(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4469120号
(P4469120)
(45)発行日　平成22年5月26日(2010.5.26)　(24)登録日　平成22年3月5日(2010.3.5)

(51)Int.Cl.　F I
H04L 12/56 (2006.01)　H04L 12/56　B

請求項の数 20　(全 11 頁)

(21)出願番号	特願2001-541213(P2001-541213)
(86)(22)出願日	平成12年11月30日(2000.11.30)
(65)公表番号	特表2003-516042(P2003-516042A)
(43)公表日	平成15年5月7日(2003.5.7)
(86)国際出願番号	PCT/US2000/032513
(87)国際公開番号	WO2001/041401
(87)国際公開日	平成13年6月7日(2001.6.7)
審査請求日	平成19年11月19日(2007.11.19)
(31)優先権主張番号	60/168,978
(32)優先日	平成11年12月3日(1999.12.3)
(33)優先権主張国	米国(US)

(73)特許権者　390035493
エイ・ティ・アンド・ティ・コーポレーション
ＡＴ＆Ｔ　ＣＯＲＰ．
アメリカ合衆国　１００１３－２４１２
ニューヨーク　ニューヨーク　アヴェニュー　オブ　ジ　アメリカズ　３２
(74)代理人　100075258
弁理士　吉田　研二
(74)代理人　100096976
弁理士　石田　純
(72)発明者　ベロービン　スティーブン　マイケル
アメリカ合衆国　ニュージャージー州　ウェストフィールド　キャスルマン　ドライブ　７１０

最終頁に続く

(54)【発明の名称】ドメイン・ネーム内にユーザ情報をエンコードするためのシステムおよび方法

(57)【特許請求の範囲】

【請求項１】

ドメイン・ネームとネットワーク・アドレスの間のマッピングに関するクエリに返答するドメイン・ネーム・システムを有する通信ネットワークで使うためのユーザ情報にアクセスするための、専用ドメイン・ネーム・サーバにおける方法であって、

ポイント・オブ・プレゼンスを介して前記通信ネットワークに接続されたユーザのネットワーク・アドレスに対するドメイン・ネームを返信するためのドメイン・ネーム・システム・クエリを受信するステップと、

前記ドメイン・ネーム・システム・クエリに応答してドメイン・ネーム・システム・レコードを生成するステップと、

前記ドメイン・ネーム・システム・レコード内に、前記ネットワーク・アドレスに関連する前記ドメイン・ネームに加えて、データベースからの情報であって前記接続されたユーザに関する情報を追加するステップと、

を含む。

【請求項２】

請求項１記載の方法において、前記追加情報が、特定のユーザのネットワーク・アドレスにマップされるドメイン・ネーム内にエンコードされる方法。

【請求項３】

請求項１記載の方法において、前記ドメイン・ネーム・システム・レコードを生成するステップが、さらに、前記ドメイン・ネーム・システム・クエリ内において識別された前

記ネットワーク・アドレスを使用して、いずれのユーザが前記通信ネットワークに接続されているかを決定するステップを包含する方法。

【請求項４】

請求項３記載の方法において、前記ドメイン・ネーム・システム・レコードを生成するステップが、さらに、ユーザに関する情報のデータベースを調べて、前記ユーザに関する追加情報を抽出するステップを包含する方法。

【請求項５】

請求項１記載の方法において、前記ユーザに関する追加情報が、暗号鍵を用いて保護される方法。

【請求項６】

請求項５記載の方法において、前記ユーザに関する追加情報の互いに異なる部分が、互いに異なる暗号鍵を用いて保護される方法。

【請求項７】

請求項１記載の方法において、前記ドメイン・ネーム・システム・クエリが、要求されている前記ユーザに関する追加情報のタイプを示す１ないしは複数の値を含み、それにより前記ドメイン・ネーム・システム・クエリ内において指定される前記追加情報のタイプが、前記ドメイン・ネーム・システム・レコード内に含められる方法。

【請求項８】

請求項１記載の方法において、前記追加情報が、前記ユーザに関するアカウント情報を包含する方法。

【請求項９】

請求項１記載の方法において、前記追加情報が、前記ユーザに関する人口統計的情報を包含する方法。

【請求項１０】

請求項１記載の方法において、前記追加情報が、前記ユーザの行為に掛けられる規制を包含する方法。

【請求項１１】

ドメイン・ネームとネットワーク・アドレスの間のマッピングに関するクエリに返答するのに適したドメイン・ネーム・システムを含む通信ネットワークで使われるユーザ情報にアクセスするための装置において、

ポイント・オブ・プレゼンスを介して前記通信ネットワークに接続されたユーザのネットワーク・アドレスに対するドメイン・ネームを返信するためのドメイン・ネーム・システム・クエリを受信する手段と、

前記ドメイン・ネーム・システム・クエリに応答してドメイン・ネーム・システム・レコードを生成する手段と、

前記ドメイン・ネーム・システム・レコード内に、前記ネットワーク・アドレスに関連する前記ドメイン・ネームに加えて、データベースからの情報であって前記接続されたユーザに関する情報を追加する手段と、

を備える装置。

【請求項１２】

請求項１１記載の装置において、前記追加情報が、特定のユーザのネットワーク・アドレスにマップされるドメイン・ネーム内にエンコードされる装置。

【請求項１３】

請求項１１記載の装置において、さらに、前記ドメイン・ネーム・システム・クエリ内において識別された前記ネットワーク・アドレスを使用して、いずれのユーザが前記通信ネットワークに接続されているかを決定する手段を包含する装置。

【請求項１４】

請求項１３記載の装置において、さらに、ユーザに関する情報のデータベースを調べて、前記ユーザに関する追加情報を抽出する手段を包含する装置。

【請求項１５】

請求項１１記載の装置において、前記ユーザに関する追加情報が、暗号鍵を用いて保護される装置。
【請求項１６】
請求項１５記載の装置において、前記ユーザに関する追加情報の互いに異なる部分が、互いに異なる暗号鍵を用いて保護される装置。
【請求項１７】
請求項１１記載の装置において、前記ドメイン・ネーム・システム・クエリが、要求されている前記ユーザに関する追加情報のタイプを示す１ないしは複数の値を含み、それにより前記ドメイン・ネーム・システム・クエリ内において指定される前記追加情報のタイプが、前記ドメイン・ネーム・システム・レコード内に含められる装置。
【請求項１８】
請求項１１記載の装置において、前記追加情報が、前記ユーザに関するアカウント情報を包含する装置。
【請求項１９】
請求項１１記載の装置において、前記追加情報が、前記ユーザに関する人口統計的情報を包含する装置。
【請求項２０】
請求項１１記載の装置において、前記追加情報が、前記ユーザの行為に掛けられる規制を包含する装置。
【発明の詳細な説明】
【０００１】
（発明の分野）
本発明は、概して通信ネットワークに関する。より詳細に述べれば、本発明は分散ネットワークにおけるユーザ情報のストアならびにアクセスに関する。
【０００２】
（発明の背景）
通信ネットワークにおいては、ネットワークによって提供されるサービスのユーザに関する情報を取り込み、使用することが基本的に必要となる――すなわち、それらのサービスを実装するため、それらのサービスに課金するため、異なるサービスのマーケティングのため、あるいはそのほかの何らかの目的のために必要となる。従来の通信ネットワークの基礎となる伝統的なモデルは、その種のユーザ情報を中央データベース内にストアするものであった。この種のデータベースの維持は、困難なことで悪評があり、多数の実用上の実装問題をもたらしている。必然的に、この種の大きな中央データベースは、急速にネットワークにおけるボトルネックとなる。
【０００３】
今日のコンピュータ・ネットワーク環境の基礎となる通信パラダイムは、ユーザ情報のストア並びに拡散に関する新たな困難を招いている。インターネットは、コンピュータ・ネットワークの地球規模のシステムである―すなわち、コンピュータ・セグメントがパケット内にメッセージを収め、それらを、ネットワークを介してインターネット・プロトコル（ＩＰ）アドレスによって識別されるあて先に送るネットワークのネットワークである。分散システム内におけるアドレスは、この分野においてドメイン・ネームと呼ばれる別のよりヒューマン・フレンドリな階層ネーミング・スキームを使用して表現することもできる。たとえば、インターネット上のワールド・ワイド・ウェブ・クライアントは、ネットワーク内のコンピュータを参照するために「www.att.com」といったドメイン・ネームを使用するが、このドメイン・ネーム・システムは、ドメイン・ネームとネットワーク・アドレスの間のマッピングを維持し、それに対するクエリに返答する分散データベースを提供する。P.Mockapetris（Ｐ．モカペトリス）による「Domain names - concepts and facilities（ドメイン・ネーム－コンセプトとファシリティ）」（ＲＦＣ　１０３４，ＩＳＩ，１９８７年１１月）、P.Mockapetris（Ｐ．モカペトリス）による「Domain names - implementation and specification（ドメイン・ネーム－実装および仕様）」（ＲＦＣ

１０３５，ＩＳＩ，１９８７年１１月）を参照されたい。これらは参照によりこれに援用されている。

【０００４】

ユーザ情報は、インターネットまたはワールド・ワイド・ウェブにわたるサービスのプロバイダにとって特に有用なものとなり得る。たとえば、インターネット・サービス・プロバイダ（ＩＳＰ）にとって、ユーザによって提供されたプロファイル情報に基づいて法的もしくは実用的な理由のためにＵｓｅｎｅｔ（ユーズネット）上のニュースグループに対するアクセスを制限すると望ましいことがある。インターネット上のサービスのプロバイダが、よりターゲットを絞ったマーケティングを提供するために、ネットワーク内において誰がサービスを使用しているかについての知識を希望することもある。現在のところ、インターネットならびにワールド・ワイド・ウェブのユーザは、しばしば、使用を希望する個別のサービスのために、個別の認証プロセスを通じてユーザ自身の識別を行い、手続きを進めなければならない。ユーザによって提供された後は、ウェブ・サーバは、いわゆる「ｃｏｏｋｉｅ（クッキー）」と呼ばれる、サーバが状態情報を記録するためにクライアント・サイドにストアするファイル内にユーザ情報をストアすることができる。クッキーは、特定ウェブ・サイトを使用するときのユーザ・プリファレンスをストアし、ユーザ用のウェブ・ページをカスタマイズするため、および／または訪問ごとに異なる広告を提供するために広く使用されている。それにもかかわらず、クッキーの使用には激しい論争が交わされ、各種のプライバシー問題にからめて認識されている。

【０００５】

加入者のプライバシーを保護し、しかもユーザが負担の大きな認証手続を通らなくてもよい、ネットワーク内のサービスを取りそろえるためのユーザに関する情報を伝達する新しい方法が必要とされている。

【０００６】

（発明の要約）

本発明は、ドメイン・ネーム・システムを基礎とするテクニックを使用し、ユーザに関する追加の情報を通信ネットワークに接続されているサービスに提供する。ユーザ情報は、動的に生成され、かつ解釈されるドメイン・ネーム内にストアされてエンコードされる。本発明の一実施態様においては、ポイント・オブ・プレゼンス（point of presence）に、あるいはその近傍に専用ドメイン・ネーム・サーバが置かれ、特定のポイント・オブ・プレゼンスを介して接続するユーザに関するプライベート・ユーザ情報に対するアクセスを有する。サービスは、ドメイン・ネームの与えられたユーザのネットワーク・アドレスを要求する標準ドメイン・ネーム・クエリを使用して、専用サーバによって構成された名前を獲得することができる。この名前は、ユーザ情報の選択された開示のみが許可されるように、異なる鍵によって暗号的にエンコードされた、ユーザに関する情報の各種の断片を含むことが可能である。本発明は、認証可能、かつユーザにトランスペアレントであり、同時にユーザのプライバシーを保護する態様に従って、選択されたユーザ情報をサービスに対して容易に供給できる方法を提供する。

【０００７】

これらの、及びこのほかの本発明の利点は、以下の詳細な説明ならびに添付の図面を参照することによって、当業者においては明らかなものとなろう。

【０００８】

（詳細な説明）

本発明の一実施態様を図解した図１を参照すると、ユーザ１０１がＩＳＰによって運用されているポイント・オブ・プレゼンス（point of presence）（ＰＯＰ）１１０を介してそのＩＳＰに接続している。この接続は、ケーブル・モデム、ＤＳＬライン、衛星リンク、あるいはアナログ電話回線を経由するモデムを用いたＰＯＰへのダイアルを含む、周知の多くの方法のいずれを用いても開設することができる。ＰＯＰ１１０は、インターネット等の通信ネットワーク１５０に対するアクセス・ポイントを提供し、通常はある種の形式の集線装置（aggregator）またはハブ、サーバ、ルータ、および／またはスイッチを含

んでいる。通信ネットワーク１５０は、ある種の形式のドメイン・ネーム・システムを有し、それが、背景において述べたようにドメイン・ネームとネットワーク・アドレスの間のマッピングを維持し、それに関するクエリに返答する分散データベースを提供する。図１においては、ドメイン・ネーム・システムがサーバ１６０として抽象的に表されている。以下の議論は、インターネットおよびインターネット内において使用されるドメイン・ネーム・システム（ＤＮＳ）を用いているが、本発明がそのように限定されることはなく、広く、別のタイプのアドレス対ネーム・マッピング・システムを有する通信ネットワークに適用することができる。

【０００９】

ユーザ１０１がＰＯＰ１１０に接続するとき、そのユーザ１０１に、ネットワーク・アドレスが割り当てられる。インターネットの場合、コンピュータがインターネット・アドレス（ＩＰ）によって識別され、規約によりそれは、たとえば１９１．１９２．１９２．２というように、a.b.c.dの形式に従ってピリオドによって区切られた４つの８ビット値としてしばしば表される３２ビットの数である。ＩＰアドレスは、静的な態様で割り当てることも可能であるが、より多くの場合には、ＩＳＰによって所有されているアドレスのプールから動的に割り当てられる。

【００１０】

本発明の好ましい実施態様によれば、専用ドメイン・ネーム・システム・サーバ１８０がＰＯＰならびにドメイン・ネーム・システムの残部に接続される。専用サーバ１８０は、好適にはＰＯＰと連結されるか、あるいはＰＯＰの統合された一部とすることができる。サーバ１８０には、ＰＯＰによって割り当てられたネットワーク・アドレスを包含するゾーンに関するドメイン・ネーム・システム・クエリに返答する責務が委任される。ＤＮＳクエリに関するサーチ・フィールドの構造、つまりd.c.b.a.in-addr.arpaが、ＩＰアドレスの割り当てが行われる通常の態様に一致していると好都合である。すなわち、単一のＰＯＰが範囲a.b.c内のＩＰアドレスを割当る場合には、単一のＤＮＳサーバにＤＮＳのc.b.a.in-addr.arpaゾーンに関する責務を委任（デリゲート）させることができる。このようにドメイン・ネーム・システムは、ネットワークのトポロジを基礎として自動的な委任スキームを提供する。（ＩＰアドレスのより大きな、あるいはより小さなブロックを割り当てるＰＯＰは、バイト境界上にサブネットが割り当てられないＤＮＳゾーンに対応する。適切な委任（デリゲート）を行うために使用可能な標準テクニックがある。たとえば、M.Crawford（Ｍ．クロウフォード）による「Binary Labels in the Domain Name System（ドメイン・ネーム・システムにおけるバイナリ・ラベル）」（ＩＥＴＦ　ＲＦＣ　２６７３，１９９９年８月）を参照されたい。この文献は、参照によりこれに援用されている。）

【００１１】

ＤＮＳサーバとＰＯＰの連結に代わる方法は、ＤＮＳの動的アップデートを使用することである。たとえば、参照によりこれに援用されている、P.Vixie（Ｐ．ビクシー）編集、S.Thomson（Ｓ．トムソン）、Y.Rekhter（Ｙ．レクター）、J.Bound（Ｊ．バウンド）による「Dynamic Updates in the Domain Name System(DNS UPDATE)（ドメイン・ネーム・システムにおける動的アップデート（ＤＮＳアップデート））」（ＩＥＴＦ　ＲＦＣ　２１３６，１９９７年４月）を参照されたい。この種のシナリオにおいては、ユーザがログインまたはログアウトするとき、ＰＯＰがサービスに変更を通知する。サービスは、ユーザに関する何らかの学習を希望するとき、その名前に関するＤＮＳクエリd.c.b.a.in-addr.arpaを発行する。たとえば図１において、ネットワーク１５０に接続されているサーバ１３０が、現在ＩＰアドレス１９１．１９２．１９２．２を使用していることがそのサーバにわかっているユーザ１０１に関する追加の情報の獲得を希望したとする。サーバ１３０は、ＲＦＣ１０３５において「レゾルバ（resolver）」と呼ばれるオペレーティング・システム・ルーチンを使用し、そのＩＰアドレスから、その名前に関するＤＮＳクエリ、191.192.192.2.IN-ADDR.ARPAを組み立てる。ＤＮＳクエリは、ネーム・サーバ１６０に対して発行されるが、ここで、そのサーバがそのクエリに返答する要求されたリソース・レコ

ードをキャッシュしていないと仮定すると、クエリのタイプに応じてそれが、別のサーバにクエリの発行元を照会するか、あるいは別のＤＮＳサーバに対して独自のクエリを発行する。今日のインターネットに実装されているように、クエリおよび返答は、ともに標準メッセージ・フォーマットで運ばれるが、それについてはＲＦＣ１０３５に記述されている。いくつかのポイントにおいて、ＤＮＳクエリは、ドメイン・ネーム空間の階層構造を通って管理（Authoritative）ネーム・サーバ、つまりサーバ１８０に送られる。サーバ１８０は、標準ＤＮＳサーバとして作用して標準ＤＮＳリソース・レコードを検索することも可能であるが、要求がＰＯＰに接続されているユーザのＩＰアドレスに向けられている場合には、ＤＮＳクエリをユーザ情報として扱って、以下のように手続きを進めることができる。サーバ１８０は、標準ＤＮＳリソース・レコードを検索するというよりは、むしろそのＤＮＳクエリに返答するリソース・レコードを動的に組み立てる。専用ＤＮＳサーバ１８０は、ログインしているユーザのデータベースを調べて、そのドメイン・ネーム内に特定ユーザに関する基本的な情報をエンコードしたドメイン・ネームの組み立てに進む。この種のエンコード済みのドメイン・ネーム用のフォーマットの例を以下に示す。情報は、好ましくは暗号化により保護されるが、それについても後述する。

【００１２】

エンコード済みドメイン・ネームを伴うリソース・レコードは、その後、ドメイン・ネーム・システムを介してサーバ１３０に返される。続いてサーバ１３０は、それが適正な暗号鍵を有していることを前提とすれば、専用ＤＮＳサーバ１８０によって提供されたドメイン・ネームから情報をデコードすることができる。ユーザ情報ＤＮＳリソース・レコードは、ＲＦＣ１０３５内により完全に記載されているフォーマットを有するほかの任意のＤＮＳリソース・レコードと同様に扱うことが可能である。ＤＮＳは、インターネットにおいて実装されているように、タイプ「Ａ」レコードを使用してドメイン・ネーム対アドレスのマッピングを指定し、タイプ「ＰＴＲ」レコードを使用してアドレス対ネームのマッピングを指定する。各種のセキュリティの関係から、多くのＤＮＳのＡＰＩは、返されたＰＴＲレコードを、それに対応するＡレコードについて尋ねることによってクロス・チェックする。言い換えると、上記のように与えられるフォーマットの名前が渡された場合には、これらのＡＰＩが自動的に、その名前に対応するアドレスについて尋ねる。動的サーバ１８０は、データベースに頼ることなくその名前からＡレコードを組み立てることができる。ＩＰアドレスは、３２ビットすべてを含む単一文字列とすることも可能であり、またＰＯＰへの委任（デリゲート）を用意するべく組み立てることもできる。これについてはさらに後述する。

【００１３】

ＤＮＳの返答の完全性（インテグリティ）は、必要であれば標準ＤＮＳセキュリティ・メカニズムの使用によって保証することができる。参照によりこれに援用されているD.Eastlake（Ｄ．イーストレイク）の「Domain Name System Security Extensions（ドメイン・ネーム・システムのセキュリティ機能拡張）」（ＲＦＣ　２５３５，ＩＥＴＦネットワーク・ワーキング・グループ，１９９９年３月）を参照されたい。

【００１４】

ＤＮＳリソース・レコードは、通常、管理（authoritative）ＤＮＳサーバが設定した所定時間にわたり、受信者によってキャッシュされる。期限は、ある種の生存時間（ＴＴＬ）フィールド内に設定される。ＴＴＬパラメータは、通常、リソース・レコードに関して管理（authoritative）ネーム・サーバに掛かる負荷と、別のネーム・サーバのキャッシュ内にあるリソース・レコードがどの程度最新のものに近いかということの間におけるトレードオフを決定する。本発明の場合は、サーバ１８０が、同一ＩＰアドレスの使用の間における時間の最低量に対応する値にＴＴＬパラメータを設定することができる。おそらくは約１分の値が適切となるが、ＴＴＬ値は、必要に応じて調整することができる。この値は、実際、各ＰＯＰにおけるダイアル・イン・レートに応じて動的に調整されている。

【００１５】

通信ネットワークを介して、ユーザのアイデンティティに関する知識を必要とする多数の

サービスが提供される。本発明は、好適に、さらなる入力を行わせる（プロンプトする）ことなく、かつそれに加えてアイデンティティの自動認証を伴った、サービス・プロバイダによるユーザの認識を可能にする。たとえば、多くの会社は、インターネットを介して何らかの自動化された態様によりカスタマ・ケアを提供している。トラブル・チケット・フォーム等の現在のオンライン・カスタマ・ケアのサポート・フォームは、ユーザに対して、ある意味においてネットワークにすでに既知となっている大量の情報の提供を要求する。本発明は、そのフォーム用のデフォルト値を自動的に記入することを可能にする。別の例として、ＩＳＰが、その電子メール（e-mail）システムの悪用に関する苦情を受け取ったとき、いずれのユーザがその責めを受けるべきであるかを追跡することは、他に迷惑を掛けるものとなる。本発明を使用すれば、その情報がＤＮＳネーム内にエンコードされる。

【００１６】

さらに別の例であるが、エイ・ティ・アンド・ティ社は、「Click-to-Dial（クリック・ツー・ダイアル）」と呼ばれるサービスを提供しており、それによりユーザは、ウェブ・ページのリンクをクリックして電話ネットワーク内におけるプロセス、つまり示された宛先及びユーザを呼び出すプロセスを起動することができる。これは、販売者に対して電話カスタマ・サービスへのアクセスを提供する特に容易な手段である。残念ながら、ユーザに対して、ユーザ自身のウェブ・ブラウザに電話番号を組み込むように要求することは、多くの欠点を有している：ユーザにとっては不快であり、エイ・ティ・アンド・ティ社を以外の他者がその電話番号を取り出せた場合にはプライバシーの侵害となり、さらには認証の問題も存在する。悪意を持った個人が偽の電話番号を供給し、何も知らない犠牲者を、たとえば性的内容があからさまに示された有料サービス等、希望していない電話番号に接続させるといったことを許容することは好ましくない。本発明を用いれば、認証が可能であり、かつ実際のユーザを突きとめることが可能な方法に従って電話番号等のユーザ情報を提供するための効果的なメカニズムが提供される。（なお、いくつかの予見しておくべきことがいまだに存在する。たとえば、２人のユーザがＩＲＣを同時に使用している場合、一方が他方のＩＰアドレス、したがってＤＮＳネームを知る可能性がある。ダイアル要求は、このサービスに加入している販売者からだけ到来し、ウェブ接続を行うために使用されるＩＰアドレスを含んでいる必要がある―プロキシ・ウェブ・サーバが使用されている場合には、それが適正に機能しない。）

【００１７】

Ａ．ネーム・フォーマット

次に示すネーム・フォーマットは、ドメイン・ネーム内にエンコードが可能な情報のタイプの一例に過ぎず、限定的あるいは決定的であることが意図されたものではない。以下の例は、通常のインターネット・サービス・プロバイダが希望する可能性の高い種類の情報をエンコードしている。

【００１８】

subaccount.account.restrict.demog.ind.IPaddr.Q.WORLDNET.ATT.NET

Ｑフィールドは、有意的な（セマンティックな）目的に使われるものではない。むしろこれは、この種の情報エンコード済みの名前に関するすべてのルックアップを自動的に適切な動的サーバ（以下、発明者による「Ｑ・サーバ」という呼称を使用する）のセットに向けるために有用となる。多くのこの種のサーバは、「Ｑ」タイプのドメイン・ネームに関するこれらの特殊なクエリを提供することができる。それに代えて、サーバを、たとえば「ＱＡ」、「ＱＢ」等のグループに分けることも可能であり、おそらくは地理的ならびに暗号化の側面の両方から分けられる。後者は、米国外の運用に関して、特に暗号化用の装置（ギア）の輸出に関する規制を前提とするとき有利であると見られる。

【００１９】

Ｑの手前のフィールドは、ＩＰアドレス（ＩＰａｄｄｒ）および「ｉｎｄ」フィールドを除いて、以下に説明するように暗号的に保護されている。「ｉｎｄ」フィールドは、暗号インジケータである。これは、残りのフィールドを保護するために、どの鍵セットが使用

されているかを示し、それにより鍵の変更が可能になる。標準的な暗号使用に加えて、鍵が変更できることは、Ｑ・サーバを維持するエンティティによる特定の限られた目的のための、また特定の週もしくは月といった制限された期間の鍵の提供または販売を可能にする。

【００２０】

「ｄｅｍｏｇ」フィールドは、ＰＯＰオペレータが有し、他への提供を望んでいる何らかのユーザの人口統計的情報をエンコードする。可能性のある候補として、ユーザについてＰＯＰオペレータが知っているほとんどすべてのものを含めることができる。たとえば、ＺＩＰ（ジップ）またはＺＩＰ＋４（ジップ・プラス・フォー）コード（郵便番号に相当する）、実際にダイアルされた電話番号（したがって、その者が「ロード・ウォーリア」であるか否かを示す）、料金プラン（５時間／月プランを申し込んでいる者がヘビー・インターネット・ユーザでないことは明らかである）、および可能性としては、その者が最近ログしたオンライン時間数の表示を挙げることができる。

【００２１】

「ｒｅｓｔｒｉｃｔ」コードは、このユーザに設けられている規制を示し、特に適切なコンテンツのタイプを示す。これらは、機能的（「アダルト・コンテンツ」の規制等）もしくはカテゴリ・ベース（「シンガポール人」、「サウジアラビア人」、「ドイツ人」等）のいずれにすることもできる。ユーザに、複数のこの種の規制を適用することもできる。この種の情報は、アダルト・コンテンツを提供するウェブ・サイトのオペレータに提供されると、非常に有用なものとなり得る。

【００２２】

「ａｃｃｏｕｎｔ」および「ｓｕｂａｃｃｏｕｎｔ」フィールドは、ユーザのアカウント名およびそれに代わる「スクリーン・ネーム」またはサブアカウントを示す。この種のサブアカウントを（たとえばほかの家族会員用に）設定したアカウントのオーナーは、前述したように、そのアカウントに対して新しい規制を設けることができる。

【００２３】

当然のことながら、このほかのフィールドを追加することもできる。オプションのフィールドは、タイプ・コードを伴うフィールドに先行させることにより指定することもできる。

【００２４】

Ｂ．暗号化エンコーディング

適切な暗号化技術によって、希望に応じて最小限に、あるいは最大限にユーザに関する秘匿を行うことが可能であり、また残りを機密にして特定の暗号鍵を販売することもできる。暗号分野の当業者であれば、上記の情報をエンコードするための、多数の暗号化方法のいずれかを案出することが可能であり、それも本発明の下に企図されている。望ましい場合には、情報の一部を暗号化せずに残し、誰もがそれを見ることができるようにもできる。この情報は、暗号的に認証を行うことが可能である。

【００２５】

「コード・ブック」コレクションに対して修正可能でない形式でデータをエンコードすることは好ましい。たとえば所定のユーザが連続する２日間にわたってサービスに接続したか否かを部外者が知り得るようにすることが望ましくないことがある。その種のデータを独自に収集するサービスに関する別の方法もあるが（たとえばwww.doubleclick.comによって使用されているクッキーベースのメカニズムを参照されたい）、上記のドメイン・ネームの使用では、プライバシーの問題として、サービスによってこれが行われることを容易にするべきではないとする。規制コードおよび人口統計的情報等の別のデータは、さらに影響を受けやすく、特に部外者が、部外者の知る個人の何かと、それに関連付けされている現在のＤＮＳネームの間における相関を見つけることができる場合にはそれが顕著になる。したがって、異なるログイン・セッションの間において、同一の情報が異なってエンコードされることが望ましい。さらに言えば、単一ログイン・セッションの間においてさえ、同一情報をＩＳＰに返す理由がなく、いくらかの時間を置いて２つのクエリがある

場合には特にそれに該当する一アカウントの使用が無制限の者は、しばしば長い時間にわたってログインのままにしていることがある。

【００２６】

しかしながら、この暗号化テクニックを現在のドメイン・ネーム・スキームとともに使用することは、返される名前の長さによる拘束を受ける。現実的な問題として、ドメイン・ネームは２５６文字より短くなければならない。これは、この種のテクニックを暗号ブロック連鎖方式として排除する。それに代えて、本発明の好ましい実施態様においては、８ビットの「暗号フィードバック」モード（ＣＦＢ－８）の使用が推奨されている。ＣＦＢ－８は、各バイトが個別に暗号化されるという特性を有する；しかしながら、生成される暗号テキスト値は、先行する８バイトに依存する。暗号化エンジンの初期状態は、「初期化ベクトル」（ＩＶ）によって設定される。これは、鍵が割り当てられた時点において選択することができる。各暗号には、３つの乱数バイトの暗号が先行する。これは、2^{24}個の可能性のあるフィールドの残りの部分の暗号を提供し、本発明の目的においてそれは充分な大きさである。

【００２７】

暗号の出力は、１６進数を用いてエンコードされる必要がある。ＢＡＳＥ６４等を使用することが好ましいが、残念ながら現在のところ、ＤＮＳネームは、ケース・インセンシティブであり、充分なアルファベットを提供しない。

【００２８】

各フィールドは、個別の鍵／ＩＶペアを使用して暗号化される必要がある。いずれのブロック暗号（３ＤＥＳまたはＡＥＳ等）も本発明の目的に関して充分である。結果は、各フィールドが独立に平文化できるようになるが、１つのフィールドの鍵を知ることによっても別のフィールドの平文化は可能にならない。

【００２９】

鍵管理の簡素化のために、各フィールドに関する個別の鍵を、シード値およびマスタ・キーから暗号的に生成することができる。たとえば、人口統計フィールド（「ｄｅｍｏｇ」フィールド）に関する実際の鍵を、タイプ値、サーバ・クラス（ＱＡ、ＱＢ等）、およびその週の「ｉｎｄ」フィールドを連結して暗号化することによって生成することができる。生成されたこの鍵は、カスタマに対する販売対象とすることができる。しかしながら、マスタ・キーを知らなければ、翌日または翌週の人口統計鍵を取り出すことはできないことになる。同時に、毎日各ＰＯＰに対して新しい鍵を配付することも必要なくなる。

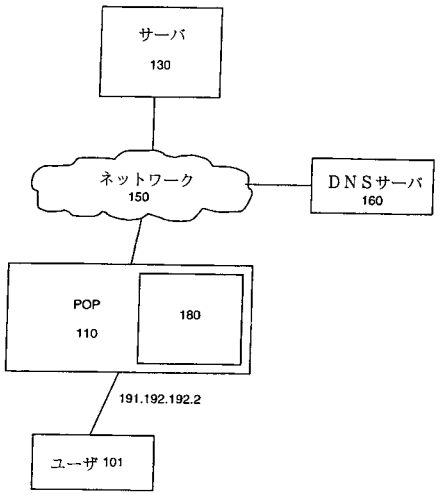
【００３０】

以上の詳細な説明は、あらゆる点において例示的かつ説明的なものであり、限定的ではないものと理解するべきであり、ここに開示されている本発明の範囲は、この詳細な説明から決定されるべきでなく、特許法の下に許容される完全な広さをもって解釈される特許請求の範囲から決定されるものとする。ここに示し、説明した実施態様は、本発明の原理の例示に過ぎず、当業者にあっては、本発明の範囲ならびに精神から逸脱することなく、各種の修正を実施することができよう。たとえば、詳細な説明においては、本発明がインターネットのＤＮＳを伴う使用に特に重点を置いて説明されている。しかしながら、本発明の原理を、アドレス対ネーム・マッピング・システムを有する別のネットワークに拡張することは可能である。

【図面の簡単な説明】

【図１】　本発明の一実施形態に係る通信ネットワークを表す概略図である。

【図１】



フロントページの続き

審査官　齋藤　浩兵

(56)参考文献　米国特許第５８１５６６５（ＵＳ，Ａ）
特表平１１－５０７７５２（ＪＰ，Ａ）
特開平１０－１１１８４８（ＪＰ，Ａ）
P.VIXIE, RFC2671:Extension Mechanisms for DNS (EDNS0), REQUEST FOR COMMENTS 'ON LINE!', １９９９年　８月　１日, ＵＲＬ, http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2671.txt
M.CRAWFORD, RFC2673:Binary Labels in the Domain Name System, REQUEST FOR COMMENTS 'ON LINE!', １９９９年　８月　１日, ＵＲＬ, http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2673.txt

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 12/56