(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2010-33539
(P2010-33539A)
(43)公開日　平成22年2月12日(2010.2.12)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330A	5B089
G06F 13/00	(2006.01)	G06F	13/00	351Z	5B285

審査請求 有　請求項の数 13　ＯＬ　（全 12 頁）

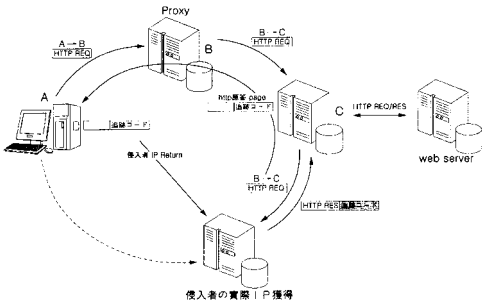
(21)出願番号　特願2009-111201 (P2009-111201)
(22)出願日　平成21年4月30日 (2009.4.30)
(31)優先権主張番号　10-2008-0074727
(32)優先日　平成20年7月30日 (2008.7.30)
(33)優先権主張国　韓国 (KR)

(71)出願人　596180076
韓國電子通信研究院
Ｅｌｅｃｔｒｏｎｉｃｓ ａｎｄ Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎｓ Ｒｅｓｅａｒｃｈ Ｉｎｓｔｉｔｕｔｅ
大韓民国大田廣域市儒城區柯亭洞１６１
１６１ Ｋａｊｏｎｇ－ｄｏｎｇ，Ｙｕｓｏｎｇ－ｇｕ，Ｔａｅｊｏｎ ｋｏｒｅａ
(74)代理人　100075812
弁理士　吉武　賢次
(74)代理人　100088889
弁理士　橘谷　英俊
(74)代理人　100082991
弁理士　佐藤　泰和

最終頁に続く

(54)【発明の名称】リバースキャッシングプロキシを用いたウェブ基盤の逆追跡システム

(57)【要約】　（修正有）
【課題】クライアントに別途のエージェントプログラムを設置しなくても匿名のサーバを経由する接続者の実際ネットワーク情報と位置を把握することができ、悪意的な接続者によりウェブ攻撃が発生した場合、ウェブサーバに被害が発生しないようにするリバースキャッシングプロキシを用いた逆追跡システム及び方法を提供する。
【解決手段】クライアントからウェブサーバに転送するＨＴＴＰのヘッダを分析して、クライアントが匿名のサーバを利用したか否かを判断するリバースキャッシングプロキシサーバと、前記プロキシサーバから匿名のサーバに対する利用の可否が通報されると、追跡コードが付加されたＨＴＴＰ応答ページを生成して前記プロキシサーバを介してクライアントに提供するウェブ追跡サーバとを含み、追跡コードは、応答ページを受信したクライアントのウェブブラウザで自動実行されてクライアントのネットワーク情報をウェブ追跡サーバに提供する。
【選択図】図１



【特許請求の範囲】
【請求項１】
ウェブサーバに接近するクライアントから転送するＨＴＴＰパケットのヘッダを分析して、前記クライアントが匿名のサーバを利用したか否かを判断するリバースキャッシングプロキシサーバと、
前記リバースキャッシングプロキシサーバから前記匿名のサーバに対する利用の可否が通報されると、前記ＨＴＴＰパケットに対する応答ページを生成し、かつ、前記応答ページには追跡コードを付加し、追跡コードが付加された応答ページを前記リバースキャッシングプロキシサーバを介して前記クライアントに提供するウェブ追跡サーバとを含み、
前記追跡コードは、前記クライアントが前記応答ページを受信する時、前記クライアントのウェブブラウザで自動実行され、前記クライアントのネットワーク情報を前記ウェブ追跡サーバに提供することを特徴とするリバースキャッシングプロキシを用いたウェブ基盤の逆追跡システム。
【請求項２】
前記リバースキャッシングプロキシサーバは、
前記匿名のサーバに対するブラックリストを具備するデータベースと、
前記ブラックリストを参照して前記クライアントが前記匿名のサーバを利用したか否かを判断するＨＴＴＰヘッダ分析モジュールと、
を含むことを特徴とする請求項１に記載のリバースキャッシングプロキシを用いたウェブ基盤の逆追跡システム。
【請求項３】
前記ＨＴＴＰヘッダ分析モジュールは、
前記ＨＴＴＰパケットの分析により前記クライアントが前記匿名のサーバを利用する時、前記ブラックリストを参照して前記クライアントが用いた匿名のサーバを判断し、
前記クライアントが用いた匿名のサーバに対するリストが前記ブラックリストに存在しない場合、前記匿名のサーバに対するリストを前記ブラックリストに追加することを特徴とする請求項２に記載のリバースキャッシングプロキシを用いたウェブ基盤の逆追跡システム。
【請求項４】
前記リバースキャッシングプロキシサーバは、
前記ウェブサーバ側ウェブページをキャッシング（cashing）するキャッシュディレクトリをさらに含み、
前記クライアントが前記匿名のサーバを用いない場合、前記クライアントが要請するウェブページを前記ウェブサーバの代わりに前記キャッシュディレクトリに要請することを特徴とする請求項２に記載のリバースキャッシングプロキシを用いたウェブ基盤の逆追跡システム。
【請求項５】
前記リバースキャッシングプロキシサーバは、
前記クライアントが要請するウェブページが前記キャッシュディレクトリに存在しない場合、前記クライアントが要請したウェブページの転送を前記ウェブサーバに要請することを特徴とする請求項４に記載のリバースキャッシングプロキシを用いたウェブ基盤の逆追跡システム。
【請求項６】
前記ウェブ追跡サーバは、
前記リバースキャッシングプロキシサーバと連結状態を維持し、前記リバースキャッシングプロキシサーバから前記クライアントのプロキシ接続の可否を受信するウェブ追跡処理モジュールと、
前記クライアントが前記プロキシサーバを経由して前記ウェブサーバに接続する時、これを前記ウェブ追跡処理モジュールから受信し、これに応答して前記ウェブサーバが前記クライアントに転送する応答ページに追跡コードを付加する追跡コード挿入モジュールと

、
前記追跡コードが前記クライアントのウェブブラウザで自動実行される時、前記自動実行された追跡コードとＸＭＬソケット通信を遂行するＸＭＬソケット通信モジュールと、
前記ＸＭＬソケット通信モジュールで前記クライアントのネットワーク情報を受信すると、これを格納するデータベースと、
を含むことを特徴とする請求項１に記載のリバースキャッシングプロキシを用いたウェブ基盤の逆追跡システム。
【請求項７】
前記追跡コードは、
Ｊａｖａスクリプトで作成され、
前記クライアントのウェブブラウザで自動実行され、
前記ウェブブラウザで自動実行の後、前記クライアントのＩＰ、ＭＡＣアドレス、及びホストのうち、どれか１つに対する情報を前記ＸＭＬソケット通信を介して前記ウェブ追跡サーバへ転送し、転送が完了すれば閉じる（Close）ことを特徴とする請求項６に記載のリバースキャッシングプロキシを用いたウェブ基盤の逆追跡システム。
【請求項８】
前記ウェブ追跡処理モジュールは、
前記クライアントへ転送された前記追跡コードが前記クライアントのネットワーク情報を転送する時、前記ネットワーク情報に基づいて前記クライアントの位置を判断するネットワーク情報照会サーバへ転送し、前記ネットワーク情報照会サーバから前記ネットワーク情報に該当する位置情報を受信した後、前記データベースに記録することを特徴とする請求項７に記載のリバースキャッシングプロキシを用いたウェブ基盤の逆追跡システム。
【請求項９】
クライアントとウェブサーバとの間に設けられるリバースキャッシングプロキシサーバを介して遂行され、
前記クライアントが前記ウェブサーバへ転送するＨＴＴＰパケットのヘッダを受信及び分析して、前記クライアントが匿名のプロキシサーバを用いて前記ウェブサーバに接近するか否かを判断するステップと、
前記クライアントが前記匿名のプロキシサーバを用いて前記ウェブサーバに接近を試みた場合、前記ＨＴＴＰパケットに対する前記ウェブサーバの応答ページを前記クライアントへ転送し、かつ、
前記クライアントのネットワーク情報を発送する追跡コードが挿入された応答ページを転送するステップと、
を含むことを特徴とするリバースキャッシングプロキシを用いたウェブ基盤の逆追跡方法。
【請求項１０】
前記追跡コードは、
Ｊａｖａスクリプトで作成され、前記クライアントのウェブブラウザで自動遂行されることを特徴とする請求項９に記載のリバースキャッシングプロキシを用いたウェブ基盤の逆追跡方法。
【請求項１１】
前記ネットワーク情報は、
前記クライアントのＩＰ、ＭＡＣアドレス、及びホストのうち、どれか１つに対する情報であることを特徴とする請求項９に記載のリバースキャッシングプロキシを用いたウェブ基盤の逆追跡方法。
【請求項１２】
前記リバースキャッシングプロキシサーバは、
前記ウェブサーバ側ウェブページをキャッシング（cashing）し、
前記クライアントが正規接続を遂行する時、前記クライアントが要求するウェブページを前記キャッシングしたウェブページに取り替えて発送することを特徴とする請求項９に

記載のリバースキャッシングプロキシを用いたウェブ基盤の逆追跡方法。
【請求項１３】
前記追跡コードは、
前記クライアントのウェブブラウザで自動遂行の後、
ＸＭＬソケット通信を介して前記クライアントのネットワーク情報を前記ウェブ追跡サーバへ転送することを特徴とする請求項９に記載のリバースキャッシングプロキシを用いたウェブ基盤の逆追跡方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、リバースキャッシングプロキシを用いたウェブ基盤の逆追跡システム及び方法に関し、特に自身のネットワーク情報を隠すために匿名のプロキシを用いてウェブサーバに非正規接続を遂行するクライアントへウェブサーバの応答ページを転送し、かつ応答ページに追跡コードを挿入して転送し、応答ページに挿入された追跡パケットがクライアントのネットワーク情報を取り出すようにすることで、ウェブサーバに侵入する接続者を追跡するリバースキャッシングプロキシを用いたウェブ基盤の逆追跡システム及び方法に関する。
【０００２】
本発明は、情報通信部及び情報通信研究振興院との情報通信研究開発事業の一環として遂行した研究から導出したものである［課題管理番号２００７－Ｓ－０２２－０２２、課題名：ＡＩＩ－ＩＰ環境の知能型サイバー攻撃監視及び追跡システム開発］。
【背景技術】
【０００３】
従来の防火壁と侵入探知システムは、受信されるネットワークパケットのヘッダを分析してネットワークパケットのソースとターゲットアドレスを獲得し、これに基づいて接続者の接続経路を推定する。したがって、ウェブサーバや、その他のネットワーク装置に侵入しようとする接続者は、自身のネットワーク情報（例えば、ＩＰ）を隠すために匿名のサーバを経由する方法を主に用いている。匿名のサーバはウェブサーバの代わりをして接続者が希望するウェブページをキャッシングしておいてから、これを接続者に提供するサーバであって、本来はネットワークトラフィックを低減するためのものであるが、現在、ウェブサーバに侵入しようとする接続者の中間経由地として活用されている。
【０００４】
これは、ＨＴＴＰパケットの構造による。ＨＴＴＰパケットは、発送地のＩＰと目的地のＩＰを記載するが、接続者が匿名のサーバを介してウェブサーバに接近すれば、接続者の発送地ＩＰが匿名のサーバに設定される。したがって、従来の防火壁や侵入探知システムは、匿名のサーバを介して接近する接続者の実際の位置を追跡することに困難性がある。勿論、接続者が用いた匿名のサーバを照会して情報を得ることもできるが、このような逆追跡過程は多くの時間と努力を要するものであり、悪意的な接続者が複数の匿名のサーバを経由したならば、接続者を探すことは一層困難になる。
【０００５】
このような問題点を解決するために、Ｊａｖａ（登録商標）アプレット、またはＡｃｔｉｖｅ－Ｘ基盤の逆追跡方式が検討されたが、接続者が自身のウェブブラウザでポップアップウィンドウを遮断したり、別途の保安プログラムを用いて無力化する場合、期待する役目を遂行することができない。
【０００６】
その他にも大韓民国登録特許１０－０５７７８２９（ウェブ接続者位置追跡システム及びその追跡方法；以下、引用文献という）は、接続者のウェブブラウザで更に他のインターネット連結プログラムを接続者が実行するように誘導し、実行されたインターネット連結プログラムが接続者の位置を確認するようにするシステム及び方法を提案したことがあるが、引用文献はクライアントに提供すべきＨＴＭＬソースコード全体を修正して動画メ

ディアプロトコルを用いた通信を遂行しなければならないという問題点がある。
【発明の開示】
【発明が解決しようとする課題】
【０００７】
本発明の目的は、接続者のクライアントがウェブサーバに接続するために転送するＨＴＴＰパケットに対する応答ページに追跡コードを付加してクライアントへ転送し、これを用いて接続者の実際ネットワーク情報及び位置を追跡するリバースキャッシングプロキシを用いたウェブ基盤の逆追跡システム及び方法を提供することにある。
【０００８】
また、本発明の他の目的は、悪意的な接続者によりウェブ攻撃が発生した場合、ウェブサーバに加えられる被害を最小化し、ウェブサーバが正常なサービスを再開できるようにするリバースキャッシングプロキシを用いたウェブ基盤の逆追跡システム及び方法を提供することにある。
【０００９】
また、本発明の更に他の目的は、クライアントに特定のエージェントプログラムを設置しなくても匿名のサーバを経由地にしてウェブサーバに接続する接続者の実際の位置とネットワーク情報が獲得できるようにするリバースキャッシングプロキシを用いたウェブ基盤の逆追跡システム及び方法を提供することにある。
【課題を解決するための手段】
【００１０】
本発明は、ウェブサーバに接近するクライアントから転送するＨＴＴＰパケットのヘッダを分析して、上記クライアントが匿名のサーバを利用したか否かを判断するリバースキャッシングプロキシサーバと、上記リバースキャッシングプロキシサーバから上記匿名のサーバに対する利用の可否が通報されると、上記ＨＴＴＰパケットに対する応答ページを生成し、かつ、上記応答ページには追跡コードを付加し、追跡コードが付加された応答ページを上記リバースキャッシングプロキシサーバを介して上記クライアントに提供するウェブ追跡サーバとを含み、上記追跡コードは、上記クライアントが上記応答ページを受信する時、上記クライアントのウェブブラウザで自動実行され、上記クライアントのネットワーク情報を上記ウェブ追跡サーバに提供することを特徴とする。
【発明の効果】
【００１１】
本発明によると、匿名のプロキシサーバを介して侵入する接続者の実際ネットワーク情報と位置を把握することができる。
【００１２】
また、クライアントに別途のエージェントプログラムを設置しなくても接続者の実際ネットワーク情報と位置を把握することができる。
【００１３】
また、匿名のプロキシサーバを経由する接続者のクライアントがウェブサーバに接続要請のためにＨＴＴＰパケットを転送すると、これに応答するウェブサーバの応答ページの中に追跡コードを挿入してフィードバックするので、接続者の疑心を避けることができる。
【００１４】
仮に、接続者によりウェブサーバに対する攻撃が発生すると、ウェブサーバの代わりをして予めキャッシングされたウェブサーバのウェブページやコンテンツを提供するようにし、これを通じてリバースキャッシングプロキシサーバがウェブサーバの代わりをして悪意的な接続者の攻撃ターゲットになるようにすることで、ウェブサーバを完全に守ることができる。
【発明を実施するための最良の形態】
【００１５】
以下、図面を参照しつつ本発明を詳細に説明する。

【００１６】
図１は、本発明のリバースキャッシングプロキシを用いたウェブ基盤の逆追跡システムの連結関係と全般的な作動概念を示す。
【００１７】
図示されたリバースキャッシングプロキシを用いたウェブ基盤の逆追跡システムは、ウェブサーバ２００とクライアント１０との間に設けられるリバースキャッシングプロキシサーバ１１０及びウェブ追跡サーバ１２０から構成される。
図面において、クライアント１０が匿名のサーバ５０に接続する時、クライアント１０のＨＴＴＰパケットには接続経路が“Ａ－>Ｂ”であり、クライアント１０が匿名のサーバ５０を経由してリバースキャッシングプロキシサーバ１１０に接続すると、接続経路は“Ｂ－>Ｃ”になるので、接続者の最終の接続経路は“Ｂ－>Ｃ”と表れる。従来の防火壁や侵入探知システムは接続者の接続経路を“Ｂ－>Ｃ”と把握する。
【００１８】
本発明において、リバースキャッシングプロキシサーバ１１０は、匿名のサーバ５０に対する情報リスト、及びウェブサーバ２００が位置する地域、または国家に対するＩＰ割り当て情報を具備する。これを用いてリバースキャッシングプロキシサーバ１１０は、接続者が匿名のサーバ５０を用いたか否かを判断する。仮に、接続者がウェブサーバ２００に非正規の接続（プロキシサーバのような中間経由地を用いた接続）を遂行する時、リバースキャッシングプロキシサーバ１１０は、ウェブサーバ２００の代わりをして接続者のクライアント１０を介してウェブサーバに転送されるＨＴＴＰパケットに対する応答ページをクライアント１０へ転送する。この際、クライアント１０へ転送される応答ページにはクライアント１０のネットワーク情報を獲得し、これをウェブ追跡サーバ１２０にフィードバックする追跡コードが含まれる。
追跡コードはＪａｖａスクリプトで作成され、クライアント１０のウェブブラウザで自動実行される。追跡コードはクライアント１０のウェブブラウザで実行された後、クライアント１０のＩＰ、ＭＡＣアドレス、及びクライアント１０が用いるホストのうち、どれか１つに対する情報を獲得することができる。獲得されたネットワーク情報はＸＭＬソケット通信を用いてウェブ追跡サーバ１２０へ転送され、ネットワーク転送が完了した後、追跡コードはＸＭＬソケット通信を終了する。したがって、ＨＴＴＰプロトコルによりウェブサーバ２００に侵入しようとする接続者は、自身のクライアント１０でＸＭＬソケット通信の遂行の可否を認知することが困難であり、自分も知らないうちにウェブサーバ２００に侵入しようとする接続者は自身のネットワーク情報が露出される。追跡コードは匿名のサーバ５０を用いる接続者のみに付加され、大多数の善意の接続者には付加されなくても良い。
【００１９】
一方、リバースキャッシングプロキシサーバ１１０は、ウェブサーバ２００に設けられるウェブページやコンテンツをキャッシングして置き、キャッシングされたウェブページやコンテンツをクライアント１０にフィードバックする。リバースキャッシングプロキシサーバ１１０は、ウェブサーバ２００の代わりをしてウェブページやコンテンツをクライアント１０に提供する。仮に、クライアント１０が要請するウェブページやコンテンツがリバースキャッシングプロキシサーバ１１０にキャッシングされていない場合、リバースキャッシングプロキシサーバ１１０は、ウェブサーバ２００に該当ウェブページやコンテンツを要請して受信し、これをクライアント１０に提供する。
【００２０】
このような特徴により、悪意的な外部接続者がウェブサーバ２００を攻撃する時、リバースキャッシングプロキシサーバ１１０がウェブサーバ２００の代わりをして攻撃に応答する。したがって、最悪の場合にもウェブサーバ２００に対する攻撃の被害はリバースキャッシングプロキシサーバ１１０が負担することになり、ウェブサーバ２００は外部攻撃により被害を蒙らない。
【００２１】

図２は、図１に図示されたリバースキャッシングプロキシサーバ１１０とウェブ追跡サーバ１２０に対する詳細ブロック概念図を示す。

【００２２】

まず、リバースキャッシングプロキシサーバ１１０は、ＨＴＴＰ要請受信モジュール１１１、ＨＴＴＰヘッダ分析モジュール１１２、データベース１１３、キャッシュディレクトリ１１４、及びＨＴＴＰ応答転送モジュール１１５を具備する。

【００２３】

ＨＴＴＰ要請受信モジュール１１１は、クライアント１０がネットワークを介してウェブサーバ２００へ転送するＨＴＴＰパケットを受信し、これをＨＴＴＰヘッダ分析モジュール１１２へ転送する。

データベース１１３は、知られた匿名のサーバ（例えば、参照符号５０）とホストに対するブラックリスト及びＩＰ割り当て情報を具備する。ＩＰ割り当て情報は、ウェブサーバ２００やリバースキャッシングプロキシサーバ１１０が位置する地域や国家に割り当て可能なＩＰ情報を意味する。

ＨＴＴＰヘッダ分析モジュール１１２は、ブラックリスト、またはＩＰ割り当て情報を参照して、既存に知られたプロキシサーバや、未だ知られてはいないが、匿名のサーバ５０を用いたことと疑わしいクライアント１０を判断する。また、ＨＴＴＰヘッダ分析モジュール１１２は、クライアント１０から要請したウェブページをキャッシュディレクトリ１１４に要請する。

【００２４】

ＨＴＴＰヘッダ分析モジュール１１２は、プロキシサーバのような中間経由地を用いたクライアント１０に対する情報をウェブ追跡サーバ１２０に通報する。以後、ＨＴＴＰヘッダ分析モジュール１１２は、ウェブ追跡サーバ１２０を介してＨＴＴＰパケットに対する応答ページ（追跡コードが挿入された応答ページ）を受信し、これをＨＴＴＰ応答転送モジュール１１５を介してクライアント１０に提供する。

【００２５】

この際、応答ページには追跡コードが挿入され、追跡コードは図１を通じて前述したように、クライアント１０のウェブブラウザで自動実行された後、ウェブ追跡サーバ１２０にクライアント１０のネットワーク情報を提供するようになる。

キャッシュディレクトリ１１４は、ウェブサーバ２００に設けられるウェブページやコンテンツを獲得して予め格納して置き、ＨＴＴＰヘッダ分析モジュール１１２からウェブページやコンテンツの要請がある時、該当するウェブページやコンテンツをリターンする。ＨＴＴＰヘッダ分析モジュール１１２は、匿名のサーバ５０を中間経由地を用いたことと疑わしいクライアント１０が転送するＨＴＴＰパケットに対する応答ページをウェブ追跡サーバ１２０から獲得してリターンする。

したがって、クライアント１０のウェブブラウザでは、追跡コードが実行された状態となり、追跡コードはウェブ追跡サーバ１２０へクライアント１０のネットワーク情報を転送する。

ウェブ追跡サーバ１２０は、ウェブ追跡処理モジュール１２１、ＸＭＬソケット通信モジュール１２２、追跡コード挿入モジュール１２３、及びデータベース１２４を含む。

【００２６】

ウェブ追跡処理モジュール１２１は、ＨＴＴＰヘッダ分析モジュール１１２と接続状態を維持し、ＨＴＴＰヘッダ分析モジュール１１２を介してプロキシサーバのような中間経由地を用いたクライアント１０に対する情報を獲得する。ウェブ追跡処理モジュール１２１は、中間経由地を用いたことと疑わしいクライアント１０に対する情報を追跡コード挿入モジュール１２３に通報する。追跡コード挿入モジュール１２３は、クライアント１０がリバースキャッシングプロキシサーバ１１０へ転送したＨＴＴＰパケットに対する応答ページに追跡コードを付加した後、ウェブ追跡処理モジュール１２１へリターンする。ウェブ追跡処理モジュール１２１は、これをＨＴＴＰヘッダ分析モジュール１１２に提供し、ＨＴＴＰヘッダ分析モジュール１１２はＨＴＴＰ応答転送モジュール１１５を介して追

跡コードが植えられた応答ページをクライアント１０へ転送する。

【００２７】

以後、クライアント１０のウェブブラウザで自動実行された追跡コードがクライアント１０のネットワーク情報（例えば、ＩＰ、ＭＡＣアドレス、及びホスト情報のうちの１つ）を獲得した後、ＸＭＬソケット通信を遂行すると、ＸＭＬソケット通信モジュール１２２は追跡コードとＸＭＬソケット通信を遂行してクライアント１０のネットワーク情報を受信する。

【００２８】

ＸＭＬソケット通信モジュール１２２が獲得したクライアント１０のネットワーク情報は、ウェブ追跡処理モジュール１２１に提供され、ウェブ追跡処理モジュール１２１はこれをデータベース１２４に記録する。

【００２９】

ウェブ追跡処理モジュール１２１は、ＸＭＬソケット通信モジュール１２２を介してクライアント１０のネットワーク情報を獲得した時点、または、今後ネットワーク管理者によりクライアント１０のネットワーク情報に対する照会要請が発生する時、ネットワーク情報照会サーバ３００へクライアント１０のネットワーク情報（例えば、ＩＰ）を転送し、ネットワーク情報照会サーバ３００を介してクライアント１０の位置情報を獲得する。ネットワーク情報照会サーバ３００は、大韓民国の場合“ＷＨＯＩＳ”サービスを提供するサーバを意味する。

【００３０】

図３は、本発明に係るリバースキャッシングプロキシを用いたウェブ基盤の逆追跡方法に対するフローチャートである。

【００３１】

本発明に係るリバースキャッシングプロキシを用いたウェブ基盤の逆追跡方法は、リバースキャッシングプロキシサーバ１１０を中心として遂行される。

【００３２】

まず、クライアント１０がウェブサーバ２００に接近するためにウェブサーバ２００へＨＴＴＰパケットを転送すると、クライアント１０が送ったＨＴＴＰパケットを受信（Ｓ４０１）し、これをＨＴＴＰヘッダ分析モジュール１１２に伝達する。

【００３３】

ＨＴＴＰヘッダ分析モジュール１１２は、ウェブサーバ２００に接近する時に使われるＨＴＴＰプロトコルに従うヘッダ情報でクライアント１０のインターネットアドレス及びホスト名を分析して、クライアント１０が匿名のサーバ（例えば、参照符号５０）を経由したか否かを確認した後、その結果をデータベース１１３に格納する（Ｓ４０２）。そのために、ＨＴＴＰヘッダ分析モジュール１１２は、データベース１１３に設けられるブラックリスト及びＩＰ割り当て情報を参照し、仮にクライアント１０がブラックリストに登録されていないプロキシサーバを用いた場合、ＩＰ割り当て情報を参照して迂回経路の利用の可否を判断し、ブラックリストに新たな迂回経路を記録する。

【００３４】

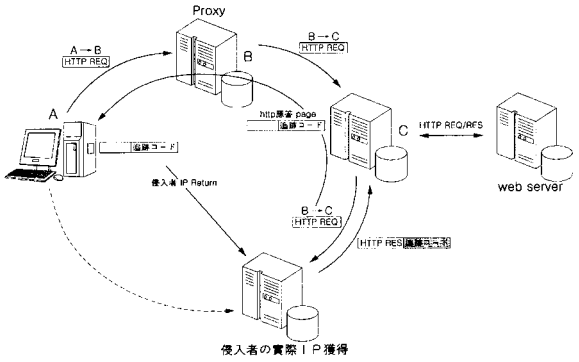
次に、ＨＴＴＰヘッダ分析モジュール１１２は、クライアントが要請したページをキャッシュディレクトリ１１４が保有しているか否かを確認する（４３０３）。仮に、クライアント１０が要請したウェブページ（または、コンテンツ、以下省略）がキャッシュディレクトリ１１４に存在しなければ、クライアント１０が要請したページが有効ページであるか否かを確認し（Ｓ４０４）、有効ページであればＨＴＴＰヘッダ分析モジュール１１２へ送る。

仮に、要請したウェブページが存在しなかったり、要請されたウェブページが有効でなければ、ウェブサーバ２００に該当ウェブページを要請する（Ｓ４０５）。 キャッシュディレクトリ１１４は、ウェブサーバ２００から該当ウェブページを受信した後、格納及びアップデートの後（Ｓ４０６）、要請されたウェブページをＨＴＴＰヘッダ分析モジュール１１２へ送る。

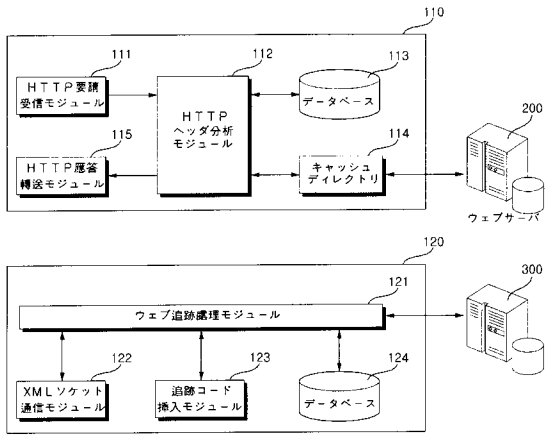
【００３５】
次に、ＨＴＴＰ応答ページを受けたＨＴＴＰヘッダ分析モジュール１１２は、ＨＴＴＰヘッダ情報分析結果を照会して、ウェブサーバ２００に接近したクライアント１０が匿名のサーバ（例えば、参照符号５０）を経由したか否かを確認する（Ｓ４０８）。
仮に、クライアント１０が匿名のプロキシを経由していなければ、ＨＴＴＰヘッダ分析モジュール１１２はＨＴＴＰ応答伝達モジュール１１５を介してクライアント１０へＨＴＴＰ応答ページを転送する。
【００３６】
仮に、クライアント１０が匿名のサーバ５０を経由したとすれば、該当匿名のサーバ５０がデータベース１１３のブラックリストに記録されているか否かを確認し、記録されていない場合、ブラックリストをアップデートする（Ｓ４０９）。次に、ウェブ追跡システム１００に該当ＨＴＴＰ応答ページを送る（Ｓ４１０）。
【００３７】
ＨＴＴＰ応答ページは、ウェブ追跡サーバ１２０の追跡コード挿入モジュール１０３に伝えられ、応答ページには不法侵入したクライアント１０のウェブブラウザで自動実行されるＪａｖａスクリプト型式の追跡コード１２０が挿入される（Ｓ４１１）。 次に、追跡コードが挿入された該当ＨＴＴＰ応答ページをリバースキャッシングプロキシ１１０を介してクライアントに伝達する（Ｓ４１２）。
【００３８】
図４は、本発明に係るクライアントで追跡コードを遂行する方法を図示した動作フローチャートである。
【００３９】
図４を参照すると、インターネットを通じてウェブサーバ２００に接近したクライアント１０に送ったＨＴＴＰ応答ページには追跡コードが隠密に隠されており、クライアント１０のウェブブラウザで自動実行される（Ｓ５０１）。
【００４０】
Ｊａｖａスクリプト型式の追跡コードは、クライアント１０が認知できないように自動で実行され、ＸＭＬソケット通信モジュール１２２と通信を遂行するためにＸＭＬソケットをオープンする（Ｓ５０２）。
次に、ＨＴＴＰプロトコルと異なるように、ＸＭＬソケットを用いたＴＣＰ／ＩＰ通信プロトコルを通じてクライアント１０がウェブ追跡システム１００に通信連結を試み（Ｓ５０３）、匿名のプロキシを使用しないクライアント１０の実際のＩＰアドレスとホスト名をウェブ追跡サーバ１２０に伝達する（Ｓ５０４）。
ウェブ追跡サーバ２００は、ＸＭＬソケットを用いたＴＣＰ／ＩＰ通信を介して獲得したクライアント１０の実際のＩＰアドレスとホスト名の追跡の結果をＤＢ１０４に格納し（Ｓ５０５）、“ＷＨＯＩＳ”サービスのようなネットワーク情報照会サービスを提供するサーバ３００を用いてクライアント１０の位置情報を獲得し、データベース１２４に共に記録する。
【００４１】
最後に、クライアント１０で駆動されている追跡コードは、ウェブ追跡サーバ１２０にクライアント側ネットワーク情報を送った後、ＸＭＬソケットを閉じて（CLOSE）、該当プロセスを終了する（Ｓ５０６）。
【００４２】
以上、説明した本発明は、添付された図面により限定されるのでなく、本発明の技術的思想から外れない範囲内で、種々の置換、変形、及び変更ができるということは、本発明が属する技術分野で通常の知識を有する当業者に当たって明白なことである。
【図面の簡単な説明】
【００４３】
【図１】本発明のリバースキャッシングプロキシを用いたウェブ基盤の逆追跡システムの連結関係と全般的な作動概念を示す図である。

【図２】図１に図示されたリバースキャッシングプロキシサーバとウェブ追跡サーバに対する詳細ブロック概念図である。
【図３】本発明に係るリバースキャッシングプロキシを用いたウェブ基盤の逆追跡方法に対するフローチャートである。
【図４】本発明に係るクライアントで追跡コードを遂行する方法を示す動作フローチャートである。
【符号の説明】
【００４４】
１１１　ＨＴＴＰ要請受信モジュール
１１２　ＨＴＴＰヘッダ分析モジュール
１１３　データベース
１１４　キャッシュディレクトリ
１１５　ＨＴＴＰ応答転送モジュール
１２１　ウェブ追跡処理モジュール
１２２　ＸＭＬソケット通信モジュール
１２３　追跡コード挿入モジュール
１２４　データベース
２００　ウェブサーバ

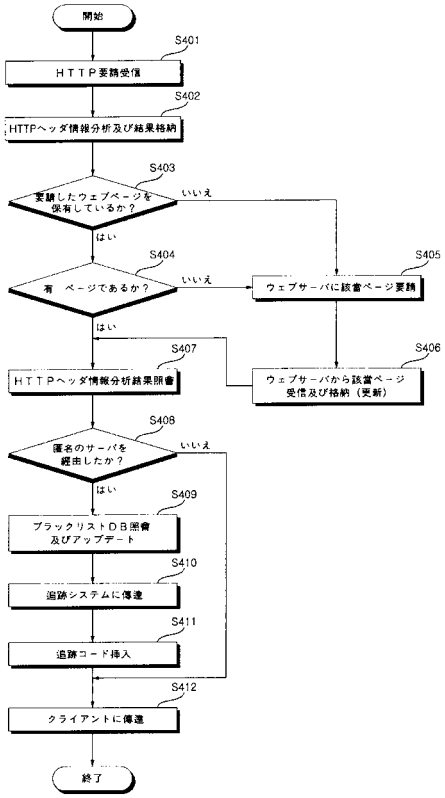
【図１】



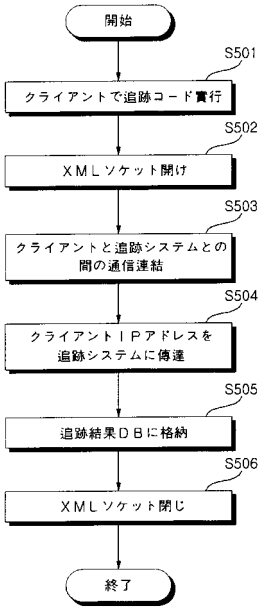
【図２】



【図３】



【図４】


開始
S501
クライアントで追跡コード実行
S502
ＸＭＬソケット開け
S503
クライアントと追跡システムとの間の通信連結
S504
クライアントＩＰアドレスを追跡システムに傳達
S505
追跡結果ＤＢに格納
S506
ＸＭＬソケット閉じ
終了

フロントページの続き

(74)代理人 100096921
弁理士 吉元 弘
(74)代理人 100103263
弁理士 川崎 康
(74)代理人 100118876
弁理士 鈴木 順生
(72)発明者 キム、ジョン、ヒュン
大韓民国テジョン、ソ‐グ、サムチョン‐ドン、ガラム、アパート、１０－１２０６
(72)発明者 キム、ゴン、リャン
大韓民国テジョン、ユソン‐グ、ガジョン‐ドン、２３６－１、エトリ、ドミトリー、３２７
(72)発明者 リュ、ジョン、ホ
大韓民国チュンナム、チョナン‐シ、サンヨン‐ドン、２０７７、サンヨン、ドンイル、ハイビル、アパート、１０４－１２０４
(72)発明者 ジョン、チ、ユン
大韓民国テジョン、ユソン‐グ、シンソン‐ドン、１４０－８、３０２
(72)発明者 ソーン、ソン、ギャン
大韓民国テジョン、ユソン‐グ、シンソン‐ドン、テリム、デュレ、アパート、１０３－４０７
(72)発明者 チャン、ボム、ホワン
大韓民国テジョン、ユソン‐グ、ジョンミン‐ドン、エキスポ、アパート、４０５－１２０５
(72)発明者 ナ、ジュン、チャン
大韓民国テジョン、ユソン‐グ、エオユン‐ドン、ハンビット、アパート、１１９－１３０４
(72)発明者 チョ、ヒュン、ソク
大韓民国テジョン、ユソン‐グ、エオユン‐ドン、ハンビット、アパート、１３１－１３０６

Ｆターム(参考) 5B089 GA19 GB02 HA10 HB05 JB02 KA17 KB06 MC02
5B285 AA01 AA05 AA06 AA07 BA03 CA32 CA33 DA04 DA05