(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4965559号
(P4965559)
(45)発行日　平成24年7月4日(2012.7.4)　(24)登録日　平成24年4月6日(2012.4.6)

(51)Int.Cl.　F I
H04L 12/28 (2006.01)　H04L 12/28　200A

請求項の数 10　(全 11 頁)

(21)出願番号	特願2008-508188 (P2008-508188)
(86)(22)出願日	平成18年4月11日 (2006.4.11)
(65)公表番号	特表2008-538883 (P2008-538883A)
(43)公表日	平成20年11月6日 (2008.11.6)
(86)国際出願番号	PCT/EP2006/061525
(87)国際公開番号	WO2006/114367
(87)国際公開日	平成18年11月2日 (2006.11.2)
審査請求日	平成21年4月10日 (2009.4.10)
(31)優先権主張番号	05447093.5
(32)優先日	平成17年4月25日 (2005.4.25)
(33)優先権主張国	欧州特許庁 (EP)

(73)特許権者　501263810
トムソン　ライセンシング
Ｔｈｏｍｓｏｎ　Ｌｉｃｅｎｓｉｎｇ
フランス国，　９２１３０　イツシー　レ　ムーリノー，　ル　ジヤンヌ　ダルク，　１－５
１－５，　ｒｕｅ　Ｊｅａｎｎｅ　ｄ’Ａｒｃ，　９２１３０　ＩＳＳＹ　ＬＥＳ　ＭＯＵＬＩＮＥＡＵＸ，　Ｆｒａｎｃｅ
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(74)代理人　100107766
弁理士　伊東　忠重

最終頁に続く

(54)【発明の名称】リソースアドレスリクエスト管理方法及び関連するゲートウェイ装置

(57)【特許請求の範囲】
【請求項１】
第１ネットワークに属する第１ネットワーク装置と第２ネットワークに属する第２ネットワーク装置との間の接続を確立するよう構成されるゲートウェイ装置であって、
当該ゲートウェイ装置は、前記第１ネットワークに接続する手段と、前記第２ネットワークに接続する手段とを有し、
前記第１ネットワークと前記第２ネットワークとのネットワーク装置は、各自のネットワーク内で一意的な真のネットワークアドレスを有し、
当該ゲートウェイ装置はさらに、前記第２ネットワーク内の前記第２ネットワーク装置に対応するネットワークリソース識別子を決定するリクエストに応答して、前記第２ネットワークに属し、ＵＲＬを有効なネットワークアドレスに変換するよう構成される第３ネットワーク装置から真のネットワークアドレスを取得する手段を有し、
当該ゲートウェイ装置はさらに、前記第１ネットワーク装置からデータに対するリクエストを受信するよう構成され、
前記データは、前記リクエストに応答して前記第２ネットワーク装置から当該ゲートウェイ装置を介し前記第１ネットワーク装置に提供され、
当該ゲートウェイ装置はさらに、
真のネットワークアドレスが前記第３ネットワーク装置から取得できない場合、前記第１ネットワーク装置から受信したネットワークリソース識別子を決定するリクエストに応答して、なりすましネットワークアドレスを提供する手段であって、各ネットワークリソ

ース識別子について個々のなりすましネットワークアドレスを提供するよう構成される手段と、
それぞれのネットワークリソース識別子の真のネットワークアドレスが取得可能になると、なりすましネットワークアドレスが以前に提供されたネットワークリソース識別子のそれぞれに対する前記第１ネットワーク装置からのアクセスに対するリクエストに応答して、真のネットワークアドレスを取得し、なりすましネットワークアドレスを前記真のネットワークアドレスに変換する手段と、
を有するゲートウェイ装置。
【請求項２】
なりすましネットワークアドレスに基づき前記第１ネットワーク装置によりなされたリクエストに対するレスポンスを提供するサーバコンポーネントをさらに有する、請求項１記載のゲートウェイ装置。
【請求項３】
前記レスポンスは、真のネットワークアドレスの欠落の理由を記述した情報を含む、請求項２記載のゲートウェイ装置。
【請求項４】
なりすましネットワークアドレスとそれのネットワークリソース識別子とを格納するメモリをさらに有する、請求項１記載のゲートウェイ装置。
【請求項５】
前記メモリはさらに、ネットワークリソース識別子に対応する真のネットワークアドレスが決定されると、前記真のネットワークアドレスを格納する、請求項４記載のゲートウェイ装置。
【請求項６】
第１ネットワークに属する少なくとも１つの第１ネットワーク装置から第２ネットワークに属する少なくとも１つの第２ネットワーク装置へのネットワークアドレスリクエストを管理する方法であって、
当該方法は、前記第１ネットワークと前記第２ネットワークとの間に接続されるゲートウェイ装置により実行され、
当該方法は、
前記少なくとも１つの第１ネットワーク装置から、ネットワークリソース識別子に対応する真のネットワークアドレスであって、前記ネットワークリソース識別子に関連付けされ、前記第２ネットワークに属するネットワーク装置のネットワークアドレスである前記真のネットワークアドレスを取得するためのリクエストを受信するステップと、
前記少なくとも１つの第２ネットワーク装置の真のネットワークアドレスが前記第２ネットワークから取得可能であるか判断するステップと、
前記少なくとも１つの第２ネットワーク装置の真のネットワークアドレスが前記第２ネットワークから取得可能でない場合、個々のなりすましネットワークアドレスが各ネットワークリソース識別子に対して提供されるなりすましネットワークアドレスを前記少なくとも１つの第１ネットワーク装置に提供するステップと、
なりすましネットワークアドレスが前記少なくとも１つの第１ネットワーク装置に提供された前記ネットワークリソース識別子の１つに対して真のネットワークアドレスが取得可能になると、前記対応する真のネットワークアドレスを取得し、前記以前に提供されたなりすましネットワークアドレスを用いて前記少なくとも１つの第１ネットワーク装置からのアクセスに対するリクエストに応答して、前記なりすましネットワークアドレスを前記真のネットワークアドレスに変換し、前記少なくとも１つの第１ネットワーク装置と前記真のネットワークアドレスにより特定されるネットワーク装置との間の接続を設定するステップと、
を有する方法。
【請求項７】
前記第１ネットワーク装置からなりすましネットワークアドレスに基づくリクエストを

受信するステップと、
応答において、前記第１ネットワーク装置によりアクセス可能なサーバに前記第１ネットワーク装置をリダイレクトするステップと、
をさらに有する、請求項６記載の方法。
【請求項８】
前記アクセス可能なサーバは、真のネットワークアドレスの欠落を生じさせたエラー状態に関する情報を提供する、請求項７記載の方法。
【請求項９】
受信したネットワークリソース識別子をそれに関連するなりすましネットワークアドレスと、取得されると対応する真のネットワークアドレスと一緒に格納するステップをさらに有する、請求項６記載の方法。
【請求項１０】
前記第１ネットワークは、ローカルエリアネットワークであり、
前記第２ネットワークは、インターネットであり、
前記ネットワークアドレスは、インターネットプロトコルアドレスであり、
前記ネットワークリソース識別子は、ＵＲＬである、請求項１記載のゲートウェイ装置。
【発明の詳細な説明】
【発明の詳細な説明】
【０００１】
本発明は、ウェブアプリケーションなどからネットワークリソースアドレスリクエストを管理する方法と、当該方法を実現するためのゲートウェイ装置とに関する。本発明は、ＩＰネットワークとＬＡＮを接続するゲートウェイにおいて使用可能であるが、このようなコンテクストに限定されるものでない。
【０００２】
ブラウザアプリケーションを備えたクライアントコンピュータが、いわゆる“ウェブページ”などを取得するため、インターネットサーバにアクセスする必要があるとき、それは、当該ページを提供するサーバに対応するＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）アドレスを知っている必要がある。通常、ブラウザは初期的に、いわゆるＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）又はＦＱＤＮ（Ｆｕｌｌｙ　Ｑｕａｌｉｆｉｅｄ　Ｄｏｍａｉｎ　Ｎａｍｅ）を知っている。
【０００３】
ＵＲＬ又はＦＱＤＮの実際のＩＰアドレスへの変換は、クライアントコンピュータによって提供されたＵＲＬ又はＦＱＤＮに基づき、ＤＮＳ（Ｄｏｍａｉｎ　Ｎａｍｅ　Ｓｙｓｔｅｍ）サーバなどの装置によって実行される。
【０００４】
ブラウザがウェブページをホストする装置、すなわち、ウェブサーバのＩＰアドレスを知ると、当該ＩＰアドレスとの接続を設定し、ＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）プロトコルなどを利用して必要とされる情報に対するリクエストを送信する。ウェブサーバは、ＨＴＭＬ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）ウェブページ、ピクチャ又は他のデータにより応答する。
【０００５】
このアドレス変換は、例えば、クライアントコンピュータがローカルエリアネットワークや他のタイプのネットワークに接続され、ゲートウェイ装置を介しインターネットに接続されるときなど、ゲートウェイ装置を介し実行されるかもしれない。
【０００６】
問題が生ずるのは、ＤＮＳサーバとの接続が不可能であるとき、例えば、ゲートウェイ装置とインターネットとの間の接続が中断されるときなどであるかもしれない。この場合、ブラウザはＩＰアドレスを取得することができない。このことは、例えば、“ホスト名が決定できない”などのエラーメッセージをブラウザに表示させることとなる。ユーザが

問題の本質を通知し、最終的に解決策を示唆するようにするため、いわゆる“スプーフィング（ｓｐｏｏｆｉｎｇ）”をゲートウェイ装置に実行させることが知られている。この機構は、ゲートウェイ装置に誤ったＩＰアドレスをブラウザに返すようにさせ、ブラウザにＤＮＳサーバとの接続が確立されたことを信じさせることからなる。その後、ゲートウェイ装置は、スプーフされたアドレスとの接続のためのリクエストを傍受し、それがあたかもウェブサーバであるかのように振る舞う。ブラウザからリクエストを受信すると、ゲートウェイは、例えば、誤ったパスワードが提供されたため、又は他の理由のためにインターネット接続がないなど、問題の性質を説明するＨＴＭＬページを返すことができる。

【０００７】

また、ＤＮＳサーバがＵＲＬ又はＦＱＤＮが知られていないことを宣言すると、スプーフされたアドレスを生成することが知られている。これを実行する目的は、クライアントにウェブサーバにリクエストを送信させることである。それは、アドレスを取得していない場合、当該リクエストを送信するための接続を確立しない。

【０００８】

ブラウザ若しくは他のアプリケーション、又はオペレーティングシステムなどの他のクライアントコンポーネントは、いわゆるＤＮＳキャッシュを実現するかもしれない。ＤＮＳキャッシュは、ＵＲＬ又はＦＱＤＮとＩＰアドレスとの間の関連付けを保持する。その後、アプリケーションはＩＰアドレスを２回リクエストする必要はなく、対応する情報へのより高速なアクセスが可能となる。しかしながら、ＤＮＳキャッシュの存在は、上述されたスプーフィング機構と組み合わされる際に問題を生じさせるかもしれない。実際、ＤＮＳサーバとの接続がリストアされると、アプリケーションはスプーフされたＩＰアドレスの使用を中止し、再びＤＮＳサーバからＵＲＬに対する実際のＩＰアドレスをリクエストするようにする。アプリケーションがスプーフされた／偽のＩＰアドレスを記憶しているという事実は、実際のアドレスを再度リクエストしないため、ユーザがもはや初期的にリクエストされたウェブサイトにアクセス不可となる結果をもたらす。

【０００９】

特定のアプリケーションでは、アプリケーションをクローズすることはＤＮＳキャッシュを消去させることが知られている。

【００１０】

本発明は、第１装置と接続するための手段と、第１ネットワーク上に設けられた第１装置に接続するための手段と、前記第１装置により提供されるネットワークリソース識別子の関数としてリアルネットワークアドレスを取得するため、第２ネットワーク上に設けられる第２装置に接続するための手段とを有するゲートウェイ装置であって、さらに、リアルネットワークアドレスが提供不可である場合、前記第１装置により提供されるネットワークリソース識別子に応答して、偽のネットワークアドレスを提供する手段を有し、該偽のネットワークアドレスを提供する手段は、異なるネットワークリソース識別子に異なる偽のネットワークアドレスを提供するよう構成されるゲートウェイ装置に関する。

【００１１】

上記偽のアドレスは、初期的なリソース識別子に対応するリアルアドレスが利用可能になると、該リアルアドレスを提供するのに利用可能である。

【００１２】

本発明の実施例によると、本装置は、偽のネットワークアドレスに基づき、前記第１装置によりなされるリクエストに対するレスポンスを提供するサーバコンポーネントをさらに有する。

【００１３】

本発明の実施例によると、前記レスポンスは、リアルネットワークアドレスの欠落の理由を記述する情報を有する。

【００１４】

本発明の実施例によると、本装置は、偽のネットワークアドレスが以前に提供されたネットワークリソース識別子のリアルネットワークアドレスを決定するようさらに構成され

る。
【００１５】
本発明の実施例によると、本装置は、リアルネットワークアドレスが決定された偽のネットワークアドレスに基づき、前記第１装置からのリクエストにより、前記第１装置を前記リアルネットワークアドレスにリダイレクトする手段をさらに有する。
【００１６】
本発明の実施例によると、本装置は、偽のネットワークアドレスと自らのネットワークリソース識別子とを格納するメモリをさらに有する。
【００１７】
本発明の実施例によると、前記メモリはさらに、ネットワークリソース識別子に対応するリアルネットワークアドレスが決定されると、該リアルネットワークアドレスをさらに格納する。
【００１８】
本発明はまた、第１ネットワークに設けられる第１装置から第２ネットワークに設けられる第２装置へのネットワークリソースアドレスリクエストを管理する方法であって、当該方法は、前記第１装置と前記第２装置との間に接続されるゲートウェイ装置により実行され、当該方法は、前記第１装置からリソース識別子を受信するステップと、前記第２装置が前記リソース識別子に対応するリアルネットワークリソースアドレスを提供可能か判断するステップと、肯定されると、前記リソースネットワークリソースアドレスを提供し、否定されると、偽のネットワークリソースアドレスを提供するステップとを有し、前記提供される偽のネットワークリソースアドレスは、前記受信したリソース識別子に一意的に関連付けされる方法に関する。
【００１９】
本発明の実施例によると、本方法は、前記第１装置からの偽のネットワークアドレスに基づくリクエストを受信するステップと、これに応答して、前記第１装置によりアクセス可能なサーバに前記第１装置をリダイレクトするステップとをさらに有する。
【００２０】
本発明の実施例によると、前記アクセス可能なサーバは、リアルネットワークアドレスの欠落を生じさせるエラー状態に関する情報を提供する。
【００２１】
本発明の実施例によると、本方法は、リアルネットワークアドレスが取得可能になると、偽のネットワークアドレスが提供された以前に受信したリソース識別子に対するリアルネットワークアドレスを取得するステップをさらに有する。
【００２２】
本発明の実施例によると、本方法は、前記第１装置からの偽のネットワークアドレスに基づくリクエストを受信すると、前記偽のネットワークアドレスに対応する前記リアルネットワークアドレスにより特定される装置と前記ゲートウェイとの間の接続を設定するステップをさらに有する。
【００２３】
本発明の実施例によると、本方法は、受信した識別子を、それに係る偽のネットワークリソースアドレスと、取得されると、前記対応するリアルネットワークアドレスと共に格納するステップをさらに有する。
【００２４】
本発明が、図面を利用して説明される具体的な実施例により詳細に説明される。本発明は、実施例の詳細な説明に限定されるべきでない。
【００２５】
図１は、ローカルエリアネットワーク１０８をインターネット１０４に接続する本実施例のゲートウェイ１０２のオブジェクトを示す。ウェブブラウザなどのインターネットアクセス１０７を要求するアプリケーションを備えたクライアントコンピュータ１０１が、ローカルエリアネットワークと接続される。図１は、インターネットに接続された１つの

ウェブサーバ１０５と１つのＤＮＳサーバ１０６を示す。もちろん、より多くのＤＮＳサーバ及びウェブサーバが接続可能であり、これら２つのタイプのサーバ以外の装置もまたインターネットに接続される。ゲートウェイ１０２は、その目的が後述されるメモリ１０３を有する。本例によると、メモリは半導体又は等価なタイプである。インターネットアプリケーション１０７はまた、ブラウザと異なるものであってもよく、コンピュータ以外の装置上で実行されるかもしれない。例えば、それは電子番組ガイドアプリケーションを有するＩＰ対応オーディオ／ビデオデコーダであってもよい。ゲートウェイ１０２はまた、装置１０２に直接設けられてもよく、この場合、ローカルエリアネットワークは存在しないことに留意されたい。

【００２６】

図２は、ゲートウェイ装置をローカルエリアネットワークとインターネットにそれぞれ接続するインタフェース２０９及び２１０を含むゲートウェイ装置１０２の各機能コンポーネントを示す。例えば、ローカルエリアネットワークは、イーサネット（登録商標）ネットワーク又はワイヤレスＩＥＥＥ８０２．１１ｂタイプネットワークであってもよい。ゲートウェイ装置１０２はさらに、ウェブサーバに類似したアプリケーションであって、ゲートウェイ装置の内部コンフィギュレーションなどに対応するウェブページを管理及び提供するＨＴＴＰサーバ２１２を有する。

【００２７】

本実施例によると、ＨＴＴＰサーバ２１２はまた、スプーフされたＩＰアドレスにリクエストする装置に情報を提供する。ＨＴＴＰプロキシ２１３は、ネットワーク１０８上のクライアントアプリケーションに対するプロキシサーバとして機能する。それは、クライアントアプリケーションにより策定されたリクエストを受信し、必要に応じてサーバ１０５などのリアルサーバにこれらのリクエストを転送し、リアルサーバのレスポンスをクライアントアプリケーションに送り返す。ＨＴＴＰプロキシは、ウェブサーバに関する限り、クライアントアプリケーションとして機能する。ＤＮＳ転送装置２１４は、クライアントアプリケーション１０７から受信したＤＮＳクエリを処理し、それらをインターネットを介し１以上のＤＮＳサーバに転送するコンポーネントである。当該コンポーネントは、ＤＮＳサーバから有効なレスポンスが受信されるか検出し、レスポンスをクライアントアプリケーションに送り返す。ＤＮＳ転送装置はまた、様々な理由により適切なＤＮＳサーバレスポンスが取得できないときに本実施例による“スプーフされた”又は“偽の”ＩＰアドレスを生成し、それらをクライアントアプリケーションに送信するコンポーネントである。ＤＮＳリクエストに応答するため１つのみのスプーフされた／偽のＩＰアドレスを使用する代わりに、このようなスプーフされたアドレスが必要とされるとき、ゲートウェイ装置のＤＮＳ転送装置は、それがＤＮＳリクエストにより受信した新たな各ＵＲＬ又はＦＱＤＮについて異なるスプーフされたＩＰアドレスを送信する。ＩＰルータコンポーネント２１１は、ローカルエリアネットワーク、ゲートウェイの他のコンポーネント及びインターネットとの間でＩＰパケットを転送する。ゲートウェイ装置１０２はまた、図１に関してすでに簡単に説明されたメモリ１０３を有する。メモリ１０３は、送信されたものに応答して各自のＵＲＬ又はＦＱＤＮと共に、ＤＮＳ転送装置２１４により決定されたスプーフされたＩＰアドレスを格納する。このため、ゲートウェイは、所与の受信したＵＲＬ／ＦＱＤＮに対して何れのスプーフされたＩＰアドレスが送信また受信したか決定することが可能である。

【００２８】

以下において、ゲートウェイ装置は、インターネット接続が存在しないことを検出すると、スプーフされたアドレスを送信することが提案される。もちろん、他の条件もまた考慮されるかもしれない。

【００２９】

図４は、クライアントアプリケーション１０７からの２つのリクエストの受信後のメモリ１０３のコンテンツの一例を与える。ＤＮＳ転送装置は、これら２つのリクエストに適したＤＮＳサーバレスポンスが受信されず、この結果、２つの異なるスプーフされたＩＰ

アドレスがクライアントアプリケーション１０７に送り返されると判断したと仮定される。クライアントアプリケーションが予想する実際のアドレスを示すカラム“実際のＩＰアドレス”は、この段階ではエンプティなままである。ＤＮＳサーバとの接続がゲートウェイ装置によって確立可能になると、それはメモリ１０３のコンテンツをチェックし、実際のＩＰアドレスが以前に決定可能でなく、それのメモリのスプーフされたＩＰアドレス及びＵＲＬ又はＦＱＤＮの各ペアについてＤＮＳサーバに実際のＩＰアドレスに対するリクエストを送信する。図５は、実際のＩＰアドレスが決定されると、メモリの状態を示す。本実施例では、メモリは３２個までのエントリを格納する。ラウンドロビン機構は、リストがフルであるとき、最も古いエントリを削除する。変形の実施例によると、ＴＴＬ（Ｔｉｍｅ－Ｔｏ－Ｌｉｖｅ）パラメータが各エントリに関連付けされる。

【００３０】

ゲートウェイ装置がデスティネーションアドレスとしてスプーフされたＩＰアドレスの１つを含むリクエストをクライアントアプリケーションから受信すると（すなわち、クライアントアプリケーションは、接続を設定しようとすると）、当該スプーフされたアドレスについて、実際のＩＰアドレスがキャッシュされたか否か、それのキャッシュメモリ１０３において確認する。

【００３１】

このような実際のＩＰアドレスが存在する場合、リクエストのスプーフされたＩＰアドレスが実際のＩＰアドレスと交換され、ゲートウェイ装置は、実際のＩＰアドレスにより特定される正しいサーバとの接続を確立し、もとのリクエストを当該サーバに転送する。

【００３２】

キャッシュメモリにこのような実際のＩＰアドレスが存在しない場合、ゲートウェイ装置は、ＨＴＭＬウェブページなどの適切なメッセージをクライアントアプリケーションに返す。当該メッセージ又はページは、好ましくは、ゲートウェイ装置が確認できる限り、実際のＩＰアドレスの欠落の理由の識別を有する。例えば、ゲートウェイ装置は、エラー状態の原因を決定するためテストを行ってもよい。すなわち、ＨＴＴＰプロトコルは、サーバが新たなＵＲＬを利用してクライアントを他の位置にリダイレクトすることを可能にする。

【００３３】

図３は、クライアントアプリケーション、ゲートウェイ装置のコンポーネント、ＤＮＳサーバ及びウェブサーバのメッセージ交換及びアクションの詳細なチャートである。

【００３４】

各ステップが後述される。

【００３５】

ステップ１：クライアント装置のウェブブラウザ（及びより正確には、ブラウザのためのオペレーティングシステム）が、ウェブサイトＵＲＬ（ｗｗｗ．ｘｙｚ．ｃｏｍなど）に対応するＩＰアドレスを要求するＤＮＳ転送装置にＤＮＳクエリを送信する。

【００３６】

ステップ２：ゲートウェイ装置のＤＮＳ転送装置は、インターネット（このため、実際のＤＮＳサーバ）との接続がないことを検出する。

【００３７】

ステップ３：ＤＮＳ転送装置は、スプーフされた／偽のＩＰアドレスにより応答することを決定する。それは、スプーフされたＩＰアドレスとＵＲＬ／ＦＱＤＮとの間の一意的な関連付けによりそれのキャッシュ／テーブルを更新する。

【００３８】

ステップ４：ウェブブラウザは、ウェブサイトのアドレスがスプーフされた／偽のＩＰアドレスであると考えるため、それとの接続を確立する。ゲートウェイ装置１０２は、この接続リクエストを“傍受”し、ゲートウェイのＨＴＴＰプロキシモジュールとの接続が確立される。ウェブブラウザは、ウェブサイトに対するＨＴＴＰリクエストを送信する。

【００３９】

ステップ５：ＨＴＴＰプロキシは、スプーフされた／偽のＩＰアドレスを検出する。当該コンポーネントは、このスプーフされたＩＰアドレスに対応する実際のＩＰアドレスが存在するか学習するため、ＤＮＳ転送装置にクエリする。

【００４０】

ステップ６：ＤＮＳ転送装置は、それのキャッシュ／テーブルをチェックし、当該スプーフされたＩＰアドレスに関するＵＲＬ／ＦＱＤＮが実際のＩＰアドレスでは決定されていなかったことを学習する。それは、ＨＴＴＰプロキシに実際のＩＰアドレスが存在しないことを通知する。

【００４１】

ステップ７：このスプーフされたＩＰアドレスに関連する実際のＩＰアドレスが存在しないことを知ると、ＨＴＴＰプロキシは、ゲートウェイ装置のＨＴＴＰサーバによりホストされるウェブページにウェブブラウザをリダイレクトする。それは、ウェブブラウザに新たなＵＲＬを示す。

【００４２】

ステップ８：ウェブブラウザは、ここでゲートウェイ装置との接続を確立し、ウェブページに対するＨＴＴＰリクエストをゲートウェイのローカルサーバに送信する。

【００４３】

ステップ９：ＨＴＴＰサーバウェブページは、インターネット接続が存在しないことを検出するか、又は他の診断テストを実行することができる。

【００４４】

ステップ１０：ＨＴＴＰサーバは、この問題を説明し、例えば、ゲートウェイ装置により実行された診断テストに基づきインターネット接続問題に対する可能な解決策を含むＨＴＭＬページにより応答する。

【００４５】

ステップ１１：ユーザは、訂正アクションを行い（例えば、ケーブルの再接続やインターネット接続パスワードの訂正など）、スクリーン上のボタン又はリンクのクリックを押下する。これにより、例えば、訂正されたパスワードのＨＴＴＰサーバへの送信がトリガーされる。

【００４６】

ステップ１２：ＨＴＴＰサーバはここで、インターネット接続が再び確立されていることを検出する。ＤＮＳサーバのアドレスは、インターネット接続が確立されると、ゲートウェイにより動的に抽出される。インターネットアドレスと共に、ゲートウェイはまた、１以上のＤＮＳサーバのアドレスを受信する。

【００４７】

ステップ１３：インターネット接続の確率は、“スプーフされた”／偽のＩＰアドレスが送信されたＵＲＬに対するＤＮＳクエリを送出するため、ゲートウェイ装置のＤＮＳ転送コンポーネントをトリガーする。それは、これらのクエリをインターネットを介しＤＮＳサーバのアドレスに送信する。

【００４８】

ステップ１４：ＤＮＳサーバは、ＵＲＬに対応する実際の又は“リアル”ＩＰアドレスにより応答する。

【００４９】

ステップ１５：ＤＮＳ転送装置は、スプーフされたＩＰアドレス、ＵＲＬ（ＦＱＤＮ）及び実際のＩＰアドレスによりそれのキャッシュ／テーブルを更新する。

【００５０】

ステップ１６：インターネット接続が再び確立されたことを知ると、インターネットゲートウェイＨＴＴＰサーバは、ウェブブラウザを当初要求されたウェブサイトに再びリダイレクトする。ＨＴＴＰサーバは、ＨＴＴＰプロキシとＨＴＴＰサーバとの間で以前に交換された当初リクエストされたウェブサイトのＵＲＬを記憶する。

【００５１】

ステップ１７：ウェブブラウザはここで、もとのウェブサイトとスプーフされた／偽のＩＰアドレスとの間のキャッシュされている関係を利用し、スプーフされた／偽のＩＰアドレスに再び接続する。ゲートウェイ装置は、当該接続を“傍受し”、これにより、実際にゲートウェイ装置のＨＴＴＰプロキシモジュールとの接続が確立される。

【００５２】

ステップ１８：ＨＴＴＰプロキシコンポーネントは、スプーフされたＩＰアドレスに対応する実際のＩＰアドレスが存在するか学習するため、ＤＮＳ転送コンポーネントをクエリする。

【００５３】

ステップ１９：ＤＮＳ転送コンポーネントは、ステップ１４においてＤＮＳサーバから受信した実際のＩＰアドレスにより応答する。

【００５４】

ステップ２０：ＨＴＴＰプロキシは、スプーフされたＩＰアドレスを実際のＩＰアドレスと交換し、ウェブページを要求するウェブサーバとの接続を確立する。

【００５５】

ステップ２１：ウェブサーバは、要求されたＨＴＭＬウェブページにより応答する。

【００５６】

ステップ２２：ＨＴＴＰプロキシはここで、ウェブサーバから受信されたレスポンスをクライアントコンピュータのウェブブラウザに転送する。クライアントコンピュータ上のユーザは、要求されたウェブサイトを自動的に受信する。これにより、クライアントアプリケーションは、それがスプーフされたＩＰアドレスを使用し続けるが、正しいサーバにアクセスする。ほとんどのオペレーティングシステムは自らのＤＮＳキャッシュを有していることに留意されたい。これは、ＤＮＳ結果であるＩＰアドレスとのＵＲＬ／ＦＱＤＮ対応をＴＴＬパラメータにより記憶するモジュールである。ウェブブラウザなどのオペレーティングシステム上で実行されるアプリケーションはまた、自らのキャッシュを有する。しかし、それらはＴＴＬパラメータを考慮していない。

【００５７】

変形となる実施例では、リアルアドレスがメモリ１０３のスプーフされたアドレスに対して利用可能であるかチェックするステップが、ＨＴＴＰプロキシ２１３の代わりにＩＰルータ２１１により実行される。また、スプーフされたＩＰアドレスをリアルＩＰアドレスと置換するステップは、ＩＰルータにより実行されてもよい（ステップ２０）。ＨＴＴＰプロキシは、スプーフされたＩＰアドレスの存在をチェックし、このようなアドレスが検出されると、クライアントアプリケーションをローカルＨＴＴＰサーバにリダイレクトする。それは、メモリ１０３のテーブルをクエリしない。本実施例は、ウェブブラウザが（偽の）アドレスを誤って記憶する一般的な問題に対する解決策を提供するだけでなく、自らのＤＮＳキャッシュにアドレスを記憶する他のプログラムに対しても適用可能である。

【００５８】

実施例の説明はインターネットプロトコルネットワーク実現形態に基づくものであるが、本発明は、識別子がアドレスにより置換される必要があり、当該フレームにおけるレスポンスのキャッシュが問題を生じさせる可能性のある他のコンテクストに適用可能である。

【図面の簡単な説明】

【００５９】

【図１】図１は、本実施例において説明されるゲートウェイ装置を利用して接続されるローカルエリアネットワーク及びインターネットの概略図である。

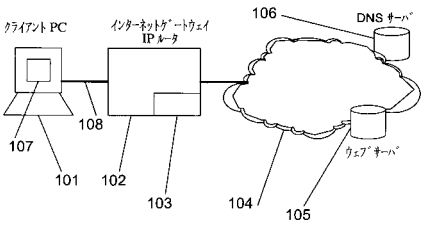
【図２】図２は、ゲートウェイ装置の機能コンポーネントの概略図である。

【図３】図３は、本実施例によるＤＮＳサーバ、ゲートウェイ装置の各コンポーネント及びクライアントアプリケーションの間の通信を説明するメッセージシーケンスチャートである。

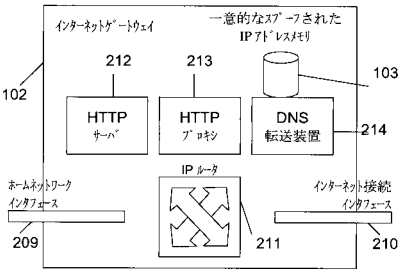
【図４】図４は、ＤＮＳサーバと接続していない期間にゲートウェイ装置によりリクエストが受信された後、本発明によるゲートウェイ装置のアドレスキャッシュメモリのコンテンツを示すテーブルを示す。

【図５】図５は、接続が再確立され、“リアル”又は実際のＩＰアドレスが決定された際の図４のテーブルを示す。

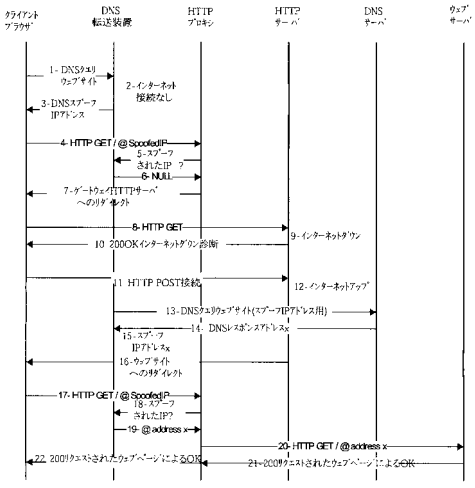
【図１】



【図２】



【図３】



【図４】

スプーフされた IP	FQDN / URL	実際の IP
a.b.c.d	Proxy.xyz.be	NULL
e.f.g.h	www.abc.be	NULL

【図５】

スプーフされた IP	FQDN / URL	実際の IP
a.b.c.d	Proxy.xyz.be	80.200.248.199
e.f.g.h	www.abc.be	216.239.57.104

フロントページの続き

(72)発明者　ファン　デ　プール，ディルク
ベルギー国，２６５０　エデヘム，アヒト・エーウェンラーン　２４／６
(72)発明者　デュ　トレ，ティエリー
ベルギー国，９０８０　ロヒリスティ，トレインデストラート　４１

審査官　脇水　佳弘

(56)参考文献　特開２００３－２９８６１８（ＪＰ，Ａ）
特開２００１－２８５３６６（ＪＰ，Ａ）
特開２００４－３２８６３０（ＪＰ，Ａ）
特開２００６－０２００１７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 12/00-66