(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2013-201618
(P2013-201618A)
(43)公開日　平成25年10月3日(2013.10.3)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/70	(2013.01)	H04L	12/56	B	5K030
G06F 21/62	(2013.01)	G06F	21/24	166A	

審査請求 未請求　請求項の数 8　ＯＬ　（全 15 頁）

(21)出願番号　特願2012-68948(P2012-68948)
(22)出願日　平成24年3月26日(2012.3.26)

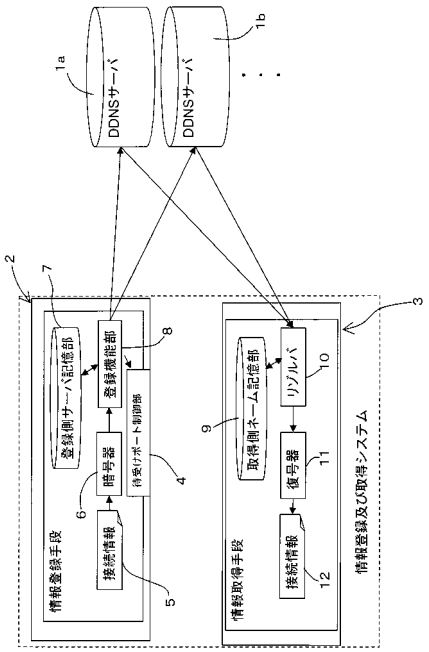
（特許庁注：以下のものは登録商標）
１．ＥＴＨＥＲＮＥＴ

(71)出願人　399041158
西日本電信電話株式会社
大阪府大阪市中央区馬場町３番１５号
(74)代理人　100074206
弁理士　鎌田　文二
(74)代理人　100084858
弁理士　東尾　正博
(74)代理人　100112575
弁理士　田川　孝由
(72)発明者　中川　知子
大阪府大阪市中央区馬場町３番１５号　西日本電信電話株式会社内
(72)発明者　川邊　隆伸
大阪府大阪市中央区馬場町３番１５号　西日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】情報登録及び取得システム

(57)【要約】
【課題】認証機能付きのデータベースサーバを用意することなく、ユーザのプライベートな情報を第三者に対して安全に登録しておき、インターネット経由で取得可能にする。
【解決手段】公開サーバとなる情報登録手段２は、自己のホスト名の登録先であるＤＮＳサーバとして機能するデータベースサーバ１ａ、１ｂのＩＰアドレスを登録先記憶部７で記憶し、自己へのリモートアクセスに要する所定情報５を暗号器６で暗号化し、登録機能部８で暗号文を情報登録手段２のホスト名の見せかけのＩＰアドレスとしたＤＮＳの登録要求をサーバ１ａ、１ｂのＩＰアドレスへ送信する。クライアントとなる情報取得手段３は、登録先記憶部７と同じ内容で名前解決要求先をネーム記憶部９で記憶し、情報登録手段２へアクセスする際、リゾルバ１０でサーバ１ａ、１ｂから取得した見せかけのＩＰアドレスを復号器１１で所定情報１２に復元する。
【選択図】図１



【特許請求の範囲】
【請求項１】
所定のデータベースサーバにネットワークを介して接続する情報登録手段と、
前記所定のデータベースサーバにインターネット経由で接続する情報取得手段とからなる情報登録及び取得システムにおいて、
前記データベースサーバは、ＤＤＮＳサーバからなり、
前記情報登録手段は、
自己に割り当てられたホスト名と前記データベースサーバのＩＰアドレスを対応付けた登録先を記憶する登録側サーバ記憶部と、
前記情報取得手段で取得するための所定情報を暗号化する暗号器と、
前記登録先として記憶されたデータベースサーバのＩＰアドレスへ、前記暗号器で得られた暗号文をＩＰアドレスに見せかけたＤＮＳの登録要求を送信する登録機能部とを有し、
前記情報取得手段は、
前記登録側サーバ記憶部と同一のホスト名を記憶する取得側ネーム記憶部と、
前記取得側ネーム記憶部に記憶されたホスト名の名前解決要求を送信するリゾルバと、
前記リゾルバが取得した前記見せかけのＩＰアドレスを前記所定情報に復号化する復号器とを有する、
ことを特徴とする情報登録及び取得システム。
【請求項２】
前記取得側ネーム記憶部は、前記登録側サーバ記憶部と同一の前記登録先を記憶し、
前記リゾルバは、前記取得側ネーム記憶部に記憶された前記データベースサーバのＩＰアドレスへ、当該ＩＰアドレスに対応付けられたホスト名の名前解決要求を送信する請求項１に記載の情報登録及び取得システム。
【請求項３】
前記データベースサーバは、前記名前解決要求に対するＤＮＳ応答をＴＴＬ０秒指定で返信する請求項１に記載の情報登録及び取得システム。
【請求項４】
前記登録側サーバ記憶部は、複数の前記登録先を記憶し、
前記登録機能部は、前記暗号文を前記複数に分割し、各分割データから見せかけのＩＰアドレスを作成し、これら見せかけのＩＰアドレスを前記複数の登録先に１つずつ割り当てて前記登録要求を送信する請求項２に記載の情報登録及び取得システム。
【請求項５】
前記登録側サーバ記憶部は、複数の前記ホスト名を記憶し、
前記登録機能部は、前記暗号文を前記複数に分割し、各分割データから見せかけのＩＰアドレスを作成し、これら見せかけのＩＰアドレスを前記複数の登録先に１つずつ割り当てて前記登録要求を送信する請求項１又は３に記載の情報登録及び取得システム。
【請求項６】
前記情報登録手段は、グローバルＩＰアドレスをもち、
前記所定情報は、前記情報登録手段へのインターネットを介したリモートアクセスに用いるための接続情報からなる請求項１から５のいずれか１項に記載の情報登録及び取得システム。
【請求項７】
前記情報登録手段は、前記リモートアクセス用に開ける待受けポート番号を所定時期の経過ごとに変更し、変更した待受けポート番号と有効期限とを含んだ前記所定情報を暗号化して前記ＤＮＳの登録要求を送信する請求項６に記載の情報登録及び取得システム。
【請求項８】
前記グローバルＩＰアドレスが、動的に割り当てられるＩＰｖ４アドレスである請求項６又は７に記載の情報登録及び取得システム。

【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、所定のデータベースサーバにネットワークを介してユーザの情報登録手段でデータ登録を行い、ユーザの情報取得手段で前記所定のデータベースサーバからインターネット経由でデータ取得を行うための情報登録及び取得システムに関する。
【背景技術】
【０００２】
常時接続サービスを利用して自宅のＰＣなどをＷｅｂサーバとして公開する際に使用するアドレス解決方法としてＤＤＮＳ（ＲＦＣ２１３６で仕様化されたＤｙｎａｍｉｃ Ｕｐｄａｔｅｓ ｉｎ ｔｈｅ Ｄｏｍａｉｎ Ｎａｍｅ Ｓｙｓｔｅｍ）が利用されている。ＤＤＮＳでは、人間に覚え辛い文字と数字の列であるＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）アドレスと、ユーザが一意に指定した理解容易な文字列からなるホスト名を紐付けてＤＤＮＳサーバで管理する。外部から自宅のＰＣなどにリモートアクセスをする端末は、ＤＤＮＳサーバに名前解決を依頼し、ホスト名からＩＰアドレスを取得することができる。プロバイダからＰＣなど払い出されるＩＰアドレスが動的に割り当てられる場合、ＰＣなどがプロバイダのインターネット接続サービス網に接続するたびに不規則に変更される可能性がある。その接続の都度、ＤＤＮＳサーバへ新しく割り当てられたＩＰアドレスを登録することで、ＩＰアドレスが変更されても同じホスト名でリモートアクセスすることが可能となる（例えば、特許文献１、２）。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２０１１－１０８２３２号公報
【特許文献２】特開２００４－１２０１２３号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、一般にＤＤＮＳはインターネットに対してオープンなサービスであり、ＤＤＮＳサーバに登録されたＩＰアドレスは、ホスト名さえ知っていれば誰でも取得することが可能である。プライベートで使用しているＶＰＮレスポンダのアドレスを外部から取得したい場合等、インターネットに対して秘匿したいがユーザ側がインターネット経由で取得したいプライベートな情報の場合、ＤＤＮＳサーバのようにオープンなデータベースサーバへ係る情報を登録することは、セキュリティの観点から適当ではない。係る登録には、ユーザ認証機能付きのデータベースサーバを用意しなければならなかった。
【０００５】
そこで、この発明が解決しようとする課題は、認証機能付きのデータベースサーバを用意することなく、ユーザのプライベートな情報を第三者に対して安全に登録しておき、インターネット経由で取得可能にすることである。
【課題を解決するための手段】
【０００６】
上記の課題を解決するため、この発明は、要するに、データベースサーバとしてＤＤＮＳサーバを活用し、ユーザのプライベートな情報を第三者に対して安全にＤＤＮＳサーバに登録する仕組みを情報登録手段と情報取得手段に実装することにより、認証機能付きのデータベースサーバを不要にした。すなわち、情報登録手段は、自己のホスト名と、この登録先にするＤＤＮＳサーバのＩＰアドレスとを対応付けた登録先を記憶し、前記情報取得手段で取得するための所定情報を暗号化し、その暗号文を自己のホスト名に対応するＩＰアドレスに見せかけたＤＮＳの登録要求を所定のＤＤＮＳサーバに送信する。このため、ＤＤＮＳサーバには、情報登録手段に割り当てられたホスト名と、見せかけのＩＰアドレスが登録され、所定情報自体は登録されない。プライベートな所定情報であれば、情報

登録手段のユーザと情報取得手段のユーザは、同じアクセス権限をもつ者に限定される。したがって、情報登録手段には、前記の登録先に関する情報の共有と、前記所定情報に復号化するための情報の保持を許すことができる。すなわち、情報取得手段は、情報登録手段に記憶された登録先と同一のホスト名を記憶し、記憶されたホスト名の名前解決要求をリゾルバで送信し、ＤＮＳ（Ｄｏｍａｉｎ　Ｎａｍｅ　Ｓｙｓｔｅｍ）を介し、所定のＤＤＮＳサーバに登録されている見せかけのＩＰアドレスを取得し、見せかけのＩＰアドレスを前記所定情報に復号化する。したがって、情報取得装置のユーザは、インターネット経由で前記所定情報を取得することができる。情報取得装置をもたない第三者は、何らかの端末から仮に情報登録手段のホスト名の名前解決を要求し得ても、無意味な見せかけのＩＰアドレスを入手できるだけであり、前記所定情報を知ることはできない。したがって、ユーザのプライベートな情報を第三者に対して安全にＤＤＮＳサーバに登録しておくことができる。

【０００７】

前記リゾルバが前記ホスト名の名前解決要求を送信する問い合わせ先は、ＤＮＳに属しているネームサーバの中から任意に定めることができ、具体的には、ＤＮＳの最上位に位置するルートサーバ、ルートサーバより下位のドメインを管理するＤＮＳサーバ、前記所定のＤＤＮＳサーバのいずれでもよい。所定のＤＤＮＳサーバを問い合わせ先にすると、ルートサーバから下位のＤＮＳサーバへ再帰的に問い合わせを行う場合と比して、見せかけのＩＰアドレスを取得するまでの待ち時間を省力することができる。

【０００８】

具体的には、前記情報取得手段が前記情報登録手段と同一の前記登録先、すなわち情報登録手段と同じ内容で前記ホスト名と前記ＤＤＮＳサーバのＩＰアドレスを対応付けた情報を記憶し、前記リゾルバが前記所定のＤＤＮＳサーバに前記ホスト名の名前解決要求を送信すれば、前記の待ち時間を省力することができる。

【０００９】

前記情報取得手段と前記ＤＤＮＳサーバ間に他のＤＮＳサーバが介在することを許容する場合、ＤＤＮＳサーバは、前記名前解決要求に対するＤＮＳ応答において当該応答を中継保持するＤＮＳサーバにおけるキャシュ時間であるＴＴＬ（Time To Live）を比較的短い値に指定して返信することが好ましい。特に、前記情報登録手段により頻繁に情報を更新する場合には、TTLを0とする。これにより、名前解決要求のＤＤＮＳサーバへの到達性は、他のＤＮＳキャッシュサーバによるキャッシュ利用の応答で遮断される心配がないため、確実である。したがって、必ずＤＤＮＳサーバで解決されて情報取得手段へ返信されるので、情報取得手段は最新の見せかけのＩＰアドレスを確実に取得することができる。

【００１０】

前記情報登録手段による登録先を複数にすれば、暗号文から複数の見せかけのＩＰアドレスを作り、複数の登録先へ暗号文を分散登録することができ、第三者による暗号文全文の取得が困難になる。また、ＩＰアドレスサイズより大きな暗号文であっても、既存のＤＤＮＳサーバの利用が可能となる。前記登録先を複数作成するパターンとして、１個のホスト名と複数のＤＤＮＳサーバのＩＰアドレスとの組み合わせＡ、複数のホスト名と１個のＤＤＮＳサーバのＩＰアドレスとの組み合わせＢ、複数のホスト名と複数のＤＤＮＳサーバのＩＰアドレスとの１対１の組み合わせＣが挙げられる。

【００１１】

例えば、前記情報登録手段に記憶された登録先と同一の登録先を前記情報取得手段が記憶する場合、前記組み合わせＡ～Ｃのいずれでも採用することが可能である。したがって、前記情報登録手段が、複数の前記登録先を記憶し、前記暗号文を前記複数に分割し、各分割データから見せかけのＩＰアドレスを作成し、これら見せかけのＩＰアドレスを前記複数の登録先に１つずつ割り当てて前記登録要求を送信することにより、前記の分散登録を実現することができる。

【００１２】

一方、前記情報登録手段に記憶された登録先に係るホスト名のみを前記情報取得手段が

記憶する場合、１個のホスト名しか利用できない前記組み合わせＡを採用することはできない。この場合、組み合わせＢ又はＣを採用すれば、登録先に係るＤＤＮＳサーバのＩＰアドレスを情報取得手段に記憶させずとも、前記の分散登録を実現することができる。具体的には、前記情報登録手段が、複数の前記ホスト名を記憶し、前記暗号文を前記複数に分割し、各分割データから見せかけのＩＰアドレスを作成し、これら見せかけのＩＰアドレスを前記複数の登録先に１つずつ割り当てて前記登録要求を送信することにより、前記の分散登録を実現することができる。

【００１３】

この発明は、プライベートに用いる情報登録手段のグローバルＩＰアドレスへインターネットからアクセスするための方法としてＤＤＮＳを利用しつつ、当該グローバルＩＰアドレスへのアクセス権限をもたない第三者による情報登録手段へのアクセスを防ぐ目的に使用することができる。すなわち、前記情報登録手段は、グローバルＩＰアドレスをもち、前記所定情報は、前記情報登録手段へのインターネットを介したリモートアクセスに用いるための接続情報からなるようにすればよい。このように所定情報をリモートアクセス用の接続情報に限定すれば、暗号文のサイズを抑え、情報登録手段のために確保すべきホスト名の数やＤＤＮＳサーバのリソース消費を抑えることができる。情報登録手段のグローバルＩＰアドレスは動的、固定のいずれでもよいが、動的に割り当てられる場合であっても、情報登録手段はＤＤＮＳクライアントなので、グローバルＩＰアドレスの更新を契機に新たな所定情報を暗号化してＤＤＮＳサーバへ再登録する自動処理が可能である。

【００１４】

例えば、情報登録手段は、リモートアクセス用に開ける待受けポート番号を所定時期の経過ごとに変更することが好ましい。これにより、外部から待受けポートへの攻撃を所定時期の経過でかわすことができる。情報登録手段が、変更した待受けポート番号と有効期限とを含む前記所定情報を暗号化して前記ＤＮＳの登録要求を送信するようにしておけば、動的な待受けポート番号であっても、情報取得手段は、復元した接続情報中の待受けポート番号及び有効期限から情報登録手段にアクセス可能な待受けポートを知ることができる。

【００１５】

前記情報登録手段のグローバルＩＰアドレスが動的に割り当てられるＩＰｖ４アドレスの場合、普及している既存のＩＰｖ４ネットワークのＤＤＮＳを利用することができる。なお、グローバルＩＰアドレスが動的又は固定のＩＰｖ６アドレスである場合でも、ＩＰｖ４用又はＩＰｖ６用のＤＤＮＳサーバを適宜に利用して、この発明を適用することができる。

【発明の効果】

【００１６】

上述のように、この発明は、所定のデータベースサーバにネットワークを介して接続する情報登録手段と、前記所定のデータベースサーバにインターネット経由で接続する情報取得手段とからなる情報登録及び取得システムにおいて、前記データベースサーバは、ＤＤＮＳサーバからなり、前記情報登録手段は、自己に割り当てられたホスト名と前記データベースサーバのＩＰアドレスを対応付けた登録先を記憶する登録側サーバ記憶部と、前記情報取得手段で取得するための所定情報を暗号化する暗号器と、前記登録先として記憶されたデータベースサーバのＩＰアドレスへ、前記暗号器で得られた暗号文をＩＰアドレスに見せかけたＤＮＳの登録要求を送信する登録機能部とを有し、前記情報取得手段は、前記登録側サーバ記憶部と同一のホスト名を記憶する取得側ネーム記憶部と、前記取得側ネーム記憶部に記憶されたホスト名の名前解決要求を送信するリゾルバと、前記リゾルバが取得した前記見せかけのＩＰアドレスを前記所定情報に復号化する復号器とを有する構成の採用により、認証機能付きのデータベースサーバを用意することなく、ユーザのプライベートな情報を第三者に対して安全に登録しておき、インターネット経由で取得可能にすることができる。

【図面の簡単な説明】

【００１７】
【図１】実施形態に係る情報登録及び取得システムの全体構成を示す機能ブロック図
【図２】実施形態に係る情報登録及び取得システムのネットワーク構造を模式的に示す図
【図３】実施形態に係る登録側サーバ記憶部、取得側ネーム記憶部の管理テーブルの概念図
【図４】実施形態に係る情報登録手段がＤＤＮＳサーバに登録するフローチャート図
【図５】実施形態に係る登録機能部がＤＤＮＳサーバへの登録を更新するフローチャート図
【図６】実施形態に係る情報取得手段が接続情報を取得するフローチャート図
【図７】実施形態に係る接続情報の情報伝達を示す機能ブロック図
【図８】実施形態の変更例における図６相当のフローチャート図
【図９】実施形態の変更例における図８相当の機能ブロック図
【図１０】実施形態の変更例における図３相当の管理テーブルの概念図
【発明を実施するための形態】
【００１８】
以下、この発明に係る情報登録及び取得システムの一実施形態（以下、単に「このシステム」と呼ぶ）を図面に基づいて説明する。このシステムは、図１、図２に示すように、所定のデータベースサーバとしてのＤＤＮＳサーバ１ａ、１ｂ・・・にネットワークを介して接続する情報登録手段２と、前記所定のＤＤＮＳサーバ１ａ、１ｂ・・・にインターネット経由で接続する情報取得手段３とからなる。
【００１９】
情報登録手段２は、インターネットに接続される。情報登録手段２は、所定のホスト名をもち、ＰＰＰｏＥ（ＰＰＰ ｏｖｅｒ Ｅｔｈｅｒｎｅｔ）接続やＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）によりグローバルＩＰアドレスを動的に割り当てられる（以下、このグローバルＩＰアドレスを単に「動的ＩＰアドレス」と呼ぶ）。例えば、情報登録手段２は、ユーザ宅のパーソナルコンピュータ、ゲートウェイ装置といった通信機器からなる。情報登録手段２は、ＤＤＮＳサーバ１ａ、１ｂ・・・のサービスを利用するクライアント端末となり、インターネットを介して自己へリモートアクセスする情報取得手段３に対して自己に実装されたソフトウェア等の機能をプライベートに提供する目的でインターネットに公開されたサーバとなる。
【００２０】
情報登録手段２は、待受けポート番号の変更を制御する待受けポート制御部４を有している。待受けポート番号は、情報取得手段３からのリモートアクセス用に開ける論理的ポートを特定する番号である（以下、単に「ポート番号」と呼ぶ）。待受けポート制御部４は、インターネットに開放する待受けポート番号を所定時期の経過ごとに変更する。具体的には、待受けポート制御部４は、情報登録手段２のＷＡＮ側通信ポートに設定可能な所定のポート番号の中で、情報取得手段３が情報登録手段２へのリモートアクセスに用いる待受けポートとして接続情報５に含められたポート番号を、接続情報５の有効期限までリモートアクセス用の待受けポートとして設定し、接続情報５の更新に合わせて待受けポート設定を更新する。
【００２１】
接続情報５は、情報登録手段２に割り当てられた動的ＩＰアドレスと、待受けポート番号を含み、他に、ルート情報、ユーザＩＤ、パスワード、それらが可変の場合には特定のために必要な鍵などを接続情報５に含めることができる。なお、ルート情報とは、特定のサーバを経由して目的のサーバにアクセスするルートの、特定のサーバのアドレスである。情報登録手段２は、割り当てられた動的ＩＰアドレス、待受けポート制御部４によって設定された待受けポート番号、有効期限等の所要の情報を収集して接続情報５を生成する。
【００２２】
また、情報登録手段２は、情報取得手段３で取得するための所定情報を暗号化する暗号

器６を有している。所定情報は、生成した接続情報５からなる。この暗号化に必要な鍵情報は、情報登録手段２に登録されるようになっている。暗号化の方式は特に限定されない。

【００２３】

また、情報登録手段２は、自己のホスト名とＤＤＮＳサーバ１ａ、１ｂ・・・のＩＰアドレスを管理する登録側サーバ記憶部７を有している。情報登録手段２は、登録側サーバ記憶部７に対する情報登録手段２のホスト名の登録と、この登録先に対応するＤＤＮＳサーバのＩＰアドレスの登録とを情報登録手段２のユーザから入力されるようになっている。登録側サーバ記憶部７は、情報登録手段２に割り当てられたホスト名とＤＤＮＳサーバ１ａ、１ｂ・・・のＩＰアドレスを対応付ける管理テーブルによって登録先を記憶する。その管理テーブルは、例えば図１、図３に示すように、情報登録手段２に割り当てられたホスト名（図中の項目名「ホスト名」）、ホスト名を登録するＤＤＮＳサーバのＩＰアドレス（図中の項目名「ＤＤＮＳサーバアドレス」）を所有している。情報登録手段２のホスト名は、ＴＣＰ／ＩＰネットワークのフルドメイン名（ＦＱＤＮ）とする。登録側サーバ記憶部７は、管理テーブルによって、情報登録手段２に割り当てられた全てのホスト名について、ホスト名ごとに登録先を記憶する。また、管理テーブルは、図１の暗号器６で得られた暗号文を複数の登録先に分散登録するために用いる順序情報（図３中の項目名「Ｎｏ．」）も所有している。例えば、図３中「Ｎｏ．１」の登録先は、図３中「●●●１．ｃｏ．ｊｐ」のホスト名と、これを登録する図１のＤＤＮＳサーバ１ａのＩＰアドレスである図３中「１０．１０．１．１」を対応付けた情報になっている。図示例の登録先Ｎｏ．１～Ｎｏ．３は、３個のホスト名と、３個のＤＤＮＳサーバのＩＰアドレスとの１対１の組み合わせ、登録先Ｎｏ．４～Ｎｏ．５は、２個のホスト名と、１個のＤＤＮＳサーバのＩＰアドレスとの組み合わせの関係にあり、５個のホスト名に係る登録先Ｎｏ．１～Ｎｏ．５によって接続情報５の暗号文を３個のＤＤＮＳサーバ１ａ、１ｂ・・・に分散登録することを前提にしている。

【００２４】

また、図１に示す情報登録手段２は、暗号器６で得られた暗号文を所定のＤＤＮＳサーバ１ａ、１ｂ・・・へＤＮＳに従った登録要求を送信する登録機能部８を有している。登録機能部８は、登録側サーバ記憶部７によって登録先として記憶されたＤＤＮＳサーバ１ａ、１ｂ・・・のＩＰアドレスに対して、暗号文をＩＰアドレスに見せかけた前記登録要求を送信する。具体的には、登録機能部８は、暗号文を登録側サーバ記憶部７に記憶された登録先の数に分割し、各分割データから見せかけのＩＰアドレスを作成し、これら見せかけのＩＰアドレスを登録側サーバ記憶部７に記憶された「Ｎｏ」の順序に対応する登録先に１つずつ割り当てて、対応するＤＤＮＳサーバ１ａ、１ｂ・・・のＩＰアドレスに対して登録要求を送信する。

【００２５】

情報登録手段２がＤＤＮＳサーバ１ａ、１ｂ・・・のＩＰアドレスへＤＮＳの登録要求を送信するまでのフローチャートを図４に例示する。情報登録手段２は、接続情報５、接続情報５の有効期限を生成し、暗号器６に投入する（Ｓ１）。暗号器６は、投入された接続情報５等を暗号化した暗号文を作成し、登録機能部３に渡す（Ｓ２）。登録機能部３は、渡された暗号文のサイズを確認する（Ｓ３）。

【００２６】

登録機能部３は、（Ｓ３）において暗号文「Ａ．Ｂ．Ｃ．Ｄ．Ｅ．Ｆ．Ｇ．Ｈ．Ｉ．Ｊ」のサイズがＩＰアドレスより大きい場合、暗号文をＩＰアドレスのサイズ「Ａ．Ｂ．Ｃ．Ｄ」、「Ｅ．Ｆ．Ｇ．Ｈ」、「Ｇ．Ｈ．１．１」に分割、不足部分に「１」を追加し（Ｓ４）、登録側サーバ記憶部７を参照して、各見せかけのＩＰアドレス（すなわち、暗号文の分割片）ごとに紐付けるホスト名を設定し、登録先であるＤＤＮＳサーバ１ａ、１ｂ・・・のＩＰアドレスを取得し（Ｓ５）、各ＤＤＮＳサーバ１ａ、１ｂ・・・のＩＰアドレスに登録要求を送信する（Ｓ６）。

【００２７】

また、登録機能部３は、（Ｓ３）において暗号文「Ａ．Ｂ．Ｃ」のサイズがＩＰアドレスより小さい場合、暗号文の不足部分に「１」を足して暗号文をＩＰアドレスのサイズ「Ａ．Ｂ．Ｃ．１」にする（Ｓ７）。以後、（Ｓ５）、（Ｓ６）の処理に進む。

【００２８】

また、登録機能部３は、（Ｓ３）において暗号文「Ａ．Ｂ．Ｃ、Ｄ」のサイズがＩＰアドレスと同じ場合、以後、（Ｓ５）、（Ｓ６）の処理に進む。

【００２９】

情報登録手段２から登録要求を受信したＤＤＮＳサーバ１ａ、１ｂ・・・は、通常と同じく、当該登録要求のメッセージ中に含まれたホスト名とＩＰアドレス（このＩＰアドレスは問う記録機能部８によって生成された見せかけのＩＰアドレス）を対応付けて自己のテーブルに登録し、このテーブルを参照して名前解決の応答メッセージに含める回答を生成する。

【００３０】

前述のように、登録機能部３は、暗号文のサイズが１つのＩＰアドレスよりも大きくなった場合には、暗号文をＩＰアドレスサイズに分割し、複数のホスト名もしくは複数のＤＤＮＳサーバ１ａ、１ｂ・・・に登録する。その際、ホスト名と登録先のＤＤＮＳサーバ１ａ、１ｂ・・・のいずれか１つとの組合せは登録側サーバ記憶部７にて管理される。暗号文のサイズがＩＰアドレスよりも大きくなった場合、１つのＤＤＮＳサーバに登録される複数のホスト名に暗号文を分割して対応付ける方法、及び複数のＤＤＮＳサーバ１ａ、１ｂ・・・に登録される同一のホスト名に暗号文を分割して対応付ける方法のいずれか一方を採用すること、又は、これら方法を併用することも可能である。

【００３１】

また、登録機能部８は、接続情報中の項目の情報が更新された契機で、例えばＤＨＣＰ等により情報登録手段２に割り当てられた動的ＩＰアドレスが更新された契機で、前述の手順（Ｓ１）～（Ｓ７）にて接続情報５等をＤＤＮＳサーバ１ａ、１ｂ・・・へ再登録する

【００３２】

また、登録機能部８は、図５にフローチャートを例示するように、随時、ＤＤＮＳサーバ１ａ、１ｂ・・・に登録した接続情報５の有効期限を監視し（Ｓ１１）、当該有効期限の直前のタイミングにおいて、ポート番号情報および有効期限を変更し（Ｓ１２）、前述の手順（Ｓ１）～（Ｓ７）にて接続情報５等をＤＤＮＳサーバ１ａ、１ｂ・・・へ再登録する（Ｓ１３）機能をもっている。

【００３３】

図１に示す待受けポート制御部４、暗号器６、登録側サーバ記憶部７、登録機能部８は、情報登録手段２にコンピュータプログラムとして実装されており、情報登録手段２の演算処理装置でコンピュータプログラムを実行することにより、情報登録手段２に備わる演算処理装置、記憶装置、ネットワークインターフェイスといったハードウェア資源上に暗号器６等が構成される。

【００３４】

一方、図１、図２に示すように、情報取得手段３は、インターネットに接続される通信機器からなる。例えば、情報取得手段３は、携帯電話、パーソナルコンピュータ等といった端末からなる。情報取得手段３は、ＤＤＮＳサーバ１ａ、１ｂ・・・のサービスを利用するクライアント端末となり、インターネットを介してリモートアクセスする情報登録手段２の機能を利用するクライアントになる。

【００３５】

情報取得手段３は、登録側サーバ記憶部７と同一の登録先を記憶する取得側ネーム記憶部９を有している。取得側ネーム記憶部９は、登録側サーバ記憶部７が記憶するものと同じ管理テーブル（図３参照）をもち、登録側サーバ記憶部７の各登録先は取得側ネーム記憶部９における各登録先と１対１で対応する。情報取得手段３は、取得側ネーム記憶部９に対する情報登録手段２のホスト名の登録と、この登録先に対応するＤＤＮＳサーバのＩ

Ｐアドレスの登録とを情報取得手段３のユーザから入力されるようになっている。情報取得手段３のユーザは、情報登録手段２のユーザと同じアクセス権限をもつ者、例えば同一人である。

【００３６】

また、情報取得手段３は、取得側ネーム記憶部９に記憶された登録先のＤＤＮＳサーバ１ａ、１ｂ・・・のＩＰアドレスに対して、当該ＤＤＮＳサーバ１ａ、１ｂ・・・のＩＰアドレスに対応付けられたホスト名の名前解決要求を送信するリゾルバ１０を有している。リゾルバ１０は、情報登録手段２が登録した全てのＤＤＮＳサーバ１ａ、１ｂ・・・に名前解決要求を送信し、各応答メッセージに含まれたＤＮＳのプロトコルに従ってＩＰアドレス（登録済みの見せかけのＩＰアドレス）を得て暗号文の全文を取得する。

【００３７】

また、情報取得手段３は、リゾルバ１０が取得した暗号文を復号化する復号器１１を有している。復号化で得られた接続情報１２は、接続情報５と同じ情報をもっている。復号化に必要な鍵情報は、情報取得手段３に登録されるようになっている。情報取得手段３は、接続情報１２に含まれた各項目の情報を適宜に用いて情報登録手段２にリモートアクセスする。なお、情報取得手段３、情報登録手段２への鍵情報の登録は、登録済みの情報登録手段のユーザ配布、媒体又はダウンロードで実装されたプログラムによるインストール、ユーザ操作によるテキスト入力等の適宜の手段で行えばよい。

【００３８】

情報取得手段３が接続情報１２を取得するまでのフローチャートを図６に例示する。リゾルバ１０は、取得側ネーム記憶部９を参照し、管理テーブルに登録先として記憶されたＤＤＮＳサーバ１ａ、１ｂ・・・のＩＰアドレスを取得する（Ｓ２１）。次に、リゾルバ１０は、取得したＤＤＮＳサーバ１ａ、１ｂ・・・のＩＰアドレスに対応付けられたホスト名の名前解決要求を送信する（Ｓ２２）。ＤＤＮＳサーバ１ａ、１ｂ・・・は、自己の対応表を参照して要求されたＩＰアドレス（見せかけのＩＰアドレス）をリゾルバ１０に応答する（Ｓ２３）。情報取得手段３は、ＤＤＮＳサーバ１ａ、１ｂ・・・の応答メッセージに含まれたホスト名に対応するＩＰアドレス（見せかけのＩＰアドレス）を取得側ネーム記憶部９の順序「Ｎｏ．」に従って統合して、暗号文を復元する（Ｓ２４）。情報取得手段３は、復元した暗号文を復号器１１に投入する（Ｓ２５）。復号器１１は、登録済みの復号鍵を用いて暗号文を複合化し（Ｓ２６）、これにより、情報取得手段３は、接続情報１２を取得する（Ｓ２７）。

【００３９】

情報取得手段３は、情報登録手段２への接続を実施する都度、（Ｓ２１）～（Ｓ２７）を実施する。また、リゾルバ１０は、既に取得した接続情報１２の有効期限を監視し、有効期限が切れた場合に再度（Ｓ２１）からの処理を開始する機能をもっている。

【００４０】

取得側ネーム記憶部９、リゾルバ１０、復号器１１は、情報取得手段３にコンピュータプログラムとして実装されており、情報取得手段３の演算処理装置でコンピュータプログラムを実行することにより、情報取得手段３に備わる演算処理装置、記憶装置、ネットワークインターフェイスといったハードウェア資源上に取得側ネーム記憶部９等が構成される。

【００４１】

図１の実施形態をＩＰｖ４（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　Ｖｅｒｓｉｏｎ４）のＤＤＮＳに適用した場合の接続情報５の登録から接続情報１２の取得までの情報伝達を図１、図７に基いて説明する。この実施例に係る接続情報５、１２は、ポート番号の有効期限、ポート番号、動的ＩＰアドレス、ルート情報、ユーザＩＤ、パスワードからなる。ポート番号の有効期限は、３６００秒間に設定した場合を例示している。ポート番号は、１０２４番に設定した場合を例示している。動的ＩＰアドレスは、「１９２．１６８．２４．１」に割り当てられた場合を例示している。ルート情報は、「１９２．１６８．２４．３」に設定した場合を例示している。ユーザＩＤ、パスワードは、情報登録手段２

でリモートアクセスの認証に用いる固有の識別情報であり、それぞれ「１５」、「２９４７４３７」に設定した場合を例示している。情報登録手段２にホスト名Ａ～Ｄが割り当てられた場合を例示している。ホスト名ＡはＮｏ．１のホスト名（図３を適宜参照のこと）、ホスト名Ｂは同じくＮｏ．２のホスト名というように対応する。

【００４２】

図１に示す情報登録手段２は、図７に示すように、ポート番号の有効期限「０Ｅ　１０」、ポート番号「０４　００」、割り当てられた動的ＩＰアドレス「Ｃ０　Ａ８　１８　０１」、ルート情報「Ｃ０　Ａ８　１８　０３」、ユーザＩＤ「０Ｆ」、パスワード「２Ｃ　Ｆ９　６Ｄ」を並べた情報を図中の平文とする。暗号器６は、この平文に図中の暗号鍵を桁対応をとって加算する暗号化により、図中の暗号文を生成する。登録機能部８は、暗号文をＩＰアドレスサイズ（ＩＰｖ４の場合４バイト）に分けて、ホスト名Ａの見せかけのＩＰアドレスとする「０Ｆ　１２　０７　０４」、ホスト名Ｂの見せかけのＩＰアドレスとする「Ｃ５　ＡＥ　１Ｆ　０９」、ホスト名Ｃの見せかけのＩＰアドレスとする「Ｃ９　Ｂ８　２９　１５」、ホスト名Ｄの見せかけのＩＰアドレスとする「２２　４０　０１　０Ｅ」、ホスト名Ｅの見せかけのＩＰアドレスとする「Ｃ５　ＡＥ　１Ｆ　０９」を生成する。登録機能部８は、ホスト名Ａと見せかけのＩＰアドレス「０Ｆ　１２　０７　０４」の登録要求を、登録側サーバ記憶部７において対付けられた登録先のＤＤＮＳサーバ１ａのＩＰアドレスに送信し、ホスト名Ｂ等についても同様に送信する。その結果、図中の暗号文は、５つの登録先に分散登録される。

【００４３】

図１に示す情報取得手段３は、図７に示すように、暗号鍵と同じ復号鍵と、登録側サーバ記憶部７の管理テーブルと同じ登録内容の取得側ネーム記憶部１０とを保持している。リゾルバ１０は、取得側ネーム記憶部９に登録先として記憶された所定のＤＤＮＳサーバ１ａ、１ｂの全てに、対応するホスト名Ａ～Ｅの名前解決要求を送信する。復号器１１は、リゾルバ１０が取得した５つの見せかけのＩＰアドレスを取得側ネーム記憶部９に記憶された統合順序に従って暗号文を復元し、復号鍵で減算する復号化により、平文すなわち接続情報１２に戻す。

【００４４】

上述のように、このシステムは、情報登録手段２へのリモートアクセスに用いる接続情報５、１２のデータサイズがＩＰアドレスよりも大きくなった暗号文をＤＤＮＳサーバ１ａ、１ｂ・・・への登録に適合したＩＰアドレスサイズにデータを分割し、暗号文を分散登録することにより、外部からは接続情報として機能しない文字列を、情報登録手段２に割り当てられたホスト名の見せかけのＩＰアドレスとして、既存のＤＤＮＳサーバ１ａ、１ｂ・・・へ登録することができる。したがって、既存のＤＤＮＳサーバ１ａ、１ｂ・・・への機能追加は不要であり、接続情報５、１２の登録・取得をセキュアに行うことができ、既存のＤＤＮＳサーバ１ａ、１ｂ・・・を利用する際、第三者からの情報登録手段２への不正アクセスを防ぐことができる。

【００４５】

また、このシステムは、接続情報５、１２に有効期限を設定し、有効期限が切れた場合にポート番号を変更した接続情報５、１２の再度登録することにより、特定のポートを狙った攻撃から、情報登録手段２のネットワークインターフェイスの背後にある情報を守ることができる。

【００４６】

このシステムの変更例を図８～図１０に基いて説明する。以下、変更点のみを述べるに留める。図８、図１０に示すように、この変更例に係る取得側ネーム記憶部９は、図３の登録先Ｎｏ．１～５に対応するホスト名のみを管理テーブルによって記憶している。

【００４７】

図８、図９に示すように、リゾルバ１０は、取得側ネーム記憶部９に記憶されたホスト名を取得すると（Ｓ２１）、情報取得手段が具備されたＰＣ（パーソナルコンピュータ）などにおいてデフォルトサーバとして事前設定された、あるいは、ＤＨＣＰにより通知さ

れたＤＮＳ上の任意のＤＮＳサーバに対して、ホスト名の名前解決要求を送信する（Ｓ２２）。図９に示すＤＤＮＳサーバ１ａ、１ｂ・・・以外のＤＮＳサーバは、それぞれインターネット上のＤＮＳに属し、自ゾーンのドメインとＩＰアドレスを対応表で管理しているＤＮＳコンテンツサーバ、又はフルリゾルバとなっている。ＤＤＮＳサーバ１ａ、１ｂ・・・は、名前解決要求に対するＤＮＳ応答において当該応答を中継保持するＤＮＳサーバにおけるキャシュ時間：ＴＴＬ（Time To Live）を０秒に指定して返信する。このため、ＤＤＮＳサーバ１ａ、１ｂ・・・の応答が他のＤＮＳサーバにキャッシュされることがなく、リゾルバ１０からの名前解決要求は、インターネット上の１個以上のＤＮＳサーバを介し、最終的にＤＤＮＳサーバ１ａ、１ｂ・・・に届けられ、ＤＤＮＳサーバ１ａ、１ｂ・・・からの返信も、同じくＤＮＳサーバを介してリゾルバ１０に到達する。したがって、情報取得手段３は、最新の見せかけのＩＰアドレスを確実に取得することができる。

【００４８】

この変更例と図１、図３例のシステムとを比較すると、この変更例は、図１０に示すように、取得側ネーム記憶部９にホスト名のみを記憶するだけで済む点で優れ、図１、図３例のシステムは、名前解決に際し、図９に示す如く、リゾルバ１０とＤＤＮＳサーバ１ａ、１ｂ・・・間に介在する各ＤＮＳサーバにおける検索、転送処理を無くし、接続情報１２を復元するまでの時間を短くすることができる点で優れる。

【００４９】

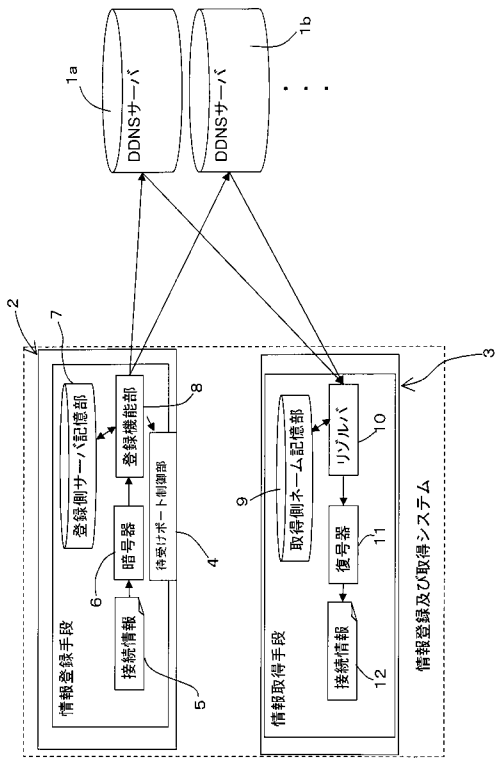
この発明の技術的範囲は、上述の実施形態に限定されず、特許請求の範囲の記載に基く技術的思想の範囲内での全ての変更を含むものである。例えば、このシステムに係るサービスを利用するユーザには、そのユーザが利用するホスト名、ＤＤＮＳサーバのＩＰアドレス等を登録済みの登録側サーバ記憶部、取得側ネーム記憶部を予め保持している情報登録手段、情報取得手段を提供してもよい。また、ユーザが予め、情報登録手段、情報取得手段に対し、サービサーから提供する媒体又はサービサーからダウンロードされたプログラムの実行により、パーソナルコンピュータ、携帯電話に備わる所定のユーザインターフェイスを介した手動入力により、利用するホスト名、ＤＤＮＳサーバ等を登録しても良い。なお、この場合は、ユーザが情報登録手段、情報取得手段に同じ管理テーブルの内容で登録することが前提になる。また、ＩＰｖ６に対応するＤＤＮＳにこのシステムを適用することも可能である。

【符号の説明】

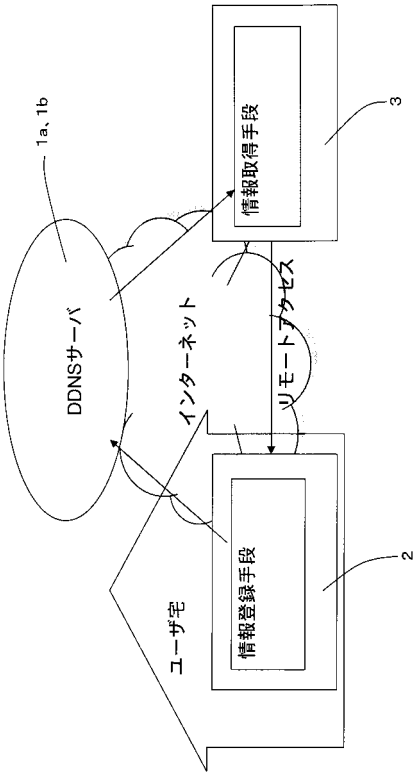
【００５０】

１ａ、１ｂ　ＤＤＮＳサーバ
２　情報登録手段
３　情報取得手段
４　待受けポート制御部
５、１２　接続情報
６　暗号器
７　登録側サーバ記憶部
８　登録機能部
９　取得側ネーム記憶部
１０　リゾルバ
１１　復号器

【図１】



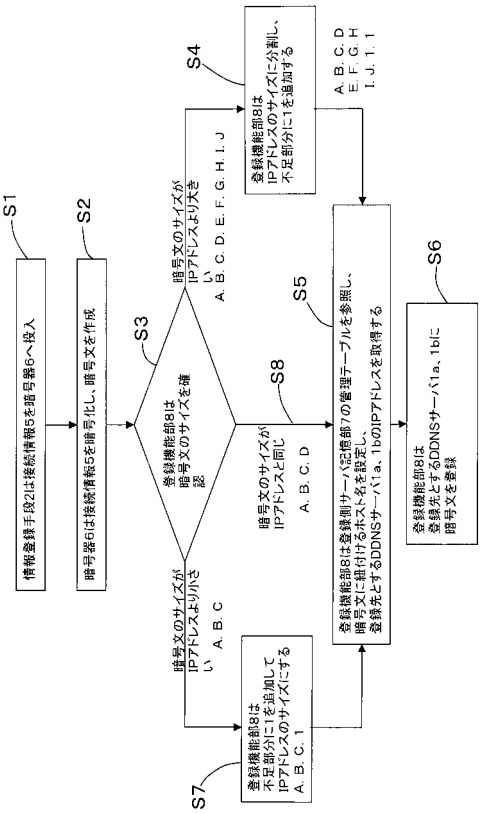
【図２】



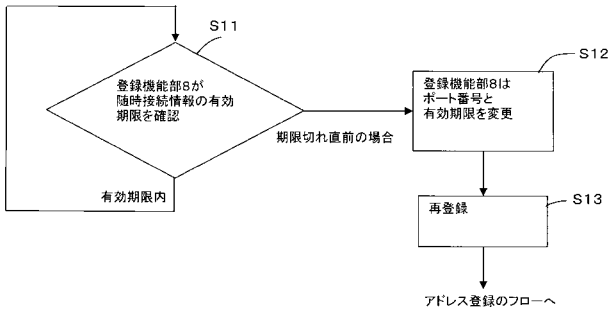
【図３】

No.	ホスト名	DDNSサーバアドレス
1	●●●.domain1.co.jp	10.10.10.1
2	●●●.domain2.co.jp	10.10.10.2
3	●●●.domain3.co.jp	10.10.10.3
4	×××.domain3.co.jp	10.10.10.3
5	△△△.domain3.co.jp	10.10.10.3
⋮		

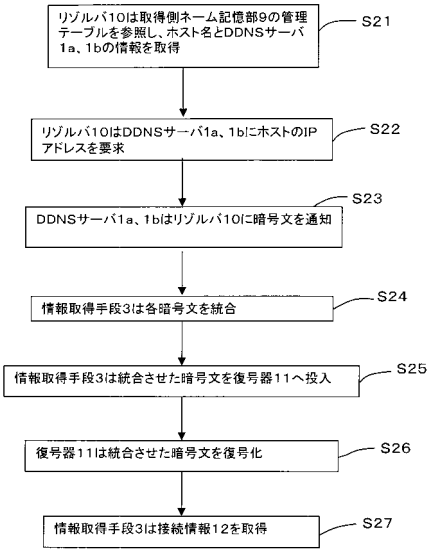
【図４】



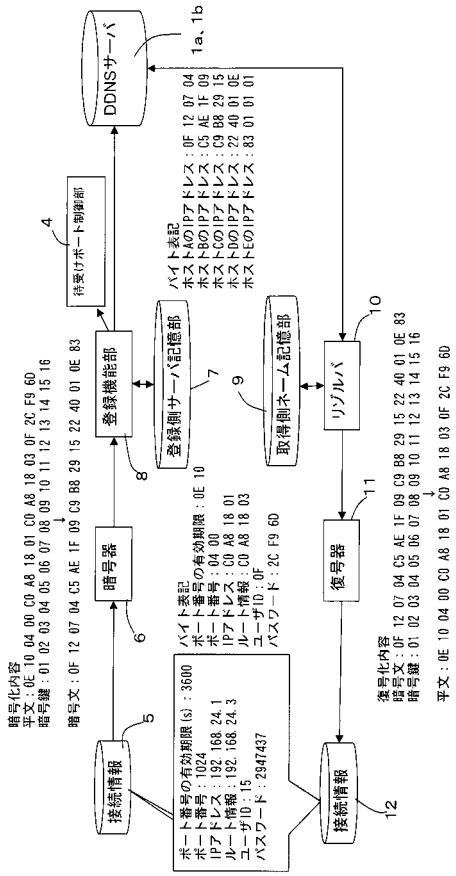
【図５】


S11
登録機能部8が
随時接続情報の有効
期限を確認
有効期限内
期限切れ直前の場合
S12
登録機能部8は
ポート番号と
有効期限を変更
S13
再登録
アドレス登録のフローへ

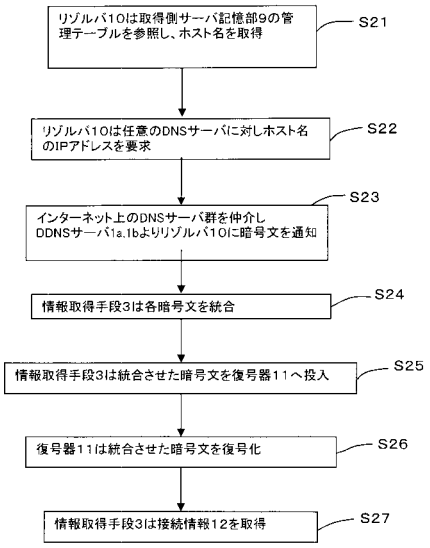
【図６】


リゾルバ10は取得側ネーム記憶部9の管理テーブルを参照し、ホスト名とDDNSサーバ1a、1bの情報を取得
S21
リゾルバ10はDDNSサーバ1a、1bにホストのIPアドレスを要求
S22
DDNSサーバ1a、1bはリゾルバ10に暗号文を通知
S23
情報取得手段3は各暗号文を統合
S24
情報取得手段3は統合させた暗号文を復号器11へ投入
S25
復号器11は統合させた暗号文を復号化
S26
情報取得手段3は接続情報12を取得
S27

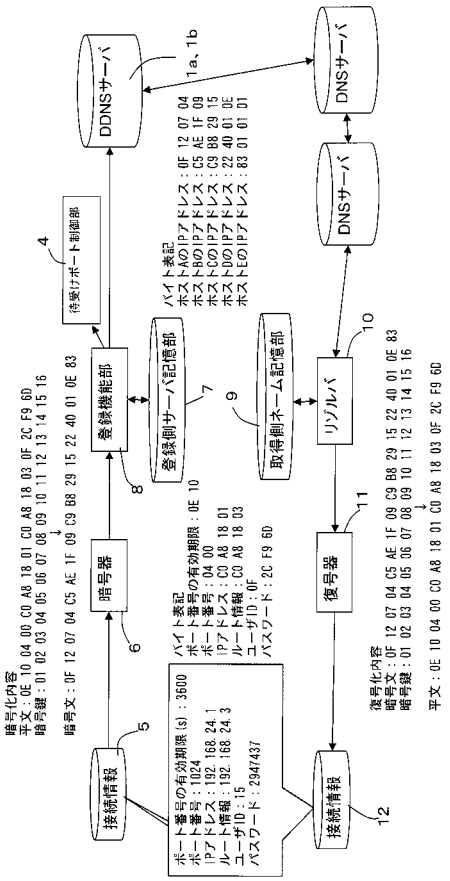
【図７】


DDNSサーバ
1a、1b
待受けポート制御部
4
登録機能部
8
暗号器
6
接続情報
5
登録側サーバ記憶部
7
取得側ネーム記憶部
9
リゾルバ
10
復号器
11
接続情報
12
バイト表記
ホストAのIPアドレス：0F 12 07 04
ホストBのIPアドレス：C5 AE 1F 09
ホストCのIPアドレス：C9 B8 29 15
ホストDのIPアドレス：22 40 01 0E
ホストEのIPアドレス：83 01 01 01
バイト表記
ポート番号の有効期限：0E 10
ポート番号：04 00
IPアドレス：C0 A8 18 01
ルート情報：C0 A8 18 03
ユーザID：0F
パスワード：2C F9 6D
ポート番号の有効期限（s）：3600
ポート番号：1024
IPアドレス：192.168.24.1
ルート情報：192.168.24.3
ユーザID：15
パスワード：2947437
暗号化内容
平文：0E 10 04 00 C0 A8 18 01 C0 A8 18 03 0F 2C F9 6D
暗号鍵：01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16
暗号文：0F 12 07 04 C5 AE 1F 09 C9 B8 29 15 22 40 01 0E 83
復号化内容
暗号文：0F 12 07 04 C5 AE 1F 09 C9 B8 29 15 22 40 01 0E 83
暗号鍵：01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16
平文：0E 10 04 00 C0 A8 18 01 C0 A8 18 03 0F 2C F9 6D

【図８】


リゾルバ10は取得側サーバ記憶部9の管理テーブルを参照し、ホスト名を取得
S21
リゾルバ10は任意のDNSサーバに対しホスト名のIPアドレスを要求
S22
インターネット上のDNSサーバ群を仲介しDDNSサーバ1a,1bよりリゾルバ10に暗号文を通知
S23
情報取得手段3は各暗号文を統合
S24
情報取得手段3は統合させた暗号文を復号器11へ投入
S25
復号器11は統合させた暗号文を復号化
S26
情報取得手段3は接続情報12を取得
S27

【図９】



【図１０】

No.	ホスト名
1	●●●.domain1.co.jp
2	●●●.domain2.co.jp
3	●●●.domain3.co.jp
4	×××.domain3.co.jp
5	△△△.domain3.co.jp
ﾛc	

フロントページの続き

(72)発明者　宮奥　健人
大阪府大阪市中央区馬場町３番１５号　西日本電信電話株式会社内

Ｆターム(参考) 5K030 GA15　HB11　HD09　JL08　KA06　LD19