(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3584838号
(P3584838)
(45)発行日　平成16年11月4日(2004.11.4)　(24)登録日　平成16年8月13日(2004.8.13)

(51)Int.Cl.[7]　F I
H04L 12/14　H04L 12/14
H04L 12/24　H04L 12/24

請求項の数 12　(全 12 頁)

(21)出願番号　特願2000-50476(P2000-50476)
(22)出願日　平成12年2月22日(2000.2.22)
(65)公開番号　特開2001-237894(P2001-237894A)
(43)公開日　平成13年8月31日(2001.8.31)
審査請求日　平成13年1月16日(2001.1.16)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100084250
弁理士　丸山　隆夫
(72)発明者　菊地　庸之
東京都港区芝五丁目７番１号　日本電気株式会社内

審査官　小林　紀和

(56)参考文献　特開２００１－０４４９９２（ＪＰ，Ａ）
特開２０００－０６９０１７（ＪＰ，Ａ）

最終頁に続く

(54)【発明の名称】パケット監視システム、パケット監視方法及びそのプログラムを記録した記録媒体

(57)【特許請求の範囲】
【請求項１】
アプリケーションサーバと該アプリケーションサーバを利用するサービス利用者とを接続する通信路上で送受信されるパケットを監視するパケット監視システムであって、
前記サービス利用者を認証する認証サーバ装置は、
前記サービス利用者の識別番号、前記サービス利用者を認証するパスワード、監視するパケットの対象を指定する監視パラメータ、前記パケットの監視方法を指定する閾値パラメータを含む利用者管理テーブルを記憶している利用者管理情報記憶手段と、
　前記サービス利用者が自装置にログイン／アウトしたタイミングで、前記パケット監視装置に前記パケットの監視の開始／終了を要求する監視要求手段と、
　を有し、
前記認証サーバ装置からの依頼により、前記通信路上で送受信されるパケットを監視するパケット監視装置は、
前記監視要求手段から監視要求があったとき、前記アプリケーションサーバ及び前記サービス利用者のいずれかから送信されたパケットの到着時刻を記憶する到着時刻記憶手段と、
　前記監視要求手段から監視要求があったとき、前記到着時刻記憶手段の記憶している到着時間を基に、前記監視パラメータと一致するパケットの到着時刻を監視し、前記到着間隔に任意の関係が存在するか否かを分析する関連性分析手段と、
　該関連性分析手段による分析の結果、前記任意の関係が存在するとき、前記サービス利

用者に通知警告する通知警告手段と、
を有することを特徴とするパケット監視システム。
【請求項２】
前記認証サーバ装置は、
前記サービス利用者の指示により前記利用者管理テーブルの前記監視パラメータ及び前記閾値パラメータを更新する利用者管理テーブル更新手段をさらに有することを特徴とする請求項１記載のパケット監視システム。
【請求項３】
前記パケット監視装置は、
前記監視要求手段から転送された前記監視パラメータを記憶する監視パラメータ記憶手段と、
前記監視要求手段から転送された前記閾値パラメータを記憶する閾値パラメータ記憶手段と、
前記監視要求手段からの監視要求の開始／終了のタイミングで、前記監視パラメータ記憶手段及び閾値パラメータ記憶手段を更新するパラメータ更新手段と、
を有することを特徴とする請求項１または２記載のパケット監視システム。
【請求項４】
前記関連性分析手段は、
前記閾値パラメータ記憶手段に閾値パラメータが記憶されているとき、前記到着間隔に任意の関係が存在し、且つ、前記閾値パラメータを超えたか否かを分析し、
前記通知警告手段は、
前記関連性分析手段による分析の結果、前記任意の関係が存在し、且つ、前記閾値パラメータを超えたとき、前記サービス利用者に通知警告することを特徴とする請求項３記載のパケット監視システム。
【請求項５】
アプリケーションサーバと該アプリケーションサーバを利用するサービス利用者とを接続する通信路上で送受信されるパケットを監視するパケット監視方法であって、
前記サービス利用者がログインしたとき、監視するパケットの対象を指定する監視パラメータを含む利用者管理テーブルから、前記監視パラメータを取得するパラメータ取得工程と、
該パラメータ取得工程により取得した監視パラメータと一致するパケットの到着時刻を監視し、前記パケットの到着間隔に任意の関係が存在するか否かを分析する関連性分析工程と、
該関連性分析工程による分析の結果、前記任意の関係が存在するとき、前記サービス利用者に通知警告する通知警告工程と、
を有することを特徴とするパケット監視方法。
【請求項６】
前記サービス利用者がログアウトしたとき、前記パラメータ分析工程による分析を終了することを特徴とする請求項５記載のパケット監視方法。
【請求項７】
前記利用者管理テーブルは、
前記サービス利用者の識別番号、前記サービス利用者を認証するパスワード、前記パケットの監視方法を指定する閾値パラメータをさらに含み、
前記パラメータ取得工程は、
前記サービス利用者が入力した前記識別番号及び前記パスワードを基に、前記利用者管理テーブルを検索し、
前記利用者管理テーブルに前記監視パラメータが登録されているとき、前記監視パラメータを取得し、
前記利用者管理テーブルに前記閾値パラメータが登録されているとき、前記閾値パラメータを取得することを特徴とする請求項５または６記載のパケット監視方法。

【請求項８】
前記関連性分析工程は、
前記パラメータ取得工程により前記閾値パラメータを取得したとき、前記パケットの到着間隔に前記任意の関係が存在し、且つ、前記閾値パラメータを越えたか否かを分析し、
前記通知警告工程は、
前記関連性分析工程による分析の結果、前記任意の関係が存在し、且つ、前記閾値パラメータを超えたとき、前記サービス利用者に通知警告することを特徴とする請求項７記載のパケット監視方法。
【請求項９】
アプリケーションサーバと該アプリケーションサーバを利用するサービス利用者とを接続する通信路上で送受信されるパケットを監視するプログラムを記録した記録媒体であって、
前記サービス利用者がログインしたとき、監視するパケットの対象を指定する監視パラメータを含む利用者管理テーブルから、前記監視パラメータを取得するパラメータ取得処理と、
該パラメータ取得処理により取得した監視パラメータと一致するパケットの到着時刻を監視し、前記パケットの到着間隔に任意の関係が存在するか否かを分析する関連性分析処理と、
該関連性分析処理による分析の結果、前記任意の関係が存在するとき、前記サービス利用者に通知警告する通知警告処理と、
をコンピュータに実行させることを特徴とするプログラムを記録した記録媒体。
【請求項１０】
前記サービス利用者がログアウトしたとき、前記パラメータ分析処理による分析を終了することを特徴とする請求項９記載のプログラムを記録した記録媒体。
【請求項１１】
前記利用者管理テーブルは、
前記サービス利用者の識別番号、前記サービス利用者を認証するパスワード、前記パケットの監視方法を指定する閾値パラメータをさらに含み、
前記パラメータ取得処理は、
前記サービス利用者が入力した前記識別番号及び前記パスワードを基に、前記利用者管理テーブルを検索し、
前記利用者管理テーブルに前記監視パラメータが登録されているとき、前記監視パラメータを取得し、
前記利用者管理テーブルに前記閾値パラメータが登録されているとき、前記閾値パラメータを取得することを特徴とする請求項９または１０記載のプログラムを記録した記録媒体。
【請求項１２】
前記関連性分析処理は、
前記パラメータ取得工程により前記閾値パラメータを取得したとき、前記パケットの到着間隔に前記任意の関係が存在し、且つ、前記閾値パラメータを越えたか否かを分析し、
前記通知警告処理は、
前記関連性分析処理による分析の結果、前記任意の関係が存在し、且つ、前記閾値パラメータを超えたとき、前記サービス利用者に通知警告することを特徴とする請求項１１記載のプログラムを記録した記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、従量課金に伴う情報量の機械的なカウントにより生じる不相当なサービス料金、または通信料金の請求を防止するパケット監視システム、パケット監視方法及びそのプログラムを記録した記録媒体に関する。

【０００２】
【従来の技術】
近年、電子メールやＷｅｂなどのサービスの利用料金は、サービスを提供しているサービスプロバイダへの接続料金や通信事業者に支払う通信料金などで決められている。現在の料金設定はサービスプロバイダ、通信事業者ともに、基本料金に加え、通信時間や距離に依存して行われているが、一部、データ通信ではデータ量に応じた従量課金も採用され始め、今後拡大する傾向にある。
【０００３】
このような状況下、インタネット技術の普及と共に、インタネット上で利用できるサービスが多様化している。利用者は、ＡＰサーバ（アプリケーションサーバ）から必要な通信ソフトウェアをダウンロードしてサービスを受ける機会が増加しており、サービスの中には独自の通信プロトコルを用い、通信ソフトウェア間で利用者の意図しない制御情報をやりとりするものが現われてきた。例えば、チャットサーバによる定期的な端末の起動確認などである。
【０００４】
【発明が解決しようとする課題】
今後拡大する従量課金においては、通信路上で流れるデータ量に応じて課金されるので、利用者の意図しない制御情報にも関わらず課金されてしまうという問題点がある。それは、情報量の機械的なカウントによるものであり、本来支払うべき料金と実際に請求される料金との不一致を大きくし、利用者はサービスプロバイダに対する不信感を募らせ、ひいてはサービスプロバイダとの契約を解除することにつながる可能性もある。
【０００５】
本発明はかかる問題点に鑑みなされたものであり、利用者の意図しない制御情報にも関わらず課金されてしまうという事態を防止し、利用者が受領したサービスに見合った適正な課金を行う機能を有するパケット監視システム、パケット監視方法及びそのプログラムを記録した記録媒体を提供することを目的とする。
【０００６】
【課題を解決するための手段】
かかる目的を達成するために、請求項１記載の発明は、アプリケーションサーバと該アプリケーションサーバを利用するサービス利用者とを接続する通信路上で送受信されるパケットを監視するパケット監視システムであって、サービス利用者を認証する認証サーバ装置は、サービス利用者の識別番号、サービス利用者を認証するパスワード、監視するパケットの対象を指定する監視パラメータ、パケットの監視方法を指定する閾値パラメータを含む利用者管理テーブルを記憶している利用者管理情報記憶手段と、サービス利用者が自装置にログイン／アウトしたタイミングで、パケット監視装置にパケットの監視の開始／終了を要求する監視要求手段と、を有し、認証サーバ装置からの依頼により、通信路上で送受信されるパケットを監視するパケット監視装置は、監視要求手段から監視要求があったとき、アプリケーションサーバ及びサービス利用者のいずれかから送信されたパケットの到着時刻を記憶する到着時刻記憶手段と、監視要求手段から監視要求があったとき、到着時刻記憶手段の記憶している到着時間を基に、監視パラメータと一致するパケットの到着時刻を監視し、到着間隔に任意の関係が存在するか否かを分析する関連性分析手段と、該関連性分析手段による分析の結果、任意の関係が存在するとき、サービス利用者に通知警告する通知警告手段と、を有することを特徴とする。
【０００７】
請求項２記載の発明は、請求項１記載の発明において、認証サーバ装置は、サービス利用者の指示により利用者管理テーブルの監視パラメータ及び閾値パラメータを更新する利用者管理テーブル更新手段をさらに有することを特徴とする。
【０００８】
請求項３記載の発明は、請求項１または２記載の発明において、パケット監視装置は、監視要求手段から転送された監視パラメータを記憶する監視パラメータ記憶手段と、監視要

求手段から転送された閾値パラメータを記憶する閾値パラメータ記憶手段と、監視要求手段からの監視要求の開始／終了のタイミングで、監視パラメータ記憶手段及び閾値パラメータ記憶手段を更新するパラメータ更新手段と、を有することを特徴とする。

【０００９】

請求項４記載の発明は、請求項３記載の発明において、関連性分析手段は、閾値パラメータ記憶手段に閾値パラメータが記憶されているとき、到着間隔に任意の関係が存在し、且つ、閾値パラメータを超えたか否かを分析し、通知警告手段は、関連性分析手段による分析の結果、任意の関係が存在し、且つ、閾値パラメータを超えたとき、サービス利用者に通知警告することを特徴とする。

【００１０】

請求項５記載の発明は、アプリケーションサーバと該アプリケーションサーバを利用するサービス利用者とを接続する通信路上で送受信されるパケットを監視するパケット監視方法であって、サービス利用者がログインしたとき、監視するパケットの対象を指定する監視パラメータを含む利用者管理テーブルから、監視パラメータを取得するパラメータ取得工程と、該パラメータ取得工程により取得した監視パラメータと一致するパケットの到着時刻を監視し、パケットの到着間隔に任意の関係が存在するか否かを分析する関連性分析工程と、該関連性分析工程による分析の結果、任意の関係が存在するとき、サービス利用者に通知警告する通知警告工程と、を有することを特徴とする。

【００１１】

請求項６記載の発明は、請求項５記載の発明において、サービス利用者がログアウトしたとき、パラメータ分析工程による分析を終了することを特徴とする。

【００１２】

請求項７記載の発明は、請求項５または６記載の発明において、利用者管理テーブルは、サービス利用者の識別番号、サービス利用者を認証するパスワード、パケットの監視方法を指定する閾値パラメータをさらに含み、パラメータ取得工程は、サービス利用者が入力した識別番号及びパスワードを基に、利用者管理テーブルを検索し、利用者管理テーブルに監視パラメータが登録されているとき、監視パラメータを取得し、利用者管理テーブルに閾値パラメータが登録されているとき、閾値パラメータを取得することを特徴とする。

【００１３】

請求項８記載の発明は、請求項７記載の発明において、関連性分析工程は、パラメータ取得工程により閾値パラメータを取得したとき、パケットの到着間隔に任意の関係が存在し、且つ、閾値パラメータを越えたか否かを分析し、通知警告工程は、関連性分析工程による分析の結果、任意の関係が存在し、且つ、閾値パラメータを超えたとき、サービス利用者に通知警告することを特徴とする。

【００１４】

請求項９記載の発明は、アプリケーションサーバと該アプリケーションサーバを利用するサービス利用者とを接続する通信路上で送受信されるパケットを監視するプログラムを記録した記録媒体であって、サービス利用者がログインしたとき、監視するパケットの対象を指定する監視パラメータを含む利用者管理テーブルから、監視パラメータを取得するパラメータ取得処理と、該パラメータ取得処理により取得した監視パラメータと一致するパケットの到着時刻を監視し、パケットの到着間隔に任意の関係が存在するか否かを分析する関連性分析処理と、該関連性分析処理による分析の結果、任意の関係が存在するとき、サービス利用者に通知警告する通知警告処理と、をコンピュータに実行させることを特徴とする。

【００１５】

請求項１０記載の発明は、請求項９記載の発明において、サービス利用者がログアウトしたとき、パラメータ分析処理による分析を終了することを特徴とする。

【００１６】

請求項１１記載の発明は、請求項９または１０記載の発明において、利用者管理テーブルは、サービス利用者の識別番号、サービス利用者を認証するパスワード、パケットの監視

方法を指定する閾値パラメータをさらに含み、パラメータ取得処理は、サービス利用者が入力した識別番号及びパスワードを基に、利用者管理テーブルを検索し、利用者管理テーブルに監視パラメータが登録されているとき、監視パラメータを取得し、利用者管理テーブルに閾値パラメータが登録されているとき、閾値パラメータを取得することを特徴とする。

【００１７】

請求項１２記載の発明は、請求項１１記載の発明において、関連性分析処理は、パラメータ取得工程により閾値パラメータを取得したとき、パケットの到着間隔に任意の関係が存在し、且つ、閾値パラメータを越えたか否かを分析し、通知警告処理は、関連性分析処理による分析の結果、任意の関係が存在し、且つ、閾値パラメータを超えたとき、サービス利用者に通知警告することを特徴とする。

【００１８】

【発明の実施の形態】

以下、本発明の実施の形態を添付図面を参照しながら詳細に説明する。

【００１９】

図１は、本発明のパケット監視システムの基本構成を示すブロック図である。図１において、サービス利用者は、サービスプロバイダ４との間でサービス料金や監視方法について契約を交わし、データ情報端末１を利用して、有線／無線通信網２、通信路３、サービスプロバイダ４、インタネット７を介して、ＡＰサーバ８からサービスやコンテンツ情報を授受する。ここで、パケットとは、ユーザデータと、ヘッダ（送受信先アドレスやサービス識別子、チェックサム、ユーザデータやヘッダのサイズ等の制御情報）とから構成されるインタネット転送プロトコルの基本転送単位ブロックを指す。

【００２０】

サービスプロバイダ４は、サービス利用者を認証する認証サーバ５、通信路３上で送受信されるパケットを監視するパケット監視装置６を有する。サービスプロバイダ４には、有線や無線による通信路を提供する通信事業者も含まれる。認証サーバ５は、利用者管理テーブルを格納している利用者管理メモリ９、利用者からの指示により利用者管理メモリ９の内容を更新する管理メモリ更新手段１０及びサービス利用者が認証サーバ５にログイン／アウトしたタイミングでパケット監視装置６に対して、監視の開始／終了を要求する監視要求手段１１を有する。

【００２１】

管理メモリ更新手段１０は、サービスプロバイダ４が契約時に提示した監視パラメータ、閾値パラメータを基に利用者管理メモリ９の内容を更新する。あるいは、サービスプロバイダ４が自身で提供しているWorld-Wide-Webのホームページ上において、サービス利用者が入力した監視パラメータ、閾値パラメータを基に利用者管理メモリ９の内容を更新する。あるいは、サービスプロバイダ４が提供するデータ情報端末１上で動作するパラメータ設定プログラム上において、サービス利用者が入力した監視パラメータ、閾値パラメータを基に利用者管理メモリ９の内容を更新する。

【００２２】

パケット監視装置６は、監視パラメータを格納しておく監視パラメータメモリ１２、閾値パラメータを格納しておく閾値パラメータメモリ１３、データ情報端末１もしくはＡＰサーバ８から送信されたパケットの到着時刻を格納しておく到着時刻メモリ１４、認証サーバ５から監視要求の開始／終了を受けたタイミングでパラメータメモリ１２、１３を更新するパラメータ更新手段１５、到着間隔の関連性を分析する関連性分析手段１６及び利用者に通知／警告を行う通知／警告手段１７を有する。

【００２３】

通知／警告手段１７は、サービスプロバイダ４が書面や掲示板にて利用者に通知／警告を行う。あるいは、サービスプロバイダ４が提供するサービスが使用している通信プロトコルに通知／警告を添付して利用者に通知／警告を行う。あるいは、サービスプロバイダ４がデータ情報端末１上で動作可能な通知／警告プログラムを送り付けることにより利用者

に通知／警告を行う。

【００２４】

監視パラメータは、送受信先アドレスと、サービス識別子と、ユーザデータ内の任意データ列と、チェックサムのいずれか、あるいはその組み合わせとする。送受信先アドレスとは、パケットを届けるための宛て先や送り元を示す制御情報である。サービス識別子とは、ＡＰサーバ８が利用者に提供するサービス（例えば、電子メールなど）を識別するための制御情報である。チェックサムとは、ユーザデータやヘッダが転送の際に壊れていないかどうかをチェックするための制御情報であり、ユーザデータやヘッダが等しい場合、チェックサムの情報も等しいものとする。

【００２５】

監視する対象とその組み合わせ（監視パラメータ）の一例を図２に示す。図２に示す監視パラメータは、送受信先アドレスとサービス識別子との組、送受信先アドレスとユーザデータ内の任意位置から始まる任意サイズのデータ列（以下、任意データ列とする。）との組、送受信先アドレスとサービス識別子と任意データ列との組、チェックサムのいずれかからなる。監視パラメータＡは、例えば、データ情報端末１から電子メールサービスを提供するＡＰサーバ８へ定期的に受信メール確認パケットが流れているか否か、チャットサービスを提供するＡＰサーバ８からデータ情報端末１へ定期的に端末の起動確認パケットが流れているか否かを監視するためのパラメータとなりうる。

【００２６】

閾値パラメータは、監視パラメータが一致してからの継続時間、連続して一致した回数、一致してから送受信されたユーザデータあるいはヘッダサイズ、一致してからの利用料金、通信路３上のトラフィック量のいずれか、あるいはその組み合わせとする。閾値パラメータの一例を図３に示す。図３に示す閾値パラメータは、監視パラメータが一致してからの継続時間（閾値Ａ）、連続して一致した回数（閾値Ｂ）、一致してから送受信されたユーザデータヘッダあるいはヘッダサイズ（閾値Ｃ）、一致してからの利用料金（閾値Ｄ）のいずれかからなる。

【００２７】

利用者管理メモリ９に記憶されている利用者管理テーブルの一例を図４に示す。利用者管理テーブルは、契約を交わした利用者の識別番号、利用者を認証するためのパスワード、監視パラメータ、閾値パラメータ及びパケット監視中か否かを示すフラグから構成される。

【００２８】

次に、本発明のパケット監視システムの動作について説明する。サービス利用者が、サービスプロバイダ４との間でサービス料金や監視方法について契約を交わし、データ情報端末１を利用し、有線／無線通信網２、通信路３、サービスプロバイダ４、インタネット７を介して、ＡＰサーバ８からサービスやコンテンツ情報を授受し、サービスプロバイダ４が、サービス利用者を認証する認証サーバ５、通信路３上で送受信されるパケットを監視するパケット監視装置６を有するシステム上で、サービス利用者が認証サーバにログイン／アウトしたタイミングで、パケット監視装置６の監視パラメータメモリ１２及び閾値パラメータメモリ１３の内容を通信／更新する動作を図５に示すフローチャートを用いて説明する。

【００２９】

図５において、監視要求手段１１は、サービス利用者が認証サーバ５にログインしたタイミングで、利用者管理メモリ９からログインした利用者を検索する（ステップＳ１）。監視要求手段１１は、サービス利用者に指示された監視パラメータが存在するか否かを確認する（ステップＳ２）。当該監視パラメータが存在する場合は（ステップＳ２／ＹＥＳ）、利用者管理メモリ９に保持されている監視パラメータと閾値パラメータとを読み込む（ステップＳ４）。読み込んだ２つのパラメータを引数として、パケットの監視開始をパラメータ更新手段１５に要求する（ステップＳ５）。ステップＳ２において、サービス利用者に指示された監視パラメータが存在しない場合は（ステップＳ３／ＮＯ）、パケットの

監視は行わない（ステップＳ３）。

【００３０】

パラメータ更新手段１５は、渡された２つのパラメータを各々、監視パラメータメモリ１２、閾値パラメータメモリ１３に格納する（ステップＳ６）。パラメータ更新手段１５は、格納した旨を監視要求手段１１に通知する（ステップＳ７）。

【００３１】

監視要求手段１１は、パラメータ更新手段１５から通知を受けると利用者管理メモリ９のログインした利用者に対応するフラグをセットする（ステップＳ８）。パラメータ更新手段１５は、関連性分析手段１６に監視パラメータで示されたパケットの到着間隔の関連性を分析するよう要求する（ステップＳ９）。

【００３２】

次に、監視要求手段１１は、サービス利用者が認証サーバ５からログアウトしたタイミングで、利用者管理メモリ９からログアウトした利用者を検索する（ステップＳ１０）。当該利用者に対応するフラグがセットされているか否かを確認する（ステップＳ１１）。フラグがセットされている場合は（ステップＳ１１／ＹＥＳ）、監視要求手段１１は、パラメータ更新手段１５に監視パラメータ及び閾値パラメータを引数としてパケットの監視終了を要求する（ステップＳ１３）。ステップＳ１１において、フラグがセットされていない場合は（ステップＳ１１／ＮＯ）、何も処理しない（ステップＳ１２）。

【００３３】

パケットの監視終了の要求を受けたパラメータ更新手段１５は、関連性分析手段１６に監視パラメータで示されたパケットの到着間隔の関連性の分析を終了するよう要求する（ステップＳ１４）。パラメータ更新手段１５は、監視パラメータメモリ１２、閾値パラメータメモリ１３からパラメータを消去する（ステップＳ１５）。パラメータ更新手段１５は、当該パラメータを消去した旨を監視要求手段１１に通知する（ステップＳ１６）。当該通知を受けた監視要求手段１１は、利用者管理メモリ９のログアウトした利用者に対応するフラグをクリアする（ステップＳ１７）。

【００３４】

次に、パケットの到着間隔の関連性を分析し、パケット送受信による問題があると判断した場合、通知／警告手段１７に通知する動作を図６に示すフローチャートを用いて説明する。到着時刻メモリ１４には、データ通信端末１、またはＡＰサーバ８からパケットが到着したタイミングで、パケットが到着した時刻、パケット送信元のアドレス、パケット受信先のアドレス、任意データ列、チェックサム、ユーザデータサイズ、ヘッダデータサイズが随時書き込まれるものとする。

【００３５】

図６において、関連性分析手段１６は、パラメータ更新手段１５から関連性分析開始要求を受け取る（ステップＳ９）。関連性分析手段１６は、当該関連性分析開始要求を受け取るとカウンタをクリアする（ステップＳ２１）。関連性分析手段１６は、監視パラメータメモリ１２を参照して監視パラメータの有無を確認する（ステップＳ２２）。監視パラメータが存在しない場合は（ステップＳ２２／ＮＯ）、関連性の分析を終了する（ステップＳ２３）。監視パラメータが存在する場合は（ステップＳ２２／ＹＥＳ）、関連性分析手段１６は、閾値パラメータメモリ１３を参照して閾値パラメータの有無を確認する（ステップＳ２４）。

【００３６】

閾値パラメータが存在する場合は（ステップＳ２４／ＹＥＳ）、関連性分析手段１６は、閾値確認フラグをセットする（ステップＳ２５）。フラグをセットしたら到着時刻メモリ１４を参照して監視パラメータに該当するパケットの有無を確認する（ステップＳ２６）。ステップＳ２４に戻り、閾値パラメータが存在しない場合は（ステップＳ２４／ＮＯ）、到着時刻メモリ１４を参照して監視パラメータに該当するパケットの有無を確認する（ステップＳ２６）。

【００３７】

パケットが存在しない場合は（ステップＳ２６／ＮＯ）、ステップＳ２２に戻る。パケットが存在する場合は（ステップＳ２６／ＹＥＳ）、関連性分析手段１６は、カウンタをインクリメントする（ステップＳ２７）。関連性分析手段１６は、カウンタが２以上か否かを確認する（ステップＳ２８）。

【００３８】

カウンタが２未満の場合は（ステップＳ２８／ＮＯ）、ステップＳ２２に戻る。カウンタが２以上の場合は（ステップＳ２８／ＹＥＳ）、関連性分析手段１６は、該当するパケットの到着時間間隔に関連性があるか否かを分析する（ステップＳ２９）。

【００３９】

ステップＳ２９において、関連性がない場合は（ステップＳ２９／ＮＯ）、ステップＳ２２に戻る。関連性がある場合は（ステップＳ２９／ＹＥＳ）、関連性分析手段１６は、閾値確認フラグがセットされているか否かを確認する（ステップＳ３０）。該当するパケットの到着時間間隔の関連性は、Ｘ秒間隔で到着している。あるいは、Ｘ秒とＹ秒間隔が交互に繰り返されている。

【００４０】

ステップＳ３０において、閾値確認フラグがセットされていない場合は（ステップＳ３０／ＮＯ）、関連性分析手段１６は、通信路３上に利用者が意図しないパケット、または利用者が故意に送信したパケットが流れているものと判断し、通知／警告手段１７に通知する（ステップＳ３１）。通知後、ステップＳ２１に戻る。ステップＳ３０において、閾値確認フラグがセットされている場合は（ステップＳ３０／ＹＥＳ）、閾値を超えたか否かを確認する（ステップＳ３２）。

【００４１】

閾値を越えていない場合は（ステップＳ３２／ＮＯ）、ステップＳ２２に戻る。閾値を越えた場合は（ステップＳ３２／ＹＥＳ）、関連性分析手段１６は、通信路３上に利用者が意図しないパケット、または利用者が故意に送信したパケットが流れているものと判断し、通知／警告手段１７に通知する（ステップＳ３３）。通知後、ステップＳ２１に戻る。

【００４２】

【発明の効果】

以上の説明から明らかなように、本発明によれば、従量課金に伴う情報量の機械的なカウントにより生じる不相当なサービス料金、または通信料金の請求を防止することができる。

【００４３】

また、サービス利用者が主に利用するサービスを考慮してパラメータを設定し、通知／警告を受けるべきパケットの種類を特定できることにより、パケット監視装置における関連性分析の処理効率を向上させることができる。

【図面の簡単な説明】

【図１】本発明の実施の形態におけるパケット監視システムの構成を示すブロック図である。

【図２】監視パラメータの一例を示した図である。

【図３】閾値パラメータの一例を示した図である。

【図４】利用者管理テーブルの一例を示した図である。

【図５】本発明の実施の形態における監視要求手段１１、パラメータ更新手段１５及び関連性分析手段１６の動作を説明するためのフローチャートである。

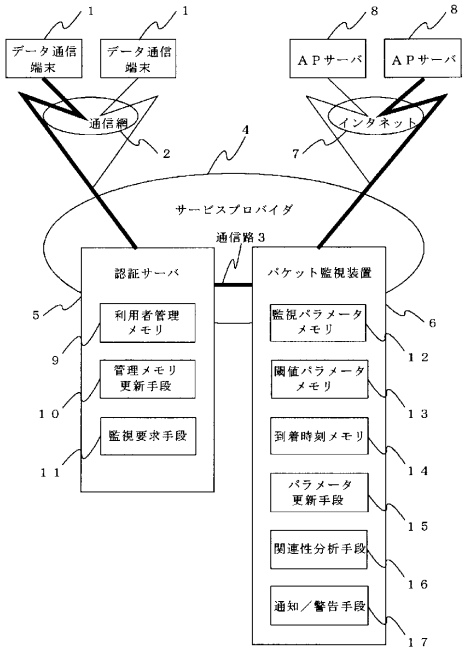
【図６】本発明の実施の形態におけるパラメータ更新手段１５、関連性分析手段１６及び通知／警告手段１７の動作を説明するためのフローチャートである。

【符号の説明】

１　データ通信端末
２　通信網
３　通信路
４　サービスプロバイダ

５　認証サーバ
６　パケット監視装置
７　インタネット
８　ＡＰサーバ
９　利用者管理メモリ
１０　管理メモリ更新手段
１１　監視要求手段
１２　監視パラメータメモリ
１３　閾値パラメータメモリ
１４　到着時刻メモリ
１５　パラメータ更新手段
１６　関連性分析手段
１７　通知／警告手段

【図１】

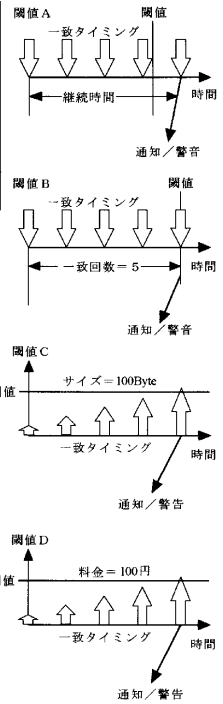


【図２】

監視パラメータ / 監視対象	パラメータA	パラメータB	パラメータC	パラメータD
送受信先アドレス	●	●	●	
サービス識別子	●		●	
任意データ列		●	●	
チェックサム				●

【図３】

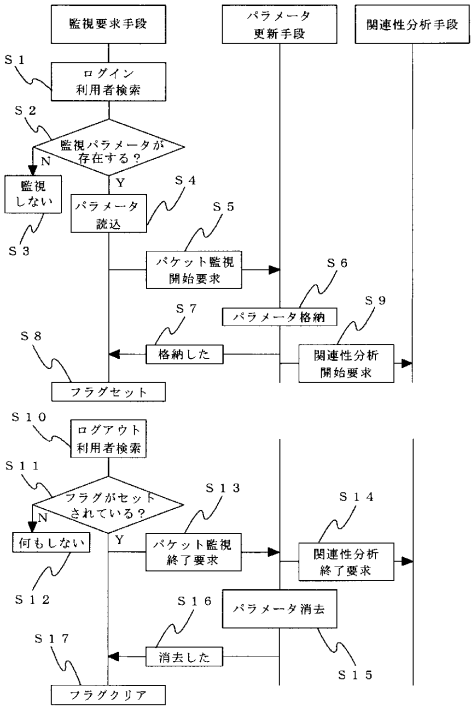
閾値パラメータ	説明
閾値A	監視パラメータが一致してからの継続時間
閾値B	連続して一致した時間
閾値C	一致してからの送受信された ユーザデータ、ヘッダサイズ
閾値D	一致してからの利用料金



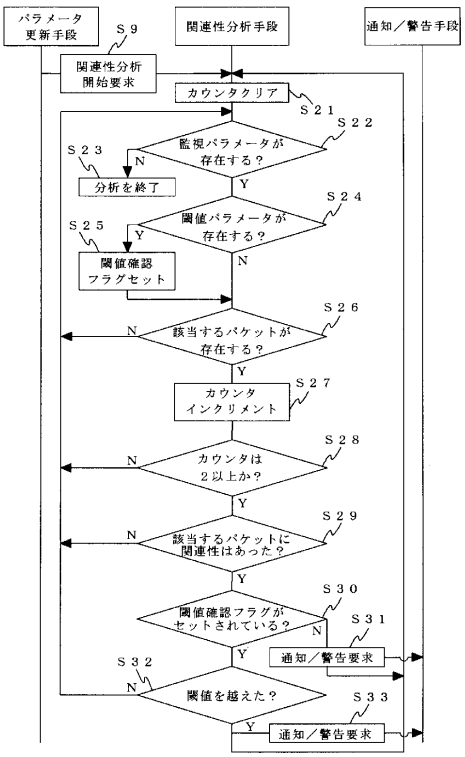
【図４】

テーブルＩＤ	利用者識別番号	パスワード	監視パラメータ	閾値パラメータ	メモリアドレス
1	ＩＤ１２３４	ＸＸＸＸ	A	A	0x1000
2	ＩＤ５６７８	ＹＹＹＹ	B	C	0x2000
3	ＩＤ９９９９	ＺＺＺＺ	D	E	0x3000

【図５】



【図６】



フロントページの続き

(58)調査した分野(Int.Cl.[7], ＤＢ名)
H04L 12/14
H04L 12/24