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

特許第4471554号
(P4471554)

(45)発行日　平成22年6月2日(2010.6.2)　(24)登録日　平成22年3月12日(2010.3.12)

(51)Int.Cl.　F I
H04L 12/56 (2006.01)　H04L 12/56 400Z
G06F 13/00 (2006.01)　G06F 13/00 351N

請求項の数 20　(全 20 頁)

(21)出願番号　特願2001-582972(P2001-582972)
(86)(22)出願日　平成13年5月4日(2001.5.4)
(65)公表番号　特表2004-507908(P2004-507908A)
(43)公表日　平成16年3月11日(2004.3.11)
(86)国際出願番号　PCT/US2001/014493
(87)国際公開番号　WO2001/086877
(87)国際公開日　平成13年11月15日(2001.11.15)
審査請求日　平成15年7月4日(2003.7.4)
審判番号　不服2007-13376(P2007-13376/J1)
審判請求日　平成19年5月8日(2007.5.8)
(31)優先権主張番号　60/202,326
(32)優先日　平成12年5月5日(2000.5.5)
(33)優先権主張国　米国(US)

(73)特許権者　500194614
ノマディックス　インコーポレイテッド
アメリカ合衆国、９１３２０　カリフォルニア州、ニューベリー・パーク、ビジネス・センター・サークル、１１００、スウィート・１００
(74)代理人　100099623
弁理士　奥山　尚一
(74)代理人　100096769
弁理士　有原　幸一
(74)代理人　100107319
弁理士　松島　鉄男

最終頁に続く

(54)【発明の名称】ネットワーク使用監視装置及びそれに関連する方法

(57)【特許請求の範囲】
【請求項１】
通信ネットワークの使用を監視する装置であって、
ユーザ要求パケット及びネットワーク応答パケットを捕獲するように適合されると共に、捕獲されたパケットをフィルタ処理して前記捕獲されたパケットから使用監視データを抽出するように適合された使用監視モジュールと、
前記フィルタ処理された使用監視データを前記使用監視モジュールから受け取るように適合されると共に、前記ユーザ要求パケット及びネットワーク応答パケットと関連するデータを格納するように適合された、前記使用監視モジュールと通信する一時データベースと、
を含む通信ネットワーク使用監視装置において、
前記使用監視モジュールは、ユーザホスト又はネットワークサーバとは独立して単一のネットワークアクセスポイントで動作し、かつ、複数のネットワークユーザから送信される全ての要求パケット、及び、複数のネットワークサービスから送信される全ての応答パケットを捕獲するように適合され、
前記一時データベースは、ユーザによって所定の最小回数未満の回数アクセスされたに過ぎないネットワークアドレスに対するユーザ監視情報を格納するものであり、
前記通信ネットワーク使用監視装置が、ユーザによって前記所定の最小回数を超えるアクセスがされたネットワークアドレスに対するユーザ監視情報を格納する主データベースを備えていることを特徴とする通信ネットワーク使用監視装置。

【請求項２】
前記使用監視モジュールを実施するゲートウエイデバイスを更に備え、前記ゲートウエイデバイスは、前記ネットワーク内のネットワークトラフィック集合点に配置され、かつ、前記ゲートウエイは、複数のネットワークユーザからの全ての要求を受け取ると共に、ネットワークサービスからの全ての応答を受け取るように適合されることを特徴とする請求項１に記載の通信ネットワーク使用監視装置。
【請求項３】
前記使用監視モジュールは、前記捕獲されたパケットをフィルタ処理してネットワークアドレスを抽出するように適合されると共に、前記使用監視データベースは、前記ネットワークアドレスを格納するように適合されることを特徴とする請求項１に記載の通信ネットワーク使用監視装置。
【請求項４】
前記ネットワークアドレスは、ＵＲＬ（ユニフォームリソースロケーター）を更に含むことを特徴とする請求項３に記載の通信ネットワーク使用監視装置。
【請求項５】
前記使用監視モジュールは、捕獲されたパケットをフィルタ処理して、ユーザ識別，ネットワークアドレス，パケットタイムスタンプ，参照ネットワークアドレス，コンテントタイプ，コンテント長，応答ステータスコード，及びユーザ照会ストリングから成るグループから選択された少なくとも一つのタイプのデータを含む使用監視データを抽出するように適合されることを特徴とする請求項１に記載の通信ネットワーク使用監視装置。
【請求項６】
前記使用監視モジュールは、ユーザによってアクセスされた一連のネットワークアドレスを監視するように、捕獲されたパケットにナビゲーションシーケンスを実行するように適合されることを特徴とする請求項１に記載の通信ネットワーク使用監視装置。
【請求項７】
前記使用監視モジュールは、ユーザが要求されたネットワークサービスアドレスへアクセスしたことを検証するためにネットワークサービス応答パケットに対してステータスコードチェックを行うように適合され、それによってアクセス可能ネットワークアドレスと関連するデータのみが前記使用監視データベースに格納されることを特徴とする請求項１に記載の通信ネットワーク使用監視装置。
【請求項８】
前記使用監視データベースは、要求されたネットワークサービスからの応答を受信することに先立って、ユーザ要求データを一時的に格納するユーザ要求データベースを更に含むことを特徴とする請求項１に記載の通信ネットワーク使用監視装置。
【請求項９】
前記所定の最小回数が１回であることを特徴とする請求項１に記載の通信ネットワーク使用監視装置。
【請求項１０】
前記使用監視データベースは、ナビゲーション順序付けのために指定された、ネットワークアドレスを格納する指定ネットワークアドレスデータベースを更に含むことを特徴とする請求項１に記載の通信ネットワーク使用監視装置。
【請求項１１】
前記使用監視モジュールは、使用監視クライアントからナビゲーション順序付けのために指定されたネットワークアドレスを受け取るように適合されることを特徴とする請求項１０に記載の通信ネットワーク使用監視装置。
【請求項１２】
前記使用監視モジュールは、ユーザが前記ネットワークアドレスへアクセスする頻度に基づいてナビゲーション順序付けのために指定されたネットワークアドレスを定義するように適合されることを特徴とする請求項１０に記載の通信ネットワーク使用監視装置。
【請求項１３】

前記使用監視データベースは、前記ユーザ要求パケットとネットワーク応答パケットとに関連するデータを格納する主データベースを更に含むことを特徴とする請求項１に記載の通信ネットワーク使用監視装置。

【請求項１４】

ネットワークユーザ使用監視データに基づいてネットワークユーザにターゲット情報を提供する、前記使用監視データベースと通信する挿入サーバを更に含むことを特徴とする請求項１に記載の通信ネットワーク使用監視装置。

【請求項１５】

前記挿入サーバは、ネットワークユーザ使用監視データに基づいてネットワークユーザにターゲット広告を提供する広告挿入サーバを更に含むことを特徴とする請求項１４に記載の通信ネットワーク使用監視装置。

【請求項１６】

前記挿入サーバは、ネットワークユーザ使用監視データに基づいてネットワークユーザにターゲットサーベイを提供するサーベイ挿入サーバを更に含むことを特徴とする請求項１４に記載の通信ネットワーク使用監視装置。

【請求項１７】

通信ネットワークにおいて使用監視を行うための方法であって、

全てのネットワークユーザ送信データパケット及びネットワークサービス送信データパケットを捕獲するステップと、

前記捕獲されたパケットをフィルタ処理して使用監視データを提供するステップと、

前記使用監視データを一時データベースへ格納するステップと、

を含む通信ネットワーク使用監視方法において、

全てのネットワークユーザ生成データパケット及びネットワークサービス生成データパケットを捕獲するステップが、ユーザホスト又はネットワークサーバとは独立してアクセスの単一のネットワークポイントにおいて生じて、複数のユーザ及び複数のネットワークサービスから送信されたデータパケットの捕獲を提供し、

前記一時データベースが、ユーザによって所定の最小回数未満の回数アクセスされたに過ぎないネットワークアドレスに対するユーザ監視情報を格納し、

主データベースが、ユーザによって前記所定の最小回数を超えるアクセスがされたネットワークアドレスに対するユーザ監視情報を格納することを特徴とする通信ネットワーク使用監視方法。

【請求項１８】

前記全てのネットワークユーザ送信データパケット及びネットワークサービス送信データパケットを捕獲するステップは、全てのネットワークユーザ送信データパケット及びネットワークサービス送信データパケットをゲートウエイデバイスにおいて捕獲するステップを更に含むことを特徴とする請求項１７に記載の通信ネットワーク使用監視方法。

【請求項１９】

前記捕獲されたパケットをフィルタ処理して使用監視データを提供するステップは、前記捕獲されたパケットをフィルタ処理して使用監視データを抽出するステップを更に含み、前記使用監視データは、ユーザ識別，ネットワークアドレス，パケットタイムスタンプ，参照ネットワークアドレス，コンテントタイプ，コンテント長，応答ステータスコード，及びユーザ照会ストリングから成るグループから選択された少なくとも一つのタイプのデータより成ることを特徴とする請求項１７に記載の通信ネットワーク使用監視方法。

【請求項２０】

前記使用監視データを使用監視データベースへ格納するステップは、前記使用監視データを主データベースへ格納するステップに先立って、前記使用監視データを一時データベースへ格納するステップを更に含むことを特徴とする請求項１７に記載の通信ネットワーク使用監視方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】
本発明は、一般的に、ネットワーク使用（network usage）を監視することに関し、より詳細には、ネットワークアクセスのポイントで使用データを捕獲（キャプチャ；capture）するように動作するネットワーク使用監視装置及びこれに関連する使用監視方法に関する。
【０００２】
【従来の技術】
インターネットや社内イントラネット等の通信ネットワークは、会社内並びに自宅において、情報の配布の望ましい形態となってきている。このようなネットワークからの情報へのアクセスの必要性の増加により、このような通信ネットワークによって配布される情報を監視するための手段を提供することが必要である。ここでは、「使用監視」と呼ばれるこのような監視は、統計的或いはその他の価値のある情報をネットワークサービスプロバイダ，ネットワークユーザ，又はネットワーク広告主のようなネットワーク受益者へ提供できる。
【０００３】
これらのネットワークサービスプロバイダは、多くの異なる適用業務において使用監視から利益を得ることができる。例えば、使用監視は、ユーザがアクセスした情報、及び、ユーザがネットワークへ提供した情報に基づいて、ネットワークユーザプロファイルを生成する能力を提供する。ユーザプロファイルは、知的保存データ（すなわち、ユーザによってアクセスされたネットワークページのコピーを保存すること）及び／又はデータの先取り（すなわち、将来のネットワークページアクセスを予測しかつそれを格納すること）のような、多くの適用業務においてサービスプロバイダにとって有益である。更に、使用監視情報は、ネットワークセキュリティ侵害の場合に、役立つ。この使用監視情報は、侵害者の履歴をトレースするために使用され得る有用な侵害後情報を提供する。
【０００４】
インターネットのような通信ネットワークは、広告主が情報を配布しかつ顧客を勧誘することができる他の媒体を提供している。毎日ではないが、しばしばインターネットに依存する多くの人々のために、広告主は、インターネットを介して広告を配布するために莫大な金額を投資している。広告主にとって、残念なことは、単に大量に配布される広告は、一般的にコスト効率が高くない。その理由は、受け手の、大部分ではないが、多くは、広告される特定の製品やサービスには興味がないからである。このように、広告主は、広告される製品やサービスに最も興味があると信じられている部分的な人々を広告のターゲットとするように働くのが一般的である。例えば、新たな家の所有者は、セキュリティシステムに最も興味があり、その結果、住宅セキュリティ会社は、それらの新たな住宅所有者へ広告することをターゲットとしている。それらの潜在的な顧客ベースをターゲットにすることができるためには、広告主は、リアルタイムで使用監視データにアクセスできなければならず、かつ、特定の製品がアドレスされる集団をアドレスするためにフォーマット化、或いは容易にフォーマット化され得るデータが提供されなければならない。
【０００５】
更に、使用監視情報は、それらが使用情報に基づいてそれらの配布情報を最適化しかつクライアント及び加入者へより良いサービスを提供するように働くので、コンテント配信ネットワーク（ＣＤＮ）にとって重要であり得る。
【０００６】
家族や会社のようなネットワークユーザは、家庭や会社内の個人の使用を監視することによって、使用監視情報から利益を得ることができる。このような監視は、個人が不適切な情報にアクセスしていないこと、或いはインターネットやイントラネットのブラウジングに過度な時間費やしていないことを保証する。
【０００７】
【発明が解決しようとする課題】
インターネットのような通信ネットワークは、多くの人々が通信を行う媒体を提供するが

、ネットワークサービスプロバイダ，ネットワーク受益者，及びユーザ自身は、一般的に、ユーザの正確な性質（性格），ユーザによってアクセスされた情報のコンテント，ユーザの実態的人口統計学的分類，その他の使用関連情報を決定できなかった。例えば、ネットワーク広告主は、ユーザに関する詳細な実態的人口統計学的分類及びユーザによって要求された実際のコンテントに関する情報の両方をリアルタイムで決定することが困難であった。ネットワークサービスプロバイダは、より知的な保存能力及び先取り能力、セキュリティ侵害調査等を提供するために任意の或るユーザによってアクセスされた情報をリアルタイムでトラッキング（追跡）することが困難であった。更に、ネットワークユーザ（すなわち、家庭や会社）は、アクセスされたコンテントやアクセスセッションの期間に関して個人（家族の個々人や従業員）の使用をトラッキングする適切な手段が提供されていなかった。

【０００８】

これに関して、現在の技術は、通信ネットワーク内の異なる離散的位置でのネットワーク使用を監視するために存在する。例えば、ネットワーク通信ストリーム内に位置するネットワークサーバ及び／又はルータは、サーバによってホストされたコンテントに対するアクセス要求のログを維持することによって使用を監視できる。これらのログは、特定のページや１セットのページにアクセスするユーザの数やそれらのページを介するナビゲーションシーケンスについての情報を提供する。ソフトウェアもまたサーバーログの統計的処理を実行するために設けられている。

ウエブサーバレベルにおいて実行されているネットワーク使用監視のいくつかの例は、Shrader等の発明者の名前で２０００年２月１５日に発行された「モニタリングリソース用のウエブサーバ・アマウント・マネージャー・プラグイン（Web Server Account Manager Plugin for Monitoring Resources）」と題された米国特許第６，０２６，４４０号に見られる。このShrader等による米国特許第６，０２６，４４０号では、アプリケーション・プログラミング・インタフェース（ＡＰＩ）が、ウエブ使用の監視をウエブサーバにおいて実行するために要求される。ウエブ使用の監視は、ネットワークのいたるところで全てのウエブサーバで実行されるべきＡＩＰを必要とする。同様の関係において、Casella等の発明者の名前で１９９９年１月１４日に公開された「ネットワークアプリケーション用のテスト及びデバッグ・ツール（Testing and Debugging Tool for Network Application）」と題された国際公開第９９／０１８１９号は、監視機能を提供するデバッギング・アプリケーションである。しかしながら、Casella等による国際公開第９９／０１８１９号の刊行物において教示される監視は、１つの特定のクライエントと１つの特定のサーバとの間におけるものである。　このCasella等による国際公開第９９／０１８１９号の刊行物では、多数のクライエントと多数のネットワークとの間の監視については教示されていない。他の例は、Page等の発明者の名前で１９９８年３月１９日に公開された「ライブ・ネットワーク・インフォメーションを取得、分析及び表示するための装置及び方法」と題された国際公開第９８／１１７０２号において見出される。このPage等による国際公開第９８／１１７０２号において、監視は、１つの特定のネットワークの使用について監視されるべき多数のクライエントのために提供するネットワーク内のダウンストリーム位置において行われる。この国際公開第９８／１１７０２号は、ネットワーク・アクセス・ポイント（すなわち、アグリゲーション（aggregation）のポイント）において行われる監視についての教示はなされておらず、従って多数のクライエント及び多数のネットワークサービスの使用監視を提供することの教示はなされていない。

同様に、使用は、メモリにユーザによってアクセスされたコンテントのログを維持することによって、ユーザレベルで、すなわち、個々のコンピュータで監視できる。このログは、アクセスされたコンテント，そのコンテントを介するナビゲーションシーケンス，及び各ページに関して費やされた時間を含む、個々のユーザの使用パターンについての情報を提供する。更に、幾つかのインターネットサービスプロバイダ（ＩＰＳ）は、最も頻繁に要求された情報を格納するプロキシキャッシングサーバを含むことができる。これらのプロキシキャッシングサーバは、プロキシキャッシングサーバを介してネットワークヘル

ーチングされるこれらのユーザのウエブコンテントの使用を監視するように設計され得る。残念ながら、プロキシキャッシングサーバは、プロキシキャッシュを適切に構成するように、ネットワークアドミニストレータ等によるユーザ介在を必要とする。更に、ほとんど全てのクライアントの要求がプロキシキャッシングサーバへ向けられるわけではないので、使用データが不完全にされかつ価値が大きく減じられる。

【０００９】

上述のように、これらの従来の技術の各々は、ウエブの離散的デバイスや部分の使用に関連すると共にそれを監視する。例えば、サーバレベル及びユーザレベルで行われる監視動作（モニタリング）は、サーバで及びユーザによってそれぞれ起こる使用を監視するに過ぎないことは明瞭である。更に、プロキシキャッシングサーバを介して行われる監視動作は、特定のＩＳＰネットワークに対するクライアントの要求の幾つかを識別するに過ぎない。これらの種々のタイプの使用監視動作は、ネットワークサービスプロバイダ，ネットワーク受益者，及びネットワークユーザに対するいくらかの助けとなるが、これらのエンティティは、潜在的には多くの異なるサービスプロバイダのネットワーク上での、多くの異なるサーバによってホストされる情報にアクセスするように試みる多くの異なるユーザをカバーする非常に広範なスケールでの使用監視を要望する。

【００１０】

【課題を解決するための手段】

従って、ネットワークアクセスポイント、すなわち、ネットワークトラフィック集合ポイント、典型的にはゲートウエイデバイスや類似のネットワークインターフェースデバイスにおいてネットワーク使用を監視するためのネットワーク使用監視モジュールが提供される。そのように、本発明のネットワーク使用監視モジュールは、ゲートウエイデバイスを介して提供される種々のネットワークサービスをアクセスするように試みている多くのネットワークユーザの使用を監視できる。このように、本発明のネットワーク使用監視モジュールによって収集された使用情報は、従来の監視技術によって提供されるものよりも顕著に頑強（ロバスト；robust）である。このように、その情報は、ネットワークサービスプロバイダ，ネットワークユーザ，ネットワーク受益者等にとって一層価値が高い。更に、本発明の使用監視方法及び装置は、多くの特定の特徴を提供して監視プロセス並びに収集される使用情報の価値を向上する。

【００１１】

一実施形態において、使用監視方法及び装置は、ユーザとネットワークサービスとの間で送信されたデータの全てのバイトを捕獲してネットワークアドレス（すなわち、ユニフォーム・リソース・ロケーション（ＵＲＬ））に関連する使用情報を記録する。典型的には、使用監視方法及び装置は、ユーザがネットワークサービスへのアクセスを行いアクセス不能であると決定されたアドレスに関連する使用情報を破棄し、結果としてのデータベースのサイズを減少してそのデータベースへの引き続くサーチ動作及びデータベースのキャッシングを向上する場合（インスタンス）に情報の記憶を限定する。また、使用監視方法及び装置は、リアルタイムでのストリーミングコンテントの監視を可能とすると共に、ウエブベースのユーザ調査の実施を容易とする。本発明の使用監視方法及び装置は、更に、ユーザ照会ストリングと、ユーザによるウエブフォームへの情報入力の監視とを可能とする。

【００１２】

重要なことは、本発明の使用監視方法及び装置は、一つ又はそれより多くの指定ネットワークアドレスを含むナビゲーションシーケンスを捕獲（キャプチャ）する。これに関して、指定されたアドレスは、事前に指定されても良いし、或いはユーザ監視モジュールによって即座に最も一般的なアドレスに決定されてもよい。或いは、使用監視方法及び装置は、アドレスがアクセスされるシーケンスや順序に関係なく、指定されたネットワークアドレスの近傍（近隣）にあるアドレスを監視することができる。本発明の使用監視方法及び装置が指定されたアドレスの近傍のアドレスを監視する技術と同様に、使用監視方法及び装置は、指定されたドメインに先行の及び／又は後続のドメインを監視してもよい。更に

、使用監視方法及び装置は、指定されたアドレスに近傍にある関連アドレス、すなわち、所定数のアドレスだけ指定されたアドレスに先行の或いは後続の関連ＵＲＬを特定のナビゲーションシーケンスに関係なく監視できる。その関連するアドレスは、多くの方法で定義されることが可能で、典型的には、他の関連アドレスから区別するためにユーザ或いはネットワークアドミニストレータによって定義される。

【００１３】

通信ネットワークの使用に関連する一層頑強なセットの情報を捕獲することによって、本発明の使用監視方法及び装置は、非常に有用な情報を使用監視情報クライアントへ提供できる。例えば、使用監視方法及び装置は、詳細な人口統計調査及びアクセスされたサイトの或いはネイティブストリーミングメディアのコンテントに関連する情報を含むことができる。更に、インターネットへのゲートウエイで、すなわち、トラフィック集合のポイントで使用を監視することによって、使用監視方法及び装置は、多くの異なるサービスプロバイダへのアクセスを要求する多くのユーザの使用を監視できる。

【００１４】

【発明の実施形態】

ここで、本発明は、本発明の好適な実施形態を示す添付の図面を参照して十分に説明される。しかしながら、本発明は、多くの異なる形態で実施されることが可能であり、ここで述べられる実施形態に限定されるものとして解釈されるべきではない。むしろ、これらの実施形態は、ここでの開示が周到であると共に完全であるように提供され、本発明の範囲を当業者に十分に伝えるものである。同様の参照番号は、全体を通して同様な構成要素を示す。

【００１５】

本発明による使用監視を実施（実現）するネットワーク１０が図１に示されている。使用監視（ＵＭ；usage monitoring）モジュール１２は、ゲートウエイデバイス１４で実施（実現；implement）又はそれと通信するように配置されることが好ましい。例えば、使用監視モジュール１２がゲートウエイデバイス１４で実施される実施形態において、そのゲートウエイデバイス１４は、カリフォルニア州、ウエストレイク　ヴィレッジにあるＮｏｍａｄｉａ，Ｉｎｃ．（ノマディックス社）によって提供され、米国特許出願シリアル番号第０８／８１６，１７４号，第０９／４５８，６０２号，第０９／４５８，５６９号，及び第０９／５４１，８７７号に記述されるユニバーサル加入者ゲートウエイであり得る。これらの出願の内容は、ここで十分に述べられているように、これらを引用することによって本願明細書に組み込まれるものとする。或いは、ゲートウエイデバイス１４は、当業者にとって公知である、プログラミングモジュールを実施できる多くの他のゲートウエイデバイスの何れかであってもよい。使用監視モジュール１２は、ゲートウエイデバイス１４と共に実施することが好ましいけれども、そのモジュールやそのモジュールを実施するデバイスがネットワーク内に位置されそれによって複数のユーザからの全ての要求／照会を受信しかつネットワーク（ネットワークトラフィック集合のポイント）よりなる全てのネットワークサービスからくる全ての応答を受信する限りにおいて、他のデバイスで実施されても良いし、独立のデバイスであっても良い。本発明の一実施形態において、使用監視モジュール１２を実施するゲートウエイデバイス１４は、複数のユーザデバイス１６と通信ネットワークの残りの部分（すなわち、ルータ１８，サービスプロバイダコンプレックス２０，及びインターネット２２）との間のネットワーク内に位置する。このように、使用監視モジュール１２は、通信ネットワーク内に含まれる全てのネットワークサービスに対するトラフィック集合のポイントとして働くアクセスのネットワークポイントで実施される。

【００１６】

ネットワークユーザは、アクセスマルチプレクサ（ＭＵＸ）２４を介してゲートウエイデバイス１４と通信する、ハンドヘルド通信デバイス，ポータブル通信デバイス（すなわち、ラップトップ），パーソナルコンピュータ等の多くの異なるユーザデバイス１６を介してゲートウエイデバイス１４と通信可能である。更に、ユーザとネットワークとの間の通

信手段に依存して、ネットワークアーキテクチャは、ＤＳＬ（デジタル加入回線），ケーブル，ＬＭＤＳ（ローカルマルチポイント分配サービス），ダイアルアップ，専用回線，無線等の種々の通信手段をリンクするように働くネットワークインターフェースデバイス（ＮＩＤ）（図１では示されていない）を含んでいる。図１は、単一のアクセスマルチプレクサを介してネットワークを通信する通信ネットワークユーザを示しているが、典型的な通信ネットワークでは、ユーザの能力を拡張するための複数のネットワークインターフェースデバイスと共に複数のアクセスマルチプレクサが備えられる。

【００１７】

一般的に、ゲートウエイデバイス１４は、ＩＳＰ（インターネットサービスプロバイダ）や企業ネットワーク（すなわち、社内イントラネット等）の何れかによって提供される種々のＩＰネットワークサービスとユーザが通信することを可能とする。図１に示されるように、ゲートウエイデバイスは、サービスプロバイダサーバコンプレックス２０，インターネット２２，或いは他のネットワークサービス（図１には示されていない）へネットワーク通信を経路指定するように働くルータ１８と通信することができる。図１は、単一のルータ１８を示しているが、典型的な通信ネットワークでは、複数のルータ及び／又はスイッチングデバイスが、ネットワーク通信をアドレス指定された宛先へ適切に経路指定するためにゲートウエイデバイスと通信する。

【００１８】

本発明によれば、使用監視モジュール１２は、ユーザとネットワークサービスとの間で通信された全てのパケットを捕獲する。フィルタ処理は、ユーザ監視クライアントが監視することを希望する全ての関連するパケット（ＨＴＴＰ要求と応答、ＤＮＳ要求と応答等）を抽出してそれらを関連する使用監視データベース３０へ送るために実行される。ネットワークサービスに対するユーザの要求及びネットワークサービスからの応答は、使用監視データベースによって捕獲される。使用監視データベース３０は、使用監視モジュール１２を実施するデバイスの内部にあっても良いし、それが使用監視モジュール１２と通信上接続される限りにおいて、デバイスの外部にあってもよい。本発明の一実施形態において、使用監視データベース３０は、ＨＴＴＰ要求及び応答と関連する情報を格納し、後に述べられるように、その情報を処理する。

【００１９】

図２は、本発明の一実施形態による、一連のデータベースを有する、使用監視動作を実施するネットワークの概略図である。ネットワークアーキテクチャにおけるトラフィック集合のポイントでのゲートウエイデバイス１４の位置の結果として、ゲートウエイデバイス１４は、インターネット又は他のネットワークサービスに対して多くの加入者からの要求を受信する。これに関して、ゲートウエイデバイス１４で実施された使用監視モジュール１２は、ゲートウエイデバイス１４がプロミスキャス・モード（ｐｒｏｍｉｓｃｕｏｕｓ ｍｏｄｅ；無差別モード）で動作するので、パケットの全てを捕獲できる。図２の実施形態において、使用監視データベース１２は、使用監視処理と関連する補助データベースへアクセスする使用監視データベースサーバ３２によって実施される。

【００２０】

使用監視モジュール１２は、本発明の一態様に従って、パケットを捕獲してそれらをそれらの夫々のデータベースへ経路指定する。捕獲されたパケットがユーザからの要求や照会を表す場合には、その要求は、要求データベース３４に格納される。ユーザ要求パケットを捕獲することに加えて、使用監視モジュール１２は、ネットワークサービスによって送信された応答及び他のメッセージを表すパケットを捕獲する。これに関して、使用監視モジュール１２は、応答をそれらの夫々の要求に突き合わせる（マッチングさせる）。ユーザ要求や照会が成功すると、すなわち、ネットワークサービスがアクセスを許可するかその照会に応答すると、その応答がユーザ要求と突き合わされて、この一致したセットの要求／応答に関連する情報が一時（テンポラリ）データベース３６又は主データベース３８へ送信される。ネットワークサービスからの応答が有効な応答が直ぐには出ないことを示す場合には、このようなアクセスは否定され、アクセスは利用不能であり、サービスエラ

ーが発生する。或いは応答が受信される前にタイムアウトが発生すると、要求データベースは、そのデータベースからの関連する要求を削除する。同様に、ネットワークサービスからの要求がユーザ要求と一致しない場合には、又はその応答が所定の許容時間ウインドウ外で発生した場合には、ネットワークサービスからの応答は破棄される。有効な応答と一致しない要求及びその応答を破棄する能力を備える本発明のこの態様は、使用監視装置に記憶を保存させることを可能とし、それによって使用監視装置を支援するために必要な記憶空間を最小とする。応答が成功しなかった要求／照会を永久的には格納しないことによって、主データベース３８は、サーチ／キャッシング動作に優れた性能を知的に提供し得る。

【００２１】

使用監視モジュール１２がユーザ要求をネットワークサービス応答に突き合わせると、その要求及び応答において見つけられる情報は、一時データベース３６又は主データベース３８の何れかに格納される。使用監視モジュール１２は、ユーザ要求がウエブページのような、特定のネットワークサービスに対する事前決定された数の初期要求の一つであるか否かを決定する。その要求が初期要求或いは事前決定された数の初期要求内であることが決定されると、その要求及び応答に見られる情報が一時データベースへ格納される。ネットワークサービスが事前決定された回数を越えてアクセスした場合には、その情報は、主データベース３８に転送されて格納され、それに続く要求／応答が、主データベースへプロキシ(proxy)されかつ格納される。一時データベースの実現によって、多くのネットワークサービスが一回に或いは最小の回数で要求されるのに過ぎないこと、従って、使用データ情報の処理が発生すると、これらの最小使用要求／応答の統計的存在は必要ないことの事実が補償される。これに関して、主データベースは、結果としての使用監視情報クライアント（すなわち、ネットワークサービスプロバイダ，ネットワーク受益者，或いはネットワークユーザ）によって、データベースの引き続く処理へより適合するように最小化される。ユーザの全てのアクティビィティを記録することとデータベースを能率的にすることとの競合する目標（ゴール）をバランスするために所定数の初期要求が選択されるように、使用監視モジュール１２が構成され得る。しかしながら、幾つかの場合には、所定数が１に設定される。

【００２２】

更に、本発明のネットワーク使用監視装置は、指定ネットワークアドレスのデータベース４０を含んでいる。指定ネットワークアドレスは、典型的に、ネットワーク使用監視アドミニストレータ、典型的にはゲートウエイデバイスアドミニストレータ等によって事前定義される、たびたびビジットされるネットワークアドレスである。指定ネットワークアドレスは、使用監視情報クライアントが特に重要と考える頻度の最も高いアドレスである。使用監視モジュール１２は、「指定されたもの」として事前定義されるこれらのネットワークアドレスのための、指定のネットワークアドレスのデータベースに、ナビゲーションシーケンスを格納させることを許容する。ナビゲーションシーケンスは、典型的には、事前定義された数の、ユーザによってアクセスされた直前及び／又は直後のネットワークアドレスを含んでいる。例えば、コマーシャルの広告主のようなネットワーク受益者は、特定のインターネットサイトが使用監視目的で指定されるべきことを望む場合がある。そのような場合、ネットワークユーザが指定インターネットサイトにアクセスすると、使用監視モジュール１２は、そのネットワークアドレスを指定されたものであると認識し、指定ネットワークアドレスのアクセスに先行する及びそれに続く先行及び後続のナビゲーションシーケンスを記録し格納する。ナビゲーションシーケンスは、セッション同士間のインターバルが所定セッションウインドウ内にある場合には、単一のユーザセッションを越えて拡張しても良いことに留意すべきである。

【００２３】

本発明の一実施形態において、ユーザ監視装置は、ＰＣ等のような処理エンジン４２（すなわち、データベース・フロントーエンド）と通信している状態にある。処理エンジンは、使用監視データベースと通信し、かつ、処理エンジン４２上で実施されるＧＵＩ（グラ

フィカルユーザインターフェース）と関連してデータベースにアクセスする。処理エンジン４２は、使用監視クライアントのコマンドに従ってデータベースにアクセスして指定ユーザ要件に従って使用監視データを処理する。本発明の一実施形態では、処理エンジン４２は、挿入サーバ４４（図２に示される）と通信する。例えば、挿入サーバ４４は、ターゲット広告挿入サーバやターゲットサーベイ挿入サーバより成る。処理エンジン４２は、必要なコマンドを実施してどの広告又はサーベイ（調査）がネットワークプロバイダ或いはネットワーク受益者に利益を与えるかを収集された使用監視データに基づいて決定する。ターゲット広告やサーベイの決定が行われると、コマンドが挿入サーバ４４へ送られ、適切な広告やサーベイがゲートウエイデバイス１４を有する通信を介してネットワークユーザへ送信される。広告やサーベイは、典型的には、ユーザの通信デバイスへ送信されるポップアップ制御パネルの形態である。

【００２４】

図３は、本発明の一実施形態による、使用監視を行う方法のフローチャートである。ステップ１００において、典型的にはゲートウエイデバイス上で実施される使用監視モジュールは、ゲートウエイデバイス１４を介してネットワークにアクセスする複数のユーザから送信されている情報の全てのバイト及びネットワークサービスから来るバイトの全てを読み出す。ゲートウエイデバイス１４は、プロミスキャスモード（無差別モード）で動作して、宛先アドレスに関係なく、情報の全てのバイトが使用監視モジュール１２によって処理されることを確実にする。ステップ１１０において、使用監視モジュール１２は、ＴＣＰ（送信制御プロトコル）フロー中にＨＴＴＰ（ハイパーテキスト転送プロトコル）ヘッダーのスタートを検出する。

【００２５】

任意ではあるが、使用監視モジュール１２は、セッションの間、インターネットＵＲＬ（ユニフォーム・リソース・ロケータ）のような異なるネットワークアドレスの所定数より多くアクセスしたネットワークユーザの使用を監視するだけであるように設計されることが可能である。これによって、データの統合性を大きく損なうことなくデータベースが減少される。その理由は、最小数のアドレスにアクセスするに過ぎないユーザは、使用監視クライアントへ極めて重要な統計的データを提供しないからである。従って、オプションステップ１２０において、ユーザに対する現在のセッションフローが所定のしきい値最小値を越えたか否かについて決定される。ユーザが、セッションの間に、ＵＲＬに所定数を越えてはアクセスしなかった場合には、使用監視モジュール１２は、ステップ１１０において、ユーザによって送信された要求を監視し続けるが、要求の数が所定のしきい値を越えるまで要求を分析しかつ格納する。

【００２６】

ユーザがセッションの間に所定数を越えて要求を発した場合、又は使用監視モジュール１２がこのオプションフィルタを実施しない場合には、ステップ１３０において、使用監視モジュール１２は、パケットのＨＴＴＰヘッダーを分析することによって、それらのパケットが要求を表すか応答を表すかを決定する。捕獲されたパケットが要求を表す場合には、ステップ１４０において、その要求が要求データベースに格納される。捕獲されたパケットが応答を表す場合には、ステップ１５０において、その応答は、その応答におけるステータスコードが有効ステータスコードか無効ステータスコードかを決定するようにチェックされる。

【００２７】

通常、ネットワークサービスアクセス又は他の要求を監視している間は、ユーザが何らかの理由（デッドリンクであった又はサーバが一時的にダウンしていたという理由）でそのサービスにアクセスできなかったという事実は考慮されない。しかしながら、本発明の一態様においては、要求されたネットワークサービスからの応答ステータスコードは、ユーザが実際にアクセスしたネットワークサービスのアドレスのみを記録するために監視され、他の要求がデータベースから削除される。その結果、記憶量と処理演算における顕著なセービング（saving）が達成される。

【００２８】
このステータスコードは、要求されたサーバによって戻される３桁の整数である。ステータスコードの第１桁は、応答のクラスを表す。戻されるより一般的なステータスコードの幾つかは、次の通りである。
１）　２００　オーケー（ＯＫ）
２）　３０１　永久に移動
３）　３０４　変更なし
４）　４０１　無許可
５）　４０３　禁止
６）　４０４　未発見
７）　５００　インターネットサーバエラー
８）　５０１　非実行
【００２９】
２００のステータスコードは、ウエブページがビジットされることができることを指示する共に、他のステータスコードは、ウエブページがビジットされないことが指示される。応答ステータスコードが無効であることが決定されると、すなわち、２００以外のステータスコードである時には、ステップ１６０において、応答が破棄され、かつ、一致要求（マッチリクエスト）が要求データベースから削除される。更に、関連するネットワーク応答の受信に先立って所定のタイムアウト期間が経過すると、ユーザ要求が要求データベースから削除される。応答ステータスコードが有効であることが決定されると、ステップ１７０において、ネットワーク応答が要求データベース中の関連するネットワーク応答と突き合わされる。過剰な時間が要求と応答との間で経過したインスタンス（事例）におけるような、戻されたネットワーク応答に対して一致が発見されない場合には、ステップ１８０において、ネットワーク応答が破棄される。
【００３０】
ステップ１９０において、任意ではあるが、使用監視方法及び装置は、一致した要求／応答が主データベースにあるか一時データベースにあるかを決定する。全ての要求／応答並びにそれに関連する情報が主データベースに格納され得るが、本発明の一態様の使用監視方法及び装置は、要求されたネットワークサービスが最初に要求された時、或いは、それが所定回数未満の回数だけ要求されるように構成された場合には、任意ではあるが、データを最初に一時データベースに格納する。その後、ネットワークサービスが所定回数を越える回数要求されると、要求／応答情報が主データベースに転送及び／又は記録される。先に議論されたように、ネットワークアドレス、例えば、インターネットＵＲＬの多くが一回要求されるに過ぎないので、主データベースのサイズが最小化され得ると共に、任意のユーザによって一回を越える回数ビジットされるネットワークサービス要求／応答の全てを格納し続ける。これは、事前定義された最小回数未満の回数のめったに要求されない別個ではあるが一時データベースを確立することによって達成され得る。
【００３１】
従って、永久（パーマネント）データベースと一時データベースの両方にエントリがない場合（又は、一時データベースへのエントリが最小しきい値限を越える必要がまだある場合）、ステップ２００において、要求／応答情報が一時データベースに格納される。エントリが永久データベースにあると、ステップ２１０において、永久データベースが更新されて新たな要求／応答エントリを指示する。更に、一時データベースにエントリがあり、かつ、現在のアクセスが永久データベースに含まれるためにそのエントリを識別すると（すなわち、所定の最小しきい値制限を超過していると）、ステップ２１０において、（単数又は複数の）エントリが一時データベースから永久データベースへ転送される。
【００３２】
本発明の一実施形態において、使用監視データベースは、要求及びそれに関連する応答のＵＲＬを格納する。一般に、ＵＲＬは、プロトコルプレフィックス，ポート番号，ドメイン名，サブディレクトリ名，及びファイル名を含んでいる。本発明の他の実施形態におい

て、使用監視データベースは、主データベースに、要求と応答に関係する種々の他のデータを含むことが好ましい。これに関して、下記のデータは、典型的には、要求／応答から収集されて適切なデータベースに格納される。

【００３３】

ａ）　加入者識別（この識別は、それをランダム数にマッピングすることによって、使用監視クライアントへ提供される前に匿名化されることができ、ユーザの年齢，性別，収入等についての情報を提供するユーザプロファイルへインデックス付けされる）

ｂ）　ＵＲＬ（ＵＲＬは、論理的にクラスタ中に配置される）

ｃ）　タイムスタンプ－パケットが使用監視モジュールによって処理された時間を指示する。

ｄ）　参照アドレス（ＨＴＴＰヘッダーから取得される）－典型的には、ハイパーリンクをアクセスされたアドレスを提供したアドレス。

ｅ）　コンテント－タイプ（典型的には、ＨＴＴＰヘッダーから取得される）

ｆ）　コンテント長

ｇ）　応答ステータスコード

ｈ）　ユーザ照会ストリング（通常、ＣＧＩ（共通ゲートウエイインターフェース）アプリケーションに対する引数として又はフォームをポスティングするネットワークユーザの結果として送られる）

【００３４】

上記のリストは、網羅的なものではなく、他の情報もまた、その情報が最終的に使用されるアプリケーションによって命令されるように要求／応答に対して抽出され得る。

【００３５】

ユーザ要求及びネットワーク応答に含まれる情報が異なる方法で格納され得ると共に、本発明の一実施形態の主データベース３８は、図５に示されるように、関係データベースであり、このデータベースは、ユーザと夫々のアドレス／ＵＲＬを関係付ける。関係データベースは、互いに関係するデータのセットを格納するために良好に確立された方法である。この事例では、ネットワークユーザがアドレスにアクセスする度に両方の項目が格納されることに代えて、各ネットワークユーザ並びに各々のアクセスされたアドレスが一度に格納される。次に、ページの各アクセスは、アドレスにアクセスするユーザのエントリとアクセスされるアドレスのエントリとを結合するノード（関係データベースにおいては、タプルと呼ばれる）として表されることができる。次に、このノードは、アクセス時に、アクセス頻度，コンテント長，及びタイプ等のような、そのアクセス（単数又は複数）に関係付ける追加の情報を含んでいる。例えば、ユーザ１１がアドレス／ＵＲＬ２５にアクセスする事例においては、関係データベースは、表１にユーザ１１を格納すると共に、表２にアドレス／ＵＲＬ２５を格納し、ノードが表１からのエントリと表２からのエントリをリンクする。データ格納（記憶）のこのフォームは、データ検索を容易にするために提供され、それによって、使用監視クライアントは、情報を編集するために、ユーザがリンクされる全てのノードをアクセスできる。

【００３６】

図４のフローチャートによれば、本発明の他の実施形態は、ナビゲーションシーケンス捕獲の形態において、使用監視動作を含むように図解される。ネットワークサービスプロバイダとネットワーク広告主のようなネットワーク受益者は、どのネットワークサービスが最頻度でアクセスされ、かつ、それらへのアクセスに如何に多くの時間が費やされるかということのみならず、これらの繰り返しアクセスされたアドレスを含むナビゲーションシーケンスを知ることに興味がある。ネットワークアドミニストレータ及び／又はゲートウエイアドミニストレータは、サービスプロバイダ又はネットワーク受益者の遺贈において、ナビゲーション順序付け監視動作に対して指定ネットワークアドレスを事前定義する又は「指定」することができる。アドミニストレータは、指定されたネットワークアドレスを指定ネットワークアドレスデータベースに格納する。指定ネットワークアドレスに関係するナビゲーションシーケンスは、指定ネットワークアドレスのアクセスの直前及び／又

は直後にユーザによってアクセスされた事前定義された数のネットワークアドレスよりなる。典型的ナビゲーションシーケンスが単一のユーザセッションの間に発生するが、ナビゲーションシーケンスは、二つのセッション同士間のインターバルが指定されたしきい値以下にある場合、その単一のユーザセッションを越えて拡張してもよい。更に、指定ネットワークアドレスは、一つのナビゲーションシーケンスを越えるものの一部であってもよく、従って、本発明の使用監視モジュールが以下の情報を捕獲し格納する。

・指定ネットワークアドレスが一部である全てのナビゲーションシーケンス
・ネットワークアドレスが一部である（ビジット（visit）の或るしきい値を越える）最も一般的なナビゲーションシーケンス
・指定ネットワークアドレスが一部である特定のナビゲーションシーケンスの頻度

典型的には、主データベースに含まれる、ナビゲーションシーケンスデータベースの構成は、ネットワークアドミニストレータ又はゲートウエイアドミニストレータの随意である。

【００３７】

当業者に知られているように、ジップの法則（Zipf's law）は、十分に長いテキストにおける或るワードの発生回数は、頻度順の逆数であることを述べている。例えば、１０番目に頻度の高いワードは、最も頻度の高いワードよりも正確に１０回だけ少ない頻度で発生する。純粋なジップの法則の関係は容易に発生しないが、累乗の法則（発生頻度順と発生頻度との間の関係が線形ではない）は、ネットワークサービスアクセス頻度のような、広範な状態において存在する。これの一つの結果として、少数のネットワークアドレスが、ユーザアクセスの大部分を補償する（例えば、利用可能ネットワークアドレスの５％がネットワークアクセスの９５％を補償する）。これらの前提は、ネットワークアドレスのほんの僅かなパーセンテージ（例えば、５％）に対する統計的データ、すなわち、ナビゲーション順序付け等が、使用監視データベース内に容易に捕獲及び格納されることが必要であることを含む。これに関して、ネットワークサービスプロバイダ及び／又はネットワーク受益者は、ナビゲーションシーケンス監視が行われる指定ネットワークアドレスを事前定義すること、或いはデータベースによって定義される最高頻度でアクセスされたネットワークアドレスを使用監視モジュールにナビゲーションシーケンス監視させることのオプションが提供される。

【００３８】

図４のフローチャートを再び参照すると、本発明の使用監視モジュールは、っほぼアルタイムで、指定ネットワークアドレスのナビゲーションシーケンスを監視する。図４のフローチャートのステップ１００～１８０は、図３のフローチャートのステップと同一であり、従って、これらのステップについては、これ以上議論する必要がない。ナビゲーションシーケンス監視動作は、本発明に従って、各ユーザによってアクセスされた先行のｋ個のネットワークアドレスのトラックをそれらの現在のセッションの間にわたり維持することによって達成される。数値ｋは、指定されたネットワークアドレスに先行する及びそれに続くネットワークアドレスの数を指す。ｋ値は、ネットワーク又はゲートウエイアドミニストレータによって指定され、異なる指定ネットワークアドレスによって異なっても良い。この記述は、指定されたネットワークアドレスの前後の両方で同じ数のネットワークアドレスが監視されてもよいが、必要に応じて、異なる値が先行及び後続するネットワークアドレスに対して指定されても良い。

【００３９】

ステップ２２０において、使用監視モジュールは、ネットワークユーザが先行のｋ個のネットワークサービスアクセスで指定されたネットワークアドレスをアクセスしたか否かを決定する。ネットワークユーザが先行のｋ個のアクセスで指定されたネットワークアドレスをアクセスしたことが決定された場合には、ステップ２３０において、現在のアクセスされたネットワークアドレスが、構成されるべきナビゲーションシーケンスへ追加される。先行のｋ個のアクセスでネットワークユーザが指定されたネットワークアドレスにアクセスしなかったことが決定された場合には、ステップ２４０において、使用監視モジュー

ルは、現在のアクセスされたネットワークアドレスが指定ネットワークアドレスベータベースへのエントリを検出しようとすることによって、指定されたネットワークアドレスであるか否かを決定する。使用監視モジュールは、現在のアクセスされたネットワークアドレスが指定されたネットワークアドレスであることが決定されると、ステップ２５０において、ユーザによってアクセスされた先行のｋ個のネットワークアドレスをナビゲーションシーケンスとして格納するためにコマンドが送られる。現在のアクセスされたネットワークアドレスが指定されたネットワークアドレスでないことが決定されると、ステップ２６０において、その特定のユーザのために、現在のアクセスされたネットワークアドレスがk_{max}個のネットワークアドレスのリストへ追加され、k_{max}個のリストが既にｋ個のネットワークアドレスを有している場合には、k_{max}個のリスト中の最も古いネットワークアドレスが破棄される。どのネットワークアドレスがネットワークユーザによってアクセスされるかが前もってわからないので、k_{max}個のリストが格納される。従って、k_{max}個のリストは、ネットワークユーザが指定されたネットワークアドレスにアクセスし、ナビゲーションシーケンスが要求されると、先行のネットワークアドレスのリスト作成のために提供される。

【００４０】

ユーザアクセス要求とネットワークサービス応答の監視動作に加えて、本発明の使用監視方法及び装置は、本発明の更に他の実施形態において、ストリーミングコンテントの使用を監視できる。ストリーミングコンテントは、ライブであってもよいし、又は記録されたものでもよい。そして、ストリーミングコンテントがネイティブストリーミングメディアサーバからゲートウエイデバイスを介してネットワークユーザへ送出されるので、捕獲動作がなされるであろう。ストリーミングコンテントは、典型的には、高ボリュームコンテントであるので、全てのストリーミングコンテントデータパケットに関連する情報を格納するのは不可能或いは現実的ではない。従って、全てのストリーミングコンテントパケットが使用監視モジュールで捕獲されるが、それらのパケットの有意な部分がフィルタ処理されてこの高トラフィックボリュームを補償する。ストリーミングコンテントパケットの定常的な監視動作によって、有意なフィルタ処理が可能となり、ストリーミングコネクションの間に転送されるデータの量、ストリーミングコネクションの存続時間等に関する情報を提供する。使用監視モジュールを実行するデバイス、典型的には、ゲートウエイデバイスに対する定常的な監視動作を発生するためには、ストリーミングコンテントの現在又は最新のステータスのトラッキングを維持するために或る量の状態をメモリに割当てることが必要である。更に、使用監視モジュール、或いはこれに代えてポスト処理アプリケーションは、ユーザが現在アクセスしているストリーミングコンテント，このストリーミングコンテントが来ているサイト，コネクションの間に転送されたデータ量，及びストリーミングコンテントパケットが特定のユーザ／ストリーミングコンテント対に対して最後に観察されたのは何時かをトラッキングする。ストリーミングコンテンツの場合には、コネクションの終了が明示されないために、使用監視モジュールはタイムアウトを実施してコンテントストリーミングが終了した時を決定する必要がある。これらのトラッキング機能が使用監視モジュールで発生され得るか、或いは、トラッキングパラメータを決定するために、フォーマット化されていないデータがストリーミングパケット毎にポスト処理アプリケーションへ送られ得る。

【００４１】

本発明の更に他の実施形態において、使用監視装置は、ターゲットサーベイをネットワークユーザに提供するために使用され得る。上述のように、挿入サーバは、使用監視データに基づいて、ターゲットサーベイをネットワークユーザに送るように実施できる。サーベイは、依頼していないネットワークユーザに送信されてもよく、そのネットワークユーザは、そのサーベイに参加することを選択できる。これに関して、ネットワークユーザは、ランダムに選択されかつポップアップスクリーンがそれらのユーザの通信デバイス上にランダムに選択された時間に現れる。例えば、発明者であるＳｈｏｒｔ氏らの名前で２０００年４月３日出願の「Ｉｎｆｏｒｍａｔｉｏｎ　Ａｎｄ　Ｃｏｎｔｒｏｌ　Ｃｏｎｓｏｌ

ｅ Ｆｏｒ Ｕｓｅ Ｗｉｔｈ Ａ Ｎｅｔｗｏｒｋ Ｇａｔｅｗａｙ Ｉｎｔｅｒｆａｃｅ（ネットワークゲートウエイインターフェースと共に使用される情報及び制御コンソール）」と題される、本発明の譲受人と同じ譲受人に譲渡された米国特許出願シリアル番号第０９／５４１，８７７号を参照のこと。この‘８７７号出願の内容は、あたかもここで十分に記述されているように、これを引用することによって本願明細書に組み込まれるものとする。

【００４２】

本発明の他の実施形態において、使用監視方法及び装置は、サーチエンジン等のような、ネットワークサービスアプリケーションへネットワークユーザが提出する照会も監視することができる。ネットワークユーザは、サーチエンジンのようなネットワークサービスアプリケーションへ提出する照会を監視することによって、ユーザの好みについての追加の知識を得ることができる。使用を監視する現在の方法は、リアルタイムで、ネットワークユーザの照会を監視する能力を備えていない。ネットワークユーザ照会ストリングのリアルタイム監視によって、ネットワーク広告主等のネットワーク受益者にネットワークユーザをプロファイルする能力を提供し、かつ、ユーザにはより多くのターゲット情報を提供する。例えば、ユーザがＦｏｒｄ（商標）ウエブサイト上でモデルＴａｕｒｕｓ（商標）をサーチすると、ネットワーク広告主は、この情報を使用して競合する製品の広告をユーザに送ることができる。

【００４３】

使用監視方法及び装置によって監視され得るユーザ入力の他の形態は、ネットワークサービス登録フォーム，アプリケーションフォーム等のユーザによってポストされるウエブフォームである。現在の方法は、ウエブ上でユーザによって提出されるフォームで情報を捕獲しない。

【００４４】

上述のように、本発明のネットワーク使用監視装置及び方法は、広範囲のネットワークユーザ関係情報を監視し格納する能力を備えている。この情報は、限定されるわけではないが、アクセスされたネットワークサービスのコンテント，ユーザ母集団の人口統計（すなわち、ユーザ母集団の年齢，性別，地理上の位置，サービスプラン等）及びネットワークがアクセスされる期間を含んでいる。これに関して、ネットワークサービスプロバイダ又は受益者は、あらゆる特定の時間に特定のネットワークサービスにアクセスするユーザのリアルタイムの統計的性格を決定できる。例えば、「３４歳から５５歳までの何人の女性が現在特定のウエブサイトにアクセス中であるか？」又は「特定のクラシックミュージック局を聴いている３５歳以下のユーザの割合はどうか？」次に、この情報は、ネットワーク受益者へ提供されることができ、この受益者は、この情報を売り込み効果的な方法でコアの聴取者に利益を提供できる。

【００４５】

主メモリ要求

以下の議論では、本発明に従って使用監視モジュールを動作するのに必要な主メモリの容量を仮に推定する。

【００４６】

アドレスの平均長がｌバイトであり、アクティブ顧客の数がｎであると仮定すると、記憶の容量は、

S_n（バイトで表した記憶容量）＝　$l \times 2k_{max} \times n$

として計算され、

最悪の場合の記憶量要求は、この特定のアクセスポイントでネットワークにアクセスするユーザの総数Ｎに依存する。

S_N（バイトで表した記憶容量）＝　$l \times 2k_{max} \times N$

【００４７】

ＩＳＰ（インターネットサービスプロバイダ）の検討結果として、いつでもユーザの１０％～２５％のみがアクティブであることが示される。その結果、典型的な記憶容量要求Ｓ

$_n$は、最悪の場合の記憶容量の要求量S_Nの約２５％に過ぎない。

【００４８】

幾つかのＵＲＬは、この長さの倍を越えて拡張（延出）するが、典型的なパケットの長さは、通常、１００バイト未満である。一般的には、より長いＵＲＬは、稀な照会から生じ、結果として、それほど頻繁には発生しない。このように、手近な目標として、ｌの平均値が１００バイトである。

【００４９】

ユーザセッションの典型的な長さは、ダイアルアップ顧客に対する５５分からＤＳＬ顧客に対する９５分まで変化する。そして、ユーザによってウエブページに費やされる平均時間は、約２分であるので、一回のネットワークセッションにおいてユーザによって訪問されるネットワークアドレスの数は、通常１００のオーダーである。これによって、ｋの値の上限を我々に与える。

【００５０】

このように、主データベースのＲＡＭの１２８ＭＢは、本発明に従って識別されたナビゲーションシーケンスを格納するのに専用のものであり、ｋの値が１００であり、ｌが１００バイトであると仮定すると、使用監視モジュールは、１２，８００名のユーザに対する最近傍（nearest neighbors）を監視できる。このように、本方法は、要求される状態の量、すなわち、維持される先行の及び後続のネットワークアドレスの数に関して良好にスケーリングし、主メモリ要求量を決定できる。

【００５１】

２次記憶容量要求

時間経過に従って、ユーザが、異なるナビゲーションシーケンスを介して指定ネットワークアドレスのより多くへ訪問するので、一般的に、主データベースに格納されるナビゲーションシーケンスの数が増加する。また、ナビゲーションシーケンス自体が長くなるに従って、ｋの値と共に、ナビゲーションシーケンスの数が増加する。ナビゲーションシーケンスについての価値のある情報を失うことなく、要求された記憶容量を減少する方法が二つある。

・シーケンスの時間経過；

タイムスタンプが各ナビゲーションシーケンスと共に格納される。このタイムスタンプは、そのシーケンスが訪問された最後の時間を示す。そのシーケンスが指定された期間内に訪問されなかった場合には、そのシーケンスがタイムアウトになり、削除される。

・稀なシーケンスの除去；

ジップの法則は、シーケンスの小部分のみがアクセスの大部分に対して責任を負うことを示している。このように、訪問回数が指定回数未満のナビゲーションシーケンスを除去することが可能である。

【００５２】

本発明の他の実施形態によれば、使用監視装置及び方法は、指定ネットワークアドレスの近傍を捕獲しかつ格納するために使用されることができる。この実施形態において、ネットワークアドレスがユーザによってアクセスされる順序には重要度がない。データベースに格納される情報のみが、指定ネットワークアドレスの指定数のページ（時間）内に発生するネットワークアドレスである。ｋとして定義された近傍におけるネットワークアドレスの数は、ユーザがネットワークアドレスにアクセスするに従って、通常、増加する。また、その数は、ｋの値と共に増加する。上記の定義された２次記憶容量要求量と同様に、近傍についての価値ある情報を失うことなく、要求された記憶容量を減少する方法が二つある。

・近傍（neighborhood）における時間経過；

タイムスタンプが近傍の一部であるエントリネットワークアドレスの各々と共に格納される。このタイプスタンプは、ネットワークアドレスが訪問された最後の時間を指示する。ネットワークサービスが指定された期間の間訪問されなかった場合、タイムアウトしかつ近傍から削除される。

・稀な近隣の除去；
ジップの法則は、近傍におけるネットワークアドレスの小部分がアクセスの大部分に対して責任を負う。従って、近傍から訪問回数が指定回数未満のネットワークアドレスを削除することが可能である。
【００５３】
上記方法としては、指定ネットワークアドレスのネットワークアドレス近傍を捕獲する方法を記述したが、指定ドメインのドメイン近傍を捕獲することも可能である。広告主は、使用監視モジュールが監視することを望むドメインを指定できる。次に、使用監視モジュールは、ユーザがアクセスした先行のｋ個のドメインのトラッキングをいつでも維持する。ユーザが指定ドメインをアクセスすると、使用監視モジュールは、ユーザによってアクセスされた先行のｋ個のドメイン及びユーザがアクセスする後続のｋ個のドメインを格納する。また、所定期間を経過したドメインの除去及びまれに訪問されたドメインを削除することによって要求される記憶容量を減少できる。
【００５４】
指定ネットワークアドレス及び一部が関連するネットワークアドレスの指定リストである、全体のナビゲーションシーケンスを捕獲することは、記憶容量と演算量が膨大過ぎるとなると考えられる。これに関連して、他の方法は、大きなタイムアウト期間Ｔ（これは、記憶容量要求と状態情報が合理的であり実施可能であることを保証するためである）内に指定ネットワークアドレスの近傍における関連するセットのネットワークアドレスをとトラッキングするために提供され、その関連するセットのネットワークアドレスは、典型的には、ゲートウエイ又はネットワークアドミニストレータによって定義される。ネットワーク広告主のシナリオでは、例えば、この関連するセットのネットワークアドレスは、指定ネットワークアドレスの競業者に属してもよい。ネットワーク広告主は、見込み顧客が、指定ネットワークアドレスの近傍（Ｆｏｒｄ（フォード社）ウエブサイト）をブラウジングしていると共に、指定のリストの関連するアドレス（Ｇｅｎｅｒａｌ　Ｍｏｔｏｒｓ（ＧＭ社）、Ｖｏｌｖｏ（ボルボ社）、ＢＭＷ（ビーエムダブリュ社）又はＭｅｒｃｅｄｅｓ（メルセデスベンツ社）ウエブサイト等のアドアレス）を訪問しているか否かを監視することを希望する場合がある。使用監視モジュールは、指定ネットワークアドレスと関連ネットワークアドレスを含む、ナビゲーションシーケンスをサーチする能力を提供し、かつ広告主に関連するサイトのネットワークアドレスを訪問する顧客の確率を提供する。
【００５５】
通信ネットワークのエッジでのその位置の結果、本発明に従う使用監視モジュールは、ネットワークサービスプロバイダ，ネットワークユーザ，及びネットワーク受益者にとって有用な標準セットのメトリックス（metrics）を収集するために、複数のユーザによって発行された要求と多数の異なるネットワークサービスによって提供された応答を監視できる。このデータは、非常に頑強（ロバスト）であり、かつ、ユーザ人口統計及びナビゲーションシーケンスと共に、ウエブ及びネイティブストリーミングコンテントを含むことができる。広範なネットワークサービスをアクセスしている複数のユーザから収集された頑強なセットのデータとインターネット上の他のエンティティに基づいて、本発明の使用監視方法及び装置は、大量の価値のあるデータをネットワークサービスプロバイダ，ネットワークユーザ，ネットワーク受益者等に提供できる。
【００５６】
前記の記述及びそれに関連する図面に示される教示の利益を有する当業者にとって、本発明の多くの変更や他の実施形態に思い至るであろう。従って、本発明は、ここで開示された特定の実施形態に制限されるべきではなく、変更や他の実施形態が添付の請求項の範囲内に含まれるとことが意図されている点に留意すべきである。ここで特定の用語が使用されているが、それらは総称的であり、記述的意味においてのみ使用されており、制限目的ではない。
【図面の簡単な説明】
【図１】　本発明の一実施形態による使用監視装置のブロック図である。

【図２】　本発明の他の実施形態による使用監視装置のブロック図である。
【図３】　本発明の一実施形態の使用監視方法及び装置によって実行される一般的動作を示すフローチャートである。
【図４】　本発明の他の実施形態による、使用監視方法及び装置によって実行されるナビゲーション順序付け動作を示すフローチャートである。
【図５】　本発明の使用監視方法及び装置の一実施形態によって利用されることができる関係データベースを示す図である。

【図１】

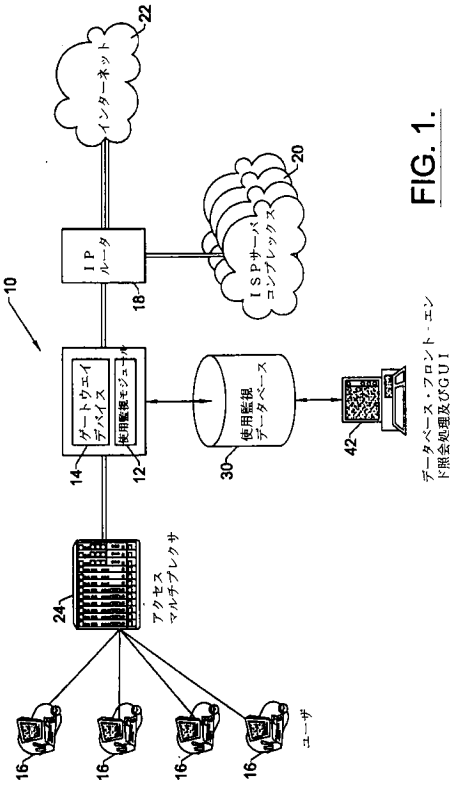

FIG. 1.

【図２】

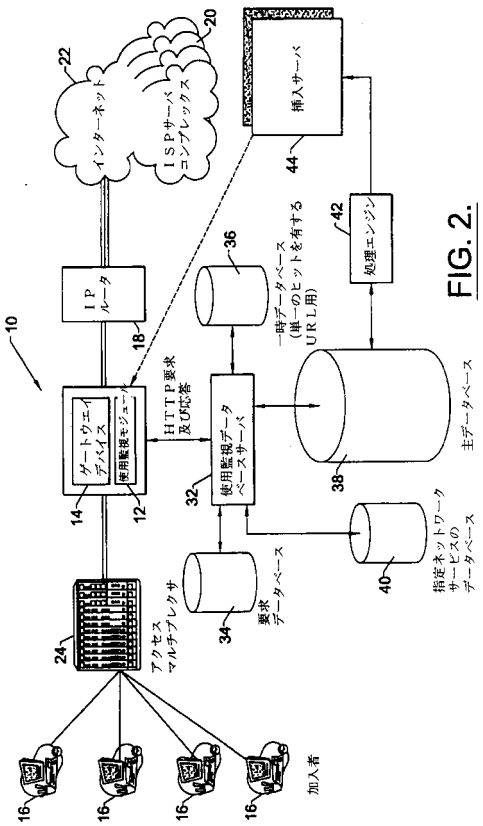

FIG. 2.

【図３】

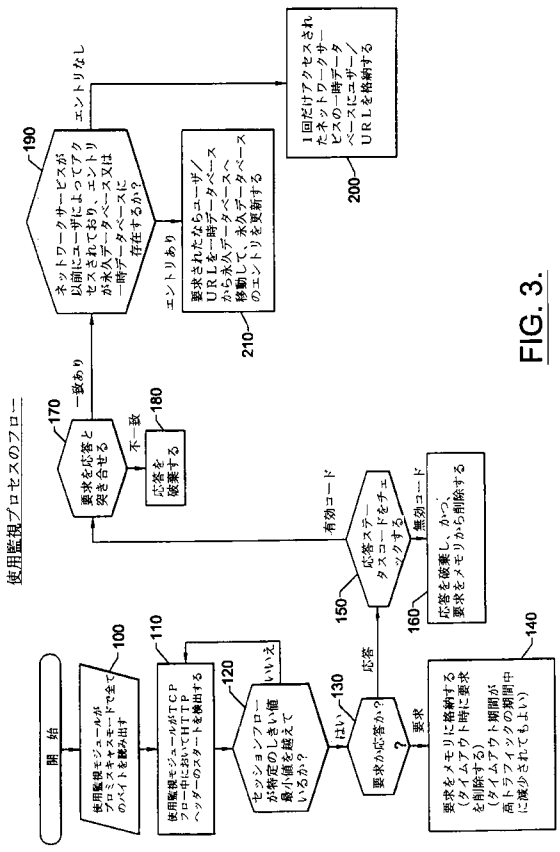

FIG. 3.

【図４】

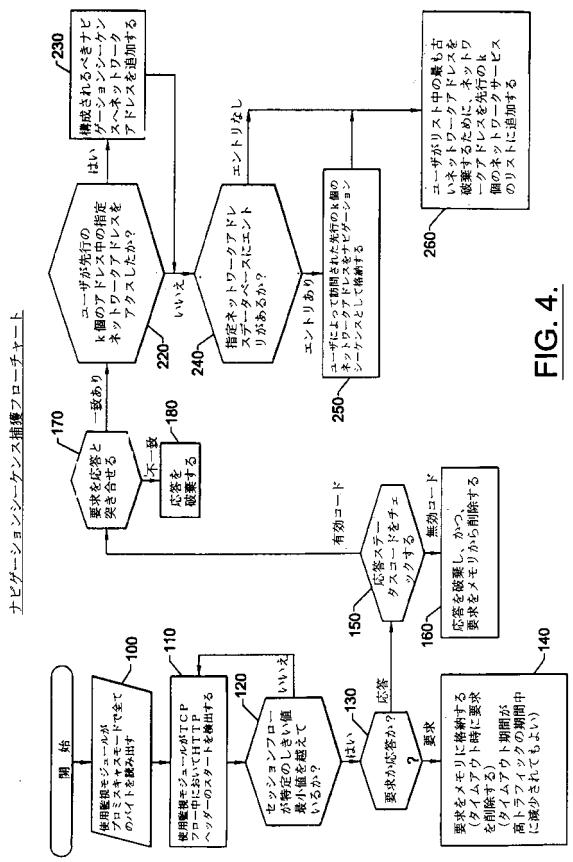

FIG. 4.

【図５】

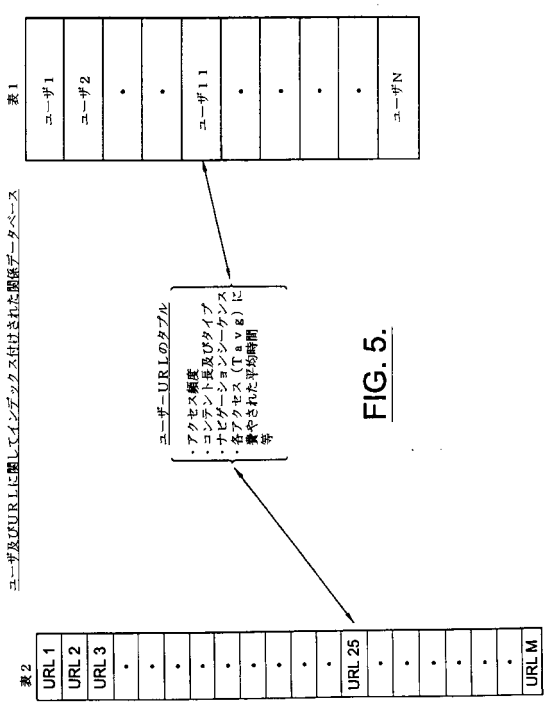

FIG. 5.

フロントページの続き

(72)発明者　ショート，ジョエル・イー
アメリカ合衆国カリフォルニア州９００４９，ロス・アンジェルス，サウス・バーリントン・アヴェニュー　７２５，＃３１０
(72)発明者　ガルグ，アヌラグ・ケイ
アメリカ合衆国カリフォルニア州９００４９，ロス・アンジェルス，ダーリントン・アヴェニュー　１１７２５，アパートメント　１
(72)発明者　バガヴァット，ヴィジャイ・クリシュナ
アメリカ合衆国カリフォルニア州９４５８３，サン・ラモン，プロモントリー・テラス　１６３６

合議体
審判長　山本　春樹
審判官　高野　洋
審判官　萩原　義則

(56)参考文献　国際公開第９８／１１７０２（WO，A1）
米国特許第６０２６４４０（US，A）
横井忠寛，間瀬憲一，インターネットの品質・トラヒック管理［ＩＩＩ］，電子情報通信学会誌，２０００年　1月２５日，Ｖｏｌ．８３，　Ｎｏ．１，ｐｐ．５７－６３
加藤　佐一、「Ｗｉｎｄｏｗｓ　ＮＴのネットワーク管理機能」コンピュータ＆ネットワークＬＡＮ、第１５巻、第８号、１９９７年８月１日、ｐｐ．２８－３３の第４図
久保田　浩司　他、「解剖イントラネット－２３　伝送路やネットワーク機器の性能管理」、日経コミュニケーション、第２６５号、１９９８年3月2日、ｐｐ．２２２－２２３の第１図

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L12/56