てられるので、モバイル無線電話のオペレータは、安全に、最終ユーザのＭＳＩＳＤＮの割り当てフォームに基づき、本人確認を行うことができる。

【００４１】

他の方法もまた考えられ、実践される。例えば、アプリケーションソフトウエアから、ＳＩＭカードにアクセスすることもＡＰＩの利用により可能であり、これもまた、本人確認に利用される。
特別な法的プロセスの見地から、ＰＫＩシステムに使われるセーフキーもまたモバイル端末で利用することができ、最終ユーザの認証に使われる。
ユーザ名とパスワードを用いた、管理サーバ３０による認証に基づく、簡易ＷＡＰベースの実行も、また、上記と同様な簡易な方法として実践されるが、セキュリティが低いので得策とはいえない。

【００４２】

上述した、本発明に係る方法について、他の実施例を下記に述べる。
最終ユーザは、公にインターネットにアクセスできる広帯域端末４０から、自分のプライベートサーバ１０上にある、Ｅメールの添付資料を見たいと思うものである。
最終ユーザは、基本的に、本発明に係る方法を実施するプロバイダに登録される。
このプロバイダには、管理サーバ３０もまた配置され、明確に、この管理サーバにより本人確認ができる。
最終ユーザは、例えば、彼のモバイル電話のＳＩＭカードに割り当てられている、パーソナルインターネットページを利用することができる。

【００４３】

Ｅメールの添付資料を見るため、最終ユーザは、アノニマス広帯域端末４０で公にアクセスするので、該端末を介して彼の個人的なインターネットページを開示する。
インターネットページを開示することにより、セッション要求が発生し、管理サーバ３０へ伝送される。管理サーバ３０は、要求されたセッションのために、明確なトークンを発生する。
こうして、管理サーバ３０はこのトークンが同じ最終ユーザの他のパラレルセッションで、まだ使われていないことを保証する。
トークンは、例えば、要求しているアノイマス広帯域端末４０のアドレスとタイムスタンプとから構成されるが、もっと単純な特殊フォントによるサインもある。それについては、管理サーバ３０が、小さなＨＴＭＬページを作成し、それをアノニマス広帯域端末４０に返送する。
このＨＴＭＬページにより、最終ユーザは、アノイマス広帯域端末４０上でトークンをビジュアルに見ることができる。

【００４４】

さらに、ＨＴＭＬページは、次のような仕組み（メカニズム）を含んでいる。
すなわち、アノニマス広帯域端末４０上に表示されるページが、管理サーバ３０により変更または実現化できる、という構成になっている。
これは、例えば、小規模なジャバスクリプト（ＪａｖａＳｃｒｉｐｔ）を用いて、コンテンツの変化に対して、１秒毎に問い合わせをする、いわゆるポーリング手法により実現できる。

【００４５】

さらに、管理サーバ３０は、モバイル無線電話網６０のモバイルデータチャンネルを経

由して、セッション要求およびそれに関連したトークンを最終ユーザのモバイル電話へ送信する。
その結果、最終ユーザは、モバイル電話５０に表示されたトークンと、アノニマス広帯域端末に表示されたトークンとを比較することができる。
もし、トークンが一致すれば、最終ユーザは、モバイル電話５０により、セッション要求を確認して、そのセッションを受け入れる。
この情報確認（アクノレッジ）は、再び、モバイル無線網６０のモバイルデータチャンネルを経由して、管理サーバ３０へ送信される。
【００４６】
セッションは、このようにして管理サーバ３０で同定される。従って、管理サーバ３０は、モバイル電話５０により指示されたその要求を、パーソナルサーバ１０にルータ２０を経由して転送する。
例えば、広帯域インターネットアクセスを利用した、ＶＰＮトンネリング技術により、パーソナルサーバ１０とルータ２０との間に安全なコネクションを確立する。モバイル電話５０とパーソナルサーバ３０との間のプロトコルは、例えば、ＨＴＴＰＳ暗号化方式により、管理サーバのみならず、ルータ２０も伝送されたコンテンツの内容を検知できないようにセキュリティを確実にする。
【００４７】
パーソナルサーバ１０から公にアクセス可能なアノイマス広帯域端末へ伝送されるべきデータの選択と制御は、モバイル電話５０を利用するか、インタラクティブにアノイマス広帯域端末４０を利用することにより、実現できる。
種々の理由から、上記２つの方法を上手く組み合わせることが、結局のところ望ましいことである。
下記の実施例に示すように、上記の制御は、モバイル電話５０を経由することによってのみ実現される。
モバイル電話５０は、モバイル無線電話チャンネルを経由して、パーソナルサーバー１０と恒久的に接続されている。
このコネクションは、管理サーバ３０、ルータ２０を経由し、さらにここからは「ＶＰＮトンネリング」を経由して、パーソナルサーバ１０へと接続されている。
パーソナルサーバ１０は、このコネクションを通して、関連する添付資料とともに、受信したＥメールの選択のために提供される。
その結果、例えば、添付資料そのものではなく、添付資料のファイルネームのみを送信する。
このようにすれば、モバイル無線電話チャンネルを利用した接続に非常に大きな伝送負荷がかかることがなく、過負荷状態になることはない。
上記方法は、また、モバイル電話上に、前記添付資料を記憶させるためのメモリーを備える必要もない。
【００４８】
最終ユーザは、アノニマス広帯域端末４０上に表示されるＥメールの添付資料を、モバイル電話５０により、選択する。
この選択は、モバイル無線電話網を通して、パーソナルサーバ１０に、再送される。
ＨＴＭＬ形式で表示される上記添付資料は、アノニマス広帯域端末４０で利用でき、そこでは、大きな見やすい形式で表示できる。
その結果、Ｅメールの添付資料に含まれているデータは、利用可能な広帯域データチャンネルを経由して、排他的に伝送される。
前記添付資料が表示されたのち、最終ユーザは、自分のモバイル電話５０により、付随的にほかのデータも選択することができ、その対応するデータをモバイル無線電話チャンネルを経由して、パーソナルサーバ１０に伝送することができる。
パーソナルサーバ１０は、従って、検閲のために、広帯域チャンネルを経由して、アノニマス広帯域端末４０で利用可能なＨＴＭＬバージョンの選別ファイルを作成できる。

前記セッションはモバイル電話５０によりクローズされる。

【００４９】

もし、モバイル無線電話チャンネルを経由するコネクションが、最終ユーザにより割り込まれたら、管理サーバ３０に知らされ、セッションは再構築される。

パーソナルサーバ１０は、また通信メッセージを受信できるが、その場合は、それ以上のデータ表示を止める。

ルータ２０とパーソナルサーバ１０との間はＨＴＴＰＳ（暗号化方式の１つでＨＴＴＰ/ＳＳＬともいう）暗号化接続されており、アノイマス広帯域端末４０からの、それ以上のどんな要求も、パーソナルサーバ１０に送信しないように、ルータ２０は再設定される。

管理サーバ３０は、セッションデータをログファイルに書き込み記憶する。

【００５０】

上述した本発明の構成および実施例は、上記に限定されるものではない。この他にもいくつかの実施例が実現されている。

例えば、ストリーミングサーバもまた、モバイル端末を通して、最終ユーザにより選択されることができる。

これにより、いわゆる、「ビデオ・オン・デマンド」プロセスが現実化される。本発明に係る方法によって、ビデオや音楽ストリームが、アノイマスな機器を使用した通信手段により利用できるようになる。

その結果、管理サーバ３０のログイン機能により、セッションの請求処理（インボイシング）が容易になる。

【産業上の利用可能性】

【００５１】

さらに、本発明に係る方法によれば、ＷＥＢインターフエイスでやりとりをするクリティカルなアプリケーションでも、安全なインターネットアクセスが実現できる。

向上した安全性が、ＩＴネットワークシステムに対し、モバイル端末で認証を実現できることを立証した。

インターネットアクセスの明瞭性は、また、モバイル端末を通して実現されたが、セッション時間（間隔）などに限定されるように、まだ、一時的なものである。

このことは、安全なアクセスを向上させるものである。

さらに云うなら、テレビ受信機をトリガーして、そこにパーソナルなデータを表示するために、ＤＶＢ－ＴやＤＶＢ－Ｈ への組み込みも考えられる等本発明の
産業への利用可能性は大きい。

【図面の簡単な説明】

【００５２】

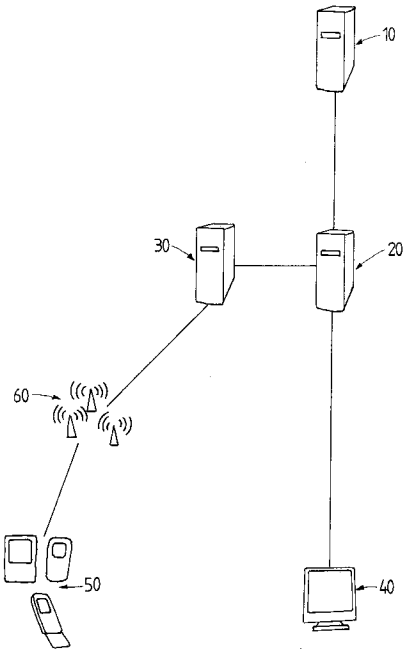
【図１】本発明のシステムを示すステム概略図である。

【符号の説明】

【００５３】

１０　サーバ
２０　ルータ
３０　管理サーバ
４０　アノニマス広帯域端末
５０　最終ユーザのモバイル端末
６０　モバイル端末が使用されるモバイル無線電話網

【図１】



フロントページの続き

(74)代理人 100114890
弁理士 アインゼル・フェリックス＝ラインハルト
(74)代理人 100101764
弁理士 川和 高穂
(72)発明者 アヌープ ナーハー
ドイツ，４０８８５ ラーティンゲン， ベックマンーシュトラーセ ７

審査官 石原 由晴

(56)参考文献 国際公開第０３／０５６８３０（WO，Ａ１）
欧州特許出願公開第０１４９９１２７（ＥＰ，Ａ１）
国際公開第０２／０８４４５６（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｂ ７／２４－７／２６
Ｈ０４Ｗ ４／００－９９／００