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

特許第5047419号
(P5047419)

(45)発行日　平成24年10月10日(2012.10.10)　(24)登録日　平成24年7月27日(2012.7.27)

(51)Int.Cl.　　F I
H04M 3/00 (2006.01)　　H04M 3/00　A
H04M 11/00 (2006.01)　　H04M 11/00　302

請求項の数 9　(全 20 頁)

(21)出願番号　特願2001-3610(P2001-3610)
(22)出願日　平成13年1月11日(2001.1.11)
(65)公開番号　特開2001-245056(P2001-245056A)
(43)公開日　平成13年9月7日(2001.9.7)
審査請求日　平成19年11月19日(2007.11.19)
(31)優先権主張番号　09/481951
(32)優先日　平成12年1月12日(2000.1.12)
(33)優先権主張国　米国(US)

(73)特許権者　596092698
アルカテル－ルーセント　ユーエスエー　インコーポレーテッド
アメリカ合衆国　０７９７４　ニュージャーシィ，マレイ　ヒル，マウンテン　アヴェニュー　６００－７００
(74)代理人　100094112
弁理士　岡部　讓
(74)代理人　100064447
弁理士　岡部　正夫
(74)代理人　100085176
弁理士　加藤　伸晃
(74)代理人　100106703
弁理士　産形　和央

最終頁に続く

(54)【発明の名称】通信方法及び通信システム

(57)【特許請求の範囲】
【請求項１】
通信ネットワークにおいてサービスを提供する方法であって、
通信ネットワークにおける少なくとも１つのサービスの提供の要求に応答して、通信セッションを開始し、開始された前記通信セッションと関連する少なくとも１つのデバイスサーバへ前記開始された通信セッションに対する呼処理機能を提供することがホストサーバに可能となるステップと、
前記ホストサーバによって提供された前記呼処理機能に従って、前記通信ネットワークにおいて前記少なくとも１つのサービスを提供することが前記少なくとも１つのデバイスサーバに可能となるステップと、
前記ホストサーバから前記デバイスサーバへ通信されるイベントを呼コーディネータに制御させるステップとを含み、前記呼コーディネータは、前記デバイスサーバと前記ホストサーバとから引き起こされた要求を受信しイベントで動作するものであり、
前記呼処理機能の前記提供が、前記ホストサーバ、前記デバイスサーバ及び前記呼コーディネータの間のレート制御及び接続制御を確立するポリシーサーバによって、前記通信ネットワークの要素の構成情報を維持する手法で制御される、方法。
【請求項２】
前記レート制御及び接続制御の確立は、ネットワーク資源の所定のセットに対するそれぞれのホストサーバ処理のアクセスを制限するために、前記ポリシーサーバが前記通信ネットワーク内に少なくとも１つのファイアウォールを動的にプログラムすることをさらに

含む、請求項１記載の方法。
【請求項３】
前記それぞれの処理のうちの少なくとも１つを実行する際に、前記通信システムがＪａｖａ仮想マシンを用いる、請求項２記載の方法。
【請求項４】
前記デバイスサーバ及び前記呼コーディネータは、クライアント／サーバ配列で結合されている、請求項３記載の方法。
【請求項５】
前記デバイスサーバ及び少なくとも１つの前記呼コーディネータは、階層ネーム空間を開示する、請求項４記載の方法。
【請求項６】
前記呼処理機能は機能アプレットを用いて定義される、請求項３記載の方法。
【請求項７】
前記デバイスサーバ及び前記呼コーディネータは、ＳＳ７信号方式ネットワークによって互いに結合されている、請求項５記載の方法。
【請求項８】
前記ポリシーサーバが、
前記通信セッションを監視し、
前記ネットワーク資源のセットの制御を維持し、そして、
前記ホストサーバ、前記デバイスサーバ及び前記呼コーディネータの動作状態を監視する、動作を更に実行する、請求項２記載の方法。
【請求項９】
前記機能アプレットが独立ソフトウェアベンダーのサーバからダウンロードされる、請求項６記載の方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、通信方法及び通信システムに関し、特に、通信ネットワークの動作の安全性に関する。
【０００２】
【従来の技術】
公衆交換電話ネットワーク（ＰＳＴＮ）、中央電話局（ＣＯ）、構内交換機（ＰＢＸ）等の電話サービスを提供する従来のよく知られた通信システムは、機能ごとの個別の島であり、このような各島は自身の固有の文法及び意味論を持っている。異なる文法、意味論、及びプロトコルの使用は、様々な島が容易に相互接続することを困難にしている。また、このことは、様々な島で切れ目なく共に動作する機能を仮想的に実現することが不可能になっている。
【０００３】
さらに、新たなサービス機能すなわちアプリケーションをネットワークのオペレータによって従来の電話ネットワークに導入するには、内部のアプリケーションプログラマや、数を制限して選択された外部のソフトウェアベンダー（ほとんどの場合、保証されたベンダー）が使用される。
【０００４】
新たなサービス機能をこのように注意深く導入する理由は、介在するベンダー数がわずかであっても、主要なサービス妨害の原因となり得る不確かなソフトウェアがそのネットワークに持ち込まれるという危惧が十分にあり得るからである。これまでに公表された通信ネットワーク障害の多くの例が存在し、その障害はネットワークオペレータ及び顧客基地局に対して多くのサービス妨害及び大きな財政上の損失を招いてきた。
【０００５】
さらに事を複雑にしているのは、音声及びデータネットワークの輻輳が集中する次世代ネ

ットワークの今日の進展がある。すなわち、次世代通信ネットワークは現在のＰＳＴＮ及びインターネットプロトコル（ＩＰ）ネットワークの進展したものになる可能性が非常に高いと考えられる。

【０００６】

現在のサービスプロバイダは、このような次世代ネットワークの開発における多くの要因によって左右される。すなわち、

（１）よく知られたインターネットは音声及びデータの分散における主要なネットワーク選択になっていく。

（２）ＩＰの利用は急激な比率で増加し、これにより相当なデータトラフィックを搬送する現在のＰＳＴＮネットワークに帯域幅の問題が発生する。

（３）ＰＳＴＮ及びパケットネットワーク（例えば、ＩＰネットワーク）の集中が終端間での通信サービの授受ができることを要求する。

（４）パケットネットワークの使用が増加するに伴って新たなサービスの創造を要求する。

（５）市場における規制廃止の増加が、音声及びデータトラフィックの両方において、確立された新たな特化サービスプロバイダのための新たなかつ競争できる通信環境を創り出していく。

【０００７】

このような次世代ネットワークを救済することについての１つの主要な基礎となる機能は、ネットワーク相互運用性である。すなわち、回路及びパケットネットワークで付加価値のある通信サービスを提供するためのサービスプロバイダの能力は、多くの異質のネットワークに亘って相互運用性を実現する能力と密接な関係にある。その異質のネットワークは広範囲の信号方式プロトコル（例えば、ＳＳ７，ＩＰ，メディアゲートウェイ制御プロトコル（ＭＧＣＰ），Ｈ．３２３，セッション初期化プロトコル（ＳＩＰ）等々）をサポートする。

【０００８】

このようなネットワーク相互運用の問題を解決するに有用なスイッチングプラットフォームを発生することを、いわゆる「ソフトウェアスイッチング」と称する。ソフトウェアスイッチング（この技術分野では「ソフトスイッチ」としても知られている）は、信号方式及び移動のためのマルチプロトコル・ソフトウェア・ソリューションであり、これにより回路及びパケットネットワークのような異質のネットワークで相互運用性を実現する。

【０００９】

このようにして、ＰＳＴＮ及びインターネット・テレフォニ・サービスのプロバイダは、ＰＳＴＮ及びＩＰドメイン間に切れ目なく相互運用性を提供することができる。しかし、次世代ネットワークにおけるソフトウェアスイッチの実行を介したネットワーク安全性及び新規サービス機能の導入に関する問題はもちろん変わることなく残る。

【００１０】

さらにまた、次世代ネットワークにおいて重要である２つの主要な安全特性がある。すなわち、いわゆる「演算」安全性及び「ネットワーク」安全性である。例えばソフトウェアスイッチのような演算安全性は、特定のソフトウェアコードの導入がシステム内で実行中の他のソフトウェアコードを破壊することができないように保証することを目的とする。演算安全性は、ソフトウェアをコード化するためのプログラミング言語を選択することによって実現することができる。

【００１１】

例えば、Ｊａｖａは、ユーザがプラットフォーム互換性やネットワーク安全性を気にすることなく、インターネットで使用し実行できるアプリケーションを作成できる一般的なプログラミング言語である。すなわち、Ｊａｖａはよく知られてフラットフォーム中立言語であり、Ｊａｖａを用いて開発されたプログラムは、いかなる修正を必要とすることなく様々なコンピュータシステムで実行できることを意味している。

【００１２】

このようなプラットフォーム非依存性は、「バイトコード」と称するコンパイルされたＪａｖａプログラムのための特殊な形式から生ずる。このバイトコードは、従来のマシンコードと同様に一連の命令であるが、いかなるプロセッサをも指定するものではない。したがって、Ｊａｖａバイトコードは、よく知られているＪａｖａインタプリタを具備しているコンピュータシステムならばどのようなものでも読み出して実行することができる。

【００１３】

したがって、バイトコード形式でＪａｖａプログラムを配列すれば、Ｊａｖａインタプリタが利用できる限り、どのようなプラットフォーム、オペレーションシステム、又はウインドウシステムでもこのプログラムの実行が可能である。このように、Ｊａｖａバイトコードファイルのようなマルチプラットフォームで実行できる単一バイナリファイルを具備する能力は、Ｊａｖａバイトコードを作成してゆくための重要な特性であり、特に、アプレットの形式において、ワールドワイドウェブ（ｗｗｗ）でのプログラムの共通の実行方法である。

【００１４】

バイトコードファイルは、一般にＪａｖａファイルをコンプライすることによって得られ、よく知られたＪａｖａ仮想マシン（ＪＶＭ）に適した形式における単一のクラスで表されるバイトの流れである。Ｊａｖａ仮想マシンはバイトコードを実行して、オブジェクト作成及び不要部分の整理のような一定の基本的能力をもつＪａｖａを提供する。重要なことは、Ｊａｖａは言語に基づく仮想マシンとして演算安全性を実現する。その演算安全性は、あるソフトウェアコードが同じ（又は、異なる）処理空間で実行中の他のソフトウェアコードを破壊することができないように保証する。

【００１５】

【発明が解決しようとする課題】

しかしながら、次世代ネットワークに関する演算安全性が重要である一方、このようなネットワークが確固とした呼処理システムを用いるためには、演算安全性だけではネットワークの安全性を保証するには不十分である。すなわち、ネットワークにおいて、サービス機能のような固有のソフトウェアコードが他のソフトウェアコードを破壊しない場合でも、その固有のソフトウェアコードがネットワークを混乱させる可能性は十分考えられる。例えば、ネットワークの任意の資源を順に使用して、ネットワークを介して任意のメッセージを送信することによってネットワークを混乱させる可能性がある。

【００１６】

いわゆるネットワーク安全性とは、アプリケーションがネットワーク資源を誤って使用し、それによりネットワークが破壊したりネットワーク効率が低下することができないように保証する安全特性のことである。さらに、特に呼処理システムについて、ネットワーク安全性は特定の機能によって生じたどのような破壊であってもその特定の機能に制限されることをも意味する。例えば、１つの呼、及び通常の呼処理システム機能における機能のバランス等に制限されることを意味する。

したがって、本発明は、次世代ネットワークのネットワーク安全性を提供することを目的とする。

【００１７】

【課題を解決するための手段】

本発明は、次世代呼処理システムにおけるネットワーク破壊に対する保護のための方法及び装置の実現を目的とする。さらに本発明によれば、いわゆる接続制御及びレート制御をともに強化するために、様々なネットワークルーティング要素をダイナミックにプログラムすることと結合したより高いレベルの呼処理プロトコル基本命令の意味制限を用いて、ネットワーク安全性を実現する。

【００１８】

本発明の実施形態によれば、このような意味制限は、あるソフトスイッチの様々な要素間で交換され得るメッセージの性質を制限する。さらに、接続制御はソフトスイッチの様々な要素間における接続数を制限し、レート制御はその接続されたところのレートを確立す

る。本発明によれば、このような接続制御及びレート制御は様々なネットワークルーティング要素をダイナミックに再プログラムすることによって成し遂げられる。例えば、接続制御は、ＴＣＰ接続のように、固有の機能を作ることを可能にする接続の数を制限するために用いられ、レート制御は、その固有の機能からのメッセージの数すなわち有効帯域幅を制限するために用いられる。

【００１９】

本発明の実施形態によれば、階層ネーム空間を開示する各資源の集合を用いる分散アーキテクチャが定義される。特に、実施形態の分散アーキテクチャはいわゆる「ルーセントテクノロジー・ソフトスイッチ」（以下、「ＬＴソフトスイッチ」という）であり、ルーセントテクノロジー社から入手できるものである。

【００２０】

実施形態におけるそのアーキテクチャは次世代ネットワークにおけるテレフォニサービスを提供することを目的とし、２つの基本的なタイプの資源すなわち、ｉ）デバイスサーバ、及びｉｉ）呼コーディネータを有する。これらは送信制御プロトコル／インターネットプロトコル（ＴＣＰ／ＩＰ）のような共通プロトコルを用いたネットワークによって相互接続されている。

【００２１】

各資源は複数の呼に関与することができる。すなわち、各資源は与えられた様々な要求を調停できる分散ファイルシステムとしての役割を果たす。利用できる様々な資源間の相互作用は、大体において独立したものであるが、従来の「クライアント／サーバ」アーキテクチャ原理にしたがって終端間の通信を実現する。

【００２２】

本発明によれば、いわゆる呼処理複合部及び機能アプレットのような固有の機能によって使用される固有のプロトコルを分離しかつ制限することによる意味制限を適用することによってネットワーク安全性が実現される。さらに、その機能の直接通信は呼処理複合部に制限される。実施形態によればその呼処理複合部は「インターエイリア」である少なくとも１つのソフトスイッチをもっている。例えば、呼制御複合部の調停要素は相互間の通信を許さない。したがって、デバイスサーバは呼コーディネータにだけ応答する。特に、そのデバイスサーバが供給を受けていた呼コーディネータにだけ応答する。

【００２３】

さらに本発明の実施形態によれば、その制限は、外部エンティティすなわち、いわゆる「ポリシーサーバ」を介してダイナミックにプログラムされる。そのポリシーサーバは呼処理複合部における全ての管理イベントを監視して、その全ての要素上の制御を維持する。このようにして、ポリシーサーバは複合の要素の動作状態を監視し、その要素に関連する構成情報を維持する。これにより、そのポリシーサーバがネットワーク安全性を容易に実現することにおける強力なエンティティになる。

【００２４】

さらに、本発明によれば、次世代ネットワークにおける破壊に対する保護は、接続制御及びレート制御をともに強化するために、様々なネットワークルーティング要素をダイナミックにプログラムすることと結合したより高いレベルの呼処理プロトコル基本命令の意味制限を用いて実現される。

【００２５】

【発明の実施の形態】

この実施形態において特に、「クライアント／サーバ」アーキテクチャの従来の方法で使用されている「デバイスサーバ」、「サーバ」という言葉において、サーバはクライアントからの要求に応じて動作し、要求がなければクライアント要求に応じて動作することはない。デバイスサーバは、呼コーディネータと通信するために使用するプロトコルにおけるプロトコル状態情報を管理する。

【００２６】

各デバイスサーバは階層ネーム空間として自分自身を開示することにより、そのデバイス

サーバによって提供されるサービスの利用を望むクライアントがそのデバイスサーバにアクセスできるようにする。クライアントはあたかも分散ファイルシステムにアクセスしているようにデバイスサーバにアクセスする。一般的なデバイスサーバは物理的／論理的な電話デバイスを提供し、これらのデバイスには、ａ）エンドポイント・デバイスサーバ、及び、ｂ）ゲートウェイサーバが含まれる。

【００２７】

エンドポイント・デバイスサーバは、キーボード、インジケータランプ、表示器等の通信のための制御器を提供し、音声ディジタル化、転送、再構成等のメディアレンダリングを実行する。エンドポイント・デバイスサーバは、電話デバイスサーバ、自動アテンダント（例えば、音声メッセージング）サーバ、インテリジェントパーソナル通信のためのサーバであるいわゆるインテリジェント・エージェント、及びその他を含むことができる。

【００２８】

エンドポイント・デバイスサーバの１つの例は電話デバイスサーバである。電話デバイスサーバは一般的に電話セットで代表され、その電話セットは、ａ）発呼開始、終端、及び制御操作のためにユーザによって使用される制御面、並びに、ｂ）オーディオアプリケーションのためのスピーカやマイクロフォン、ビデオアプリケーションのための表示画面、及びその他のメディアレンダリング・エンジンで構成される。

【００２９】

実際の制御面及びメディアレンダリングの細部は、様々な固有の実施形態において異なっている。すなわち、電話セット又は通信デバイスごとに異なっている。例えば、標準の簡単な旧式電話サービス（ＰＯＴＳ）の電話セットには表示器がなく、その制御面の多くの面が帯域内信号方式に対するＰＯＴＳ電話機セット自身のメディアを用いて実際に実行される。

【００３０】

これと対照に、いわゆるパーソナルコンピュータ（ＰＣ）ソフト電話は、メニュー／ウインドウを制御面として使用し、ＰＣのサウンドカードを介して行われるオーディオレンダリングを有する。別のタイプの電話デバイスはＰＣが実行する標準のＨ．３２３クライアントである。Ｈ．３２３クライアントに対する代行は、一般的には共通プロトコルネットワークにおいて、このような電話デバイスを実行し、ファイルシステム・インターフェース等のネーム空間インターフェースを開示する。これら全ての電話デバイス及び他の電話デバイスは、適当な電話デバイスサーバに接続される。

【００３１】

ダイヤルトーン、リンギング、及びその他のような標準のテレフォニ・コンセプトは、固有の電話デバイスに属する細部であることは明らかである。したがって、ＰＯＴＳ電話機をサポートする電話デバイスサーバはおそらくダイヤルトーンを供給し、これに対してＰＣユーザインターフェースはダイヤルトーンのアナログ信号は直接には持たず、それ故にＰＣ電話をサポートしている電話デバイスサーバはダイヤルトーンを供給しない。重要な概念は、呼コーディネータのように電話デバイスサーバを使用する他のどんなクライアントも、エンドポイントデバイスの個々の細部及び付属する細部について意識しないことである。

【００３２】

ＰＯＴＳ電話機セットに対しても、電話デバイスサーバはＰＣの形式で実行する。そのＰＣは、ＰＯＴＳ電話機セットに接続されたＰＯＴＳインターフェースカード、及びＴＣＰ／ＩＰ接続のネットワークカードを具備している。ＴＣＰ／ＩＰで使用する場合は、ＴＣＰ／ＩＰ接続を得るために使用可能などのような通信デバイスでもネットワークカードとして可能である。

【００３３】

例えば、ネットワーク・インターフェース・カード（ＮＩＣ）、従来のアナログモデム、光ファイバ・インターフェー・スカード、ＩＳＤＮモデム、ディジタル加入者ループ（ＤＳＬ）技術の全ての形式、及びその他がネットワークカードとして可能である。電話デバ

イスサーバは、ＴＣＰ／ＩＰカードのように、呼コーディネータ及び他のデバイスサーバによって使用されるネットワークに接続するために用意された、加入者ループキャリア又は構内交換機（ＰＢＸ）の形式で実行する。

【００３４】

ゲートウェイサーバはいわゆる２つの側面を持っている。１つの側面はあたかもデバイスサーバであるかのように、呼コーディネータに見えるように実行し、呼コーディネータ又は他のデバイスサーバによって使用されるネットワークにゲートウェイデバイスサーバを接続するために実行する。ゲートウェイサーバの他の側面は、制御及び操作と同様に、電話サービスの先に存在する島に対するインターフェースに適合したインターフェースを具備している。

【００３５】

ゲートウェイサーバの例としてはラインデバイスサーバがある。実際に、ラインデバイスインターフェースは一般的にレガシーネットワークインターフェースであり、よく知られているＰＳＴＮのように、電話サービスの先に存在する島を介して複数の電話発呼をサポートする能力を持っている。

【００３６】

ゲートウェイデバイスサーバの主な機能は、デバイスサーバ及び呼コーディネータが接続しているネットワークと他の外部ネットワーク、例えばテレフォニの島の１つであるネットワークとの間でゲートウェイとしての役割を果たすことである。このために、ゲートウェイデバイスサーバはネットワークにおける確定したエンティティであり、そのネットワークの適当なプロトコルを使用する。

【００３７】

自己のクライアントすなわち呼コーディネータに対してネーム空間を開示することによって、個々のゲートウェイデバイスサーバはその呼コーディネータをそのネットワークの特定の信号方式プロトコルから保護する。このことはそのゲートウェイデバイスサーバにおいてプロトコルの特定の状態を維持することによって遂行される。デバイスサーバは、多数の呼コーディネータを取り扱うのと同じように、単一の呼コーディネータからの多数の発呼を取り扱う。このような多数の相互作用及び多重化を取り扱うために、デバイスサーバはローカル状態を維持する。

【００３８】

呼コーディネータは様々なデバイスサーバとの間で通信を実行する。呼コーディネータは、デバイスサーバが取り付けられたネットワークに接続されたコンピュータによって実行されるソフトウェアモジュールとして動作する。呼コーディネータを実行するコンピュータはデバイスサーバの１つの若しくは複数のコンピュータと分離されるか、又は、そのコンピュータはデバイスサーバの複数のコンピュータ若しくはそのネットワークに取り付けられた他のコンピュータと処理力を共有する。

【００３９】

あるいはまた、その呼コーディネータの機能性が複数のコンピュータに分散されて、それらのコンピュータがデバイスサーバのコンピュータといかなる組み合わせであれ、分離され若しくは共有される。さらに、単一のネットワークには複数の呼コーディネータを取り付ける。

【００４０】

発呼／通信、及び関連するいかなる管理タスクであれ、呼コーディネータによって完全に取り扱われる。従来の「クライアント／サーバ」アーキテクチャの各「クライアント」における呼コーディネータ機能は、例えば様々なデバイスサーバに対してサービス要求を開始する。一般的には、このような要求は呼コーディネータによって検知されたいわゆる「イベント」に対する応答である。デバイスサーバはクライアントであるので、様々なサーバからのサービスを要求することができる。すなわち、デバイスサーバ又はゲートウェイサーバは、特定の発呼及びストアされた規則若しくは登録の上に供給されるサービスに該当する。

【００４１】
デバイスサーバは通信状態を意識することはない。通信状態は多数のデバイスサーバ間における相互作用である。あるいはまた、通信状態は呼コーディネータによって維持されるものである。呼コーディネータは階層ネーム空間として通信状態を開示する。デバイスサーバのクライアントとしての呼コーディネータは、デバイスサーバが通信を実行するように操作する。呼コーディネータはさらに、このような相互作用を「呼セッション」として知られている階層ネーム空間として獲得するとともに開示する。
【００４２】
呼コーディネータは発呼を一連のステップとして処理する。その各ステップは、「機能アプレット」と称するコンピュータで実行可能な小さなコードによって実行される。機能アプレットは呼処理における特定のステップを実行し、一般的には呼コーディネータによって開示されたネーム空間の呼ツリーを処理する。すなわち、機能アプレットのローディングは別として、呼コーディネータ及び機能アプレットはもっぱら呼ツリーを介して通信する。
【００４３】
機能アプレットはダイナミックにロードされ、呼コーディネータによって実行される。本発明によれば、機能アプレットコードはネットワークのどこでも位置づけすることができる。また、機能アプレットコードはネットワーク若しくは独立ソフトウェアベンダーから離れてロードすることができる。あるいはまた、機能アプレット自身をネットワークの他のどこででも実行することができる。セッション状態は、呼コーディネータによって階層ネーム空間として開示される呼ツリーを用いて処理されるので、機能アプレット自身の位置又はその実行は、進行中の呼／セッションの処理の部分とは無関係である。
【００４４】
上記の説明から明らかなように、異質の通信ネットワークの間でのネットワーク相互運用性を実現する能力は、次世代通信ネットワークを提供する上で重要である。本発明の様々な態様は、このような通信ネットワークにおけるネットワーク安全性を提供することを目的としている。
【００４５】
図１は、本発明によるネットワーク安全性を実現するＰＳＴＮ／ＩＰ通信ネットワーク１００におけるアーキテクチャ例を示している。図に示すように、アーキテクチャ１００は、ＰＯＴＳ電話機１０５及び１１０、ＩＰ電話機１１５、ＳＳ７ネットワーク１２０及び１２５（ＰＳＴＮの一部で形成されている）、ＩＰネットワーク１３０、トランクゲートウェイ１４０及び１４５、アクセスゲートウェイ１５０、ディレクトリ１３５、並びに、呼処理複合部１５５を備えている。実施形態においては、呼処理複合部はソフトスイッチを有するが、特にこの場合の実施形態としては、ルーセント・テクノロジー社から入手できる上記したＬＴソフトスイッチが好ましい。
【００４６】
図１に示すように、呼処理複合部１５５を構成するのは、呼コーディネータ１６０、デバイスサーバ１７０、１７０－１、１７０－２、及び１７０－３、ユーザ機能アプレット１７５、サービスプロバイダサブレット１８０、ディレクトリコーディネータ１８５、並びに、ポリシーサーバ１６５である。
【００４７】
呼コーディネータ１６０は上記したようにオブジェクトであり、呼処理セッション等の複数の通信セッションにおいて必要なイベントの全体の流れを管理し、また、管理されている各呼の情報を維持する。例を上げれば、呼コーディネータ１６０によって維持される情報は、ユーザ機能アプレット、サービスプロバイダサブレット、及びデバイスサーバのように、呼処理要求において利用されるような、呼指定項目を含んでいる。後で詳述するように、呼コーディネータ１６０によって維持される情報は共通のネーム空間として与えられ、そのシステムで関係のあるエンティティであればその情報にアクセスできるようになっている。

【００４８】
呼処理複合部１５５におけるデバイスサーバ１７０、１７０－１、１７０－２、及び１７０－３はそれぞれ、異なるプロトコルを用いて様々なネットワーク要素との間で通信することができる。例えば、デバイスサーバ１７０は、図に示すようにＳＳ７デバイスサーバであり、ＳＳ７ネットワーク１２０及びトランクゲートウェイ１４０を経由して、よく知られたＳＳ７信号方式プロトコルにおける通信を容易にする。同様に、デバイスサーバ１７０－３は、図に示すようにＳＩＰデバイスサーバであり、ＩＰネットワーク１３０のようなパケットネットワークを経由して、よく知られたＳＩＰ信号方式プロトコルにおける通信を容易にする。
【００４９】
呼処理複合部１５５は、異なるプロトコルやゲートウェイ構成の各々に対応するデバイスサーバを通信要求に応じて利用する。さらに、このようなゲートウェイへの通信又はゲートウェイからの通信は呼処理複合部１５５内に完全に包含され、これにより使用されているプロトコルを認識している通信システム内の他の要素に対する要求を排除する。このようにして、アーキテクチャ１００の例のような通信システムへの新規ゲートウェイの提供は、呼処理複合部１５５の他のいかなる部分にも衝撃を与えることなく、そのゲートウェイのタイプに対応する適切なデバイスサーバを追加することによって簡単に実行される。
【００５０】
図２は、デバイスサーバにおけるネーム空間ツリー２００を示している。従来のファイルシステムのように、ネーム空間ツリー２００のルートノード２１０は「＃／」で示される。イベント制御２２０はファイルであり、そのファイルの中に呼コーディネータに対して示されるべきイベントが書き込まれ、そのファイルの中に呼コーディネータからのサービス要求が書き込まれる。
【００５１】
したがって、呼を発生すべき指示及びダイヤルされる数字がイベント制御２２０に配置される。ノードデータ２３０は、呼が設定されるとすぐにメディアの交渉のために使用される。ノードユーザ２４０は、上述したようにまた後で詳述するように、デバイスサーバに対する呼の処理中の呼コーディネータによって機能アプレットが動作すべきであることに関する指示を含んでいる。
【００５２】
さらに、図３は呼コーディネータのネーム空間３００の例を示している。ネーム空間３００において、ネーム空間のルートノード３１０は「＃／」である。ルートノード３１０の下にグローバルイベント制御ファイル３２０がある。グローバルイベント制御ファイル３２０は、呼全体に関係する全てのイベントを保持する。例えば、時間経過によるレートスケジュール序列の変化のように、全体的に情報序列に関係するイベントを保持する。さらに、グローバルイベント制御ファイル３２０は、特定の呼コーディネータに位置している全ての呼処理イベントについて知ることを望むイベント明細記録のようなプログラムによって開かれて解読される。
【００５３】
呼ツリーノード３３０もまたルートノード３１０の下にあり、呼コーディネータ１６０のようにアクティブな呼コーディネータの管轄のもとで全てのアクティブな呼を有する。したがって、アクティブな呼の各々に対してアクティブな呼ノード３４０が存在する。図３においては、アクティブな呼が１つだけしか示されていないが、本発明によれば、多数の呼コーディネータ及びアクティブな呼が存在することは明らかである。
【００５４】
アクティブな呼ノード３４０の下には、呼ワイドイベント制御ファイル３５０及び番号ノード３６０が呼のデバイスごとに存在する。呼ワイドイベント制御ファイル３５０は、全体としての呼に関係するイベントのために使用される。呼ワイドイベント制御ファイル３５０は、この特定の呼に関連する全ての呼処理イベントを提供する。呼コーディネータ及び機能アプレットは、呼ワイドイベント制御ファイル３５０を介して通信を行う。

【００５５】
番号ノード３６０の各々は、提供するデバイスのネットワーク・ルータブル・アドレスによって識別される。番号ノードは実際に、識別されたデバイスによって開示された全体のネーム空間を提供する。したがって、番号ノードは実際は単一のノードではなく、それ自身がデバイスサーバのネーム空間のツリーになっていて、番号ノード３６０のロケーションに位置づけされたツリーのルートノードを持っている。
【００５６】
図１において、ユーザ機能アプレット１７５は呼における関係者を提供するオブジェクトである。すなわち、ユーザ機能アプレット１７５の実行はそのセッション関係者に関連する必要なサービス論理を実行する。例えば、ユーザ機能アプレット１７５は、よく知られている通話中着信サービスのような発呼者によって要求されたときに、機能アプレット／サービスを提供することになる。このことによって、サービスプロバイダやサードパーティサービスベンダーがサービスを作成することができ、特定のサービスプロバイダの一連のサービスを介して作成したサービスを提供できる。
【００５７】
このように、サービスプロバイダサブレット１８０は、サービス提供をカスタマイズするサービスプロバイダによって利用されるオブジェクトである。例えば、サービスプロバイダサブレット１８０を利用することで、サービスプロバイダは呼処理複合部１５５の動作をカスタマイズすることができ、その日のより低い市外料金レートを利用した異なる時間に異なる通信キャリアを介して、トラフィックの経路を決定する。
【００５８】
なおさらに、ディレクトリコーディネータ１８５は、ＰＳＴＮ及びＩＰネットワークの双方を経由して、特定のサービス提供を要求されたディレクトリ１３５と通信する。例えば、ディレクトリ１３５は、よく知られたサービス制御ポイント（ＳＣＰ）データベース、又はライトウェイト・ディレクトリ・アクセス・プロトコルに基づくデータベース、又はＳＩＰアクティブ・ディレクトリを有することができる。このようにして、呼処理複合部１５５の中でディレクトリコーディネータ１８５の直接の協力により、システム内の他の要素は、特定の機能の提供を要求する情報のためのディレクトリ１３５とのインターフェースから解放される。
【００５９】
本発明によれば、接続制御及びレート制御をともに強化するために、様々なネットワークルーティング要素をダイナミックにプログラムすることと結合したより高いレベルの呼処理プロトコル基本命令の意味制限を用いて、ネットワーク安全性が実現される。本発明によれば、呼処理複合部１５５及びユーザ機能アプレット１７５のような固有の機能によって使用される固有のプロトコルを分離しかつ制限することによる意味制限を適用することによって、ネットワーク安全性が実現される。さらに、その機能の直接通信は呼処理複合部１５５に制限される。
【００６０】
さらに、本発明の実施形態によれば、その制限は、ポリシーサーバ１６５を介してダイナミックにプログラムされる。ポリシーサーバ１６５は呼処理複合部１５５における全ての管理イベントを監視して、その全ての要素上の制御を維持する。このようにして、ポリシーサーバはソフトスイッチの要素の健全性を監視し、その要素に関連する構成情報を維持する。これにより、ポリシーサーバ１６５がネットワーク安全性を容易に実現することにおける強力なエンティティになる。図１においては、ポリシーサーバは呼処理複合部の一部として示されているが、呼処理複合部とは分離して外部において実現してもよい。
【００６１】
さらに、本発明によれば、次世代ネットワークにおける破壊に対する保護は、接続制御及びレート制御をともに強化するために、様々なネットワークルーティング要素をダイナミックにプログラムすることと結合したより高いレベルの呼処理プロトコル基本命令の意味制限を用いて実現される。以下の説明により容易に理解できるように、ある通信セッショ

ンの間に発生した一連の機能の中で、電話発呼はＰＯＴＳ電話機１０５とＩＰ電話機１１５との間に広がる。

【００６２】

例えば、ＰＯＴＳ電話機１０５は従来の方法でＳＳ７ネットワーク１２０に接続され、ＰＯＴＳインターフェースを経由してＳＳ７デバイスサーバ１７０に接続されている。ＳＳ７デバイスサーバ１７０、呼コーディネータ１６０及びＳＩＰデバイスサーバ１７０－３は、データリンクによってさらにＩＰネットワーク１３０に接続されている。

【００６３】

ＩＰネットワーク１３０は、例えば、インターネットのようなネットワーク又はいわゆるイントラネットである。このように、ＳＩＰデバイスサーバ１７０－３は、ＩＰネットワーク１３０を経由して、例えば従来のＴＣＰ接続によりＩＰ電話機１１５に接続される。ＰＯＴＳ電話機１０５とＩＰ電話機１１５との間で電話発呼を遂行するためには、以下に例示する機能が作用する。

【００６４】

ＰＯＴＳ電話機１０５により電話発呼が発生される場合には、ＰＯＴＳ電話機１０５は例えば発呼者によって普通のやり方でオフフックされる。これにより信号がＳＳ７デバイスサーバ１７０に送られる。ＳＳ７デバイスサーバ１７０は、ＰＯＴＳ電話機１０５に対してダイヤルトーンを供給するか又はダイヤルトーンを供給させる。ＰＯＴＳ電話機１０５において行われたダイヤリングに応答して、ＳＳ７デバイスサーバ１７０はダイヤルトーンを停止するか又は停止させ、ダイヤルされた数字を得る。

【００６５】

その後、ＳＳ７デバイスサーバ１７０はイベントを発生する。そのイベントの発生は、ＳＳ７デバイスサーバ１７０の階層ネーム空間で表されるツリーのイベント制御ファイルに書き込むことによって実行される。すでに明らかなように、ＳＳ７デバイスサーバ１７０の階層ネーム空間はツリーデータ構造で表される。

【００６６】

その後、呼コーディネータ１６０等のアクティブな呼コーディネータは、サポートしている全てのデバイスサーバのネーム空間ツリーのイベント制御ファイルを検査する。これにより、呼コーディネータ１６０はＩＰネットワーク１３０の構成又はトポロジーを認識する。認識した構成又はトポロジーは、サーバの背後にある特定のデバイスと同じように例えばデバイスサーバのアドレス等のロケーションが含まれている。

【００６７】

したがって、例えば、呼コーディネータ１６０は、電話デバイスサーバによって対応される電話の所有者の識別、その電話に電話番号があるならばその電話番号、及び直接に対応されるライン、又は着信可能性をラインデバイスサーバによって記憶している。呼コーディネータ１６０にこの認識を提供するための情報は、呼コーディネータ１６０の中に前もってプログラムされているか、又は既存のプロセスを用いて呼コーディネータ１６０によってダイナミックに見つけられるか、又はこれらの組み合わせを用いて遂行される。

【００６８】

上述のイベント制御ファイルの解読に応じて、呼コーディネータ１６０は、イベントが行われたか、及び何かの動作が要求されたかを判別することを義務づけられる。上述した例において、呼コーディネータ１６０は、ＰＯＴＳ電話機１０５のユーザがダイヤルされた数字によって示される電話番号に発呼することを希望するか判別する。発呼者が希望する方法においてこのことを実行するために、呼コーディネータ１６０はユーザ機能アプレット１７５等の必要なアプレットを実行させる。

【００６９】

本発明の実施形態によれば、呼を樹立するために実行される指定アプレットは、おそらく、発呼者についての単一のカスタムアプレット、発呼者についての一般アプレット、発呼者についての一連のカスタムアプレット、発呼者についての一連の一般アプレット、被呼者についての単一のカスタムアプレット、被呼者についての一般アプレット、被呼者につ

いての一連のカスタムアプレット、被呼者についての一連の一般アプレット、上記の任意の組み合わせ、及び又は、例えばＩＳＶのアプリケーションのために書き込まれた他のアプレットである。

【００７０】

これらのアプレットは全て、呼コーディネータ１６０内に配置されるか、又は（呼処理複合部１５５内において）呼コーディネータ１６０の外部に配置されるか、又はこれらの組み合わせとなる。また、これらのアプレットは全て、呼コーディネータ１６０によって実行されるか、又はＩＰネットワーク１３０やＳＳ７ネットワーク１２０及び１２５にそれぞれ接続されたサーバ若しくは呼コーディネータ等の他の資源によって実行される。

【００７１】

例えば、発呼者は、ダイヤルされた電話番号の作用として、指定された被呼者にコンタクトを取るために、多数の電話番号のシーケンスを識別できる機能を特定することができた。機能を特定できた場合には、呼コーディネータ１６０はこの機能に対するアプレットを実行して、ダイヤルされた番号が多数の電話番号のシーケンスに関連したか否かを判別できる。

【００７２】

ダイヤルされた番号が多数の電話番号のシーケンスに関連しなかったイベントの場合には、呼コーディネータ１６０は省略時（デフォルト）呼配置アプレットを実行する。ダイヤルされた番号が多数の電話番号のシーケンスに関連したイベントの場合には、呼コーディネータ１６０はそのシーケンスの最初の電話番号を取得して、省略時呼配置アプレットを実行する。

【００７３】

ダイヤルされた番号と取得した番号とが異なる場合、すなわち呼が完成されなかった場合には、制御はシーケンスアプレットに戻り、次の番号がある場合にはその番号を取得して、再び省略時呼配置アプレットを実行する。そのシーケンスのいずれの電話番号も完成できなかった場合には、シーケンスアプレットは制御を呼コーディネータ１６０に戻す。呼コーディネータ１６０は他のアプレットを実行する。例えば、被呼者に着信できなかった旨を発呼者に通知するためのメッセージを送出する。

【００７４】

単一の電話番号についてＩＰ音声接続が要求されている場合には、呼コーディネータ１６０は、ＩＰネットワーク１３０に対して、取得された数字に対応する被呼者のネットワークルータブルアドレスを判別する。この判別は呼コーディネータ１６０内部又は呼コーディネータ１６０に関連するマッパーによって実行される。本来、そのマッパーはルーティングエンジンである。マッパーの機能は、ある１つのアプレット例えば実行中のアプレットに対して、呼を完成できる可能性のあるゲートウェイデバイスサーバ又は電話デバイスサーバにおけるアドレスの限定されたリストを供給することである。

【００７５】

この実施形態においてはＩＰ接続が要求されているので、マッパーはＳＩＰデバイスサーバ１７０－３のアドレスを返す。呼コーディネータ１６０はクライアントとして、ＳＩＰデバイスサーバ１７０－３からのサービスを要求する。特に、呼コーディネータ１６０は、ＰＯＴＳ電話機１０５から得られた電話番号への接続を確立するようにＳＩＰデバイスサーバ１７０－３に要求する。このことは、適当なコマンド例えば接続確立コマンドを、ＳＩＰデバイスサーバ１７０－３のネーム空間ツリーのイベント制御ファイルに書き込むことによって実行される。

【００７６】

従来のＴＣＰ／ＩＰインターフェース等を経由した呼コーディネータ１６０からのサービス要求に応じて、ＳＩＰデバイスサーバ１７０－３は、要求された接続、すなわち自身からＩＰネットワーク１３０への接続、そして最終的にはＩＰ電話機１１５への接続を確立するための処理を開始する。ＩＰ電話機１１５への接続が終了した場合には、呼コーディネータ１６０はＳＳ７デバイスサーバ１７０とＳＩＰデバイスサーバ１７０－３との間の

メディアパスを確立する。このことは、ＳＳ７デバイスサーバ１７０及びＳＩＰデバイスサーバ１７０－３のそれぞれのネーム空間ツリーのイベント制御ファイルに、呼コーディネータ１６０がメディア連結性のサービス要求を書き込むことによって実行される。

【００７７】

呼の確立及び接続が成功した場合には、呼コーディネータ１６０は、そのイベントにおいて、さらなるサービスがその呼に要求されているかを監視する。例えば、通信デバイスの１つが「オンフック」に移行することに応答して呼終了が要求される。あるいは、追加機能処理、例えば、通話中着信、呼転送、又は勘定分配が要求される。

【００７８】

呼が設定されたときは、サービスを提供すべきことの必要性は、ＳＳ７デバイスサーバ１７０やＳＩＰデバイスサーバ１７０－３の関係する方のネーム空間ツリーのイベント制御ファイルに配置された要求によって指示される。呼コーディネータ１６０はそのイベント制御ファイルを解読して、適当なアプレットを実行し、また、クライアントとして適切なデバイスサーバに対してサービス要求を発行する。

【００７９】

呼を終了するために、例えば、ＰＯＴＳ電話機１０５はオンフックに移行する。このイベントは、ＳＳ７デバイスサーバ１７０のネーム空間ツリーのイベント制御ファイルに書き込まれ、呼コーディネータ１６０はそのイベントを認識することになる。そのイベントに応答して、呼コーディネータ１６０によってアプレットが実行される。本発明によれば、そのイベントはＳＳ７デバイスサーバ１７０及びＳＩＰデバイスサーバ１７０－３からの切断サービスを要求する。この要求は、切断されるべきそれぞれの電話番号とともに、両者のネーム空間ツリーのイベント制御ファイルの各々に書き込まれることによって実行される。

【００８０】

同様に、ＩＰ電話機１１５が呼を終了する場合にも、このイベントの指示がＳＩＰデバイスサーバ１７０－３のネーム空間ツリーのイベント制御ファイルに書き込まれる。ＳＩＰデバイスサーバ１７０－３のイベント制御ファイルにおいてこのイベントが検出された場合には、呼コーディネータ１６０は関連するアプレットを実行する。本発明の実施形態によれば、そのイベントはＳＳ７デバイスサーバ１７０及びＳＩＰデバイスサーバ１７０－３からの切断サービスを要求する。この要求は、切断されるべきそれぞれの電話番号とともに、両者のネーム空間ツリーのイベント制御ファイルの各々に書き込まれることによって実行される。

【００８１】

上記した実施形態において高く評価できることの１つとして、例示したテレフォニサービスの提供はいくつかの処理又は処理の連続の実行を伴う。例えば、呼コーディネータ、デバイスサーバ、及び機能アプレット、並びに異質のネットワークを介した多数のプロトコルの使用を伴う。

【００８２】

詳細に説明したように、この実施形態は、Ｊａｖａ仮想マシン等の仮想マシンを用いたシステムを使用して実行される。ネットワーク安全性の提供は、アプリケーションがネットワーク資源を誤って使用し、それによりネットワークが破壊したりネットワーク効率が低下することができないように保証することが重要である。さらに、特に呼処理システムについて、ネットワーク安全性の提供は、特定の機能によって生じたどのような破壊であってもその特定の機能に制限されることを保証する。例えば、１つの呼、及び通常の呼処理システム機能における機能のバランス等に制限される。

【００８３】

前に説明したように、本発明によれば、ネットワーク安全性は、いわゆる接続制御及びレート制御をともに強化するために、様々なネットワークルーティング要素をダイナミックにプログラムすることと結合したより高いレベルの呼処理プロトコル基本命令の意味制限を用いて実現される。例えば、このような意味制限は、あるソフトスイッチの様々な要素

間で交換され得るメッセージの性質を制限する。

【００８４】

さらに、接続制御はソフトスイッチの様々な要素間における接続数を制限し、レート制御はその接続されたところのレートを確立する。本発明によれば、このような接続制御及びレート制御は様々なネットワークルーティング要素をダイナミックに再プログラムすることによって成し遂げられる。本発明によれば、ネットワーク安全性は、呼処理複合部１５５のような呼処理複合及びユーザ機能アプレット１７５のような固有の機能によって使用される固有のプロトコルを分離することによる意味制限を適用することによって実現される。さらに、その機能の直接通信は呼処理複合部１５５に制限される。

【００８５】

さらに、本発明の実施形態によれば、その制限は、ポリシーサーバ１６５を介してダイナミックにプログラムされる。ポリシーサーバ１６５は呼処理複合部１５５における全ての管理イベントを監視して、その全ての要素上の制御を維持する。このようにして、ポリシーサーバはソフトスイッチの要素の健全性を監視し、その要素に関連する構成情報を維持する。これにより、ポリシーサーバがネットワーク安全性の提供を容易に実現することにおける強力なエンティティになる。

【００８６】

図４は、本発明による通信ネットワークにおけるネットワーク安全性を提供するための動作４００を示すフローチャートである。まず、呼処理要求等の通信セッションが初期化される（ブロック４１０）。特定の通信セッションのために適切な機能アプレットが選択される（ブロック４２０）。本発明の様々な実施形態によれば、複数の機能アプレットが以下に示すように、選択又は供給される。すなわち、（ｉ）呼処理複合内に直接に、（ｉｉ）ソフトスイッチから直接に、（ｉｉｉ）ユーザから、（ｉｖ）独立ソフトウェアベンダー（ＩＳＶ）から、（ｖ）サービスプロバイダから、又は（ｖｉ）これらの組み合わせによって、選択又は供給される。

【００８７】

選択された機能アプレット及び通信セッションとして、本発明によれば、ポリシーサーバ（例えば、図１におけるポリシーサーバ１６５）は、特定のレート制御機能及び接続制御機能を初期化して、ネットワークの選択エンティティ内にダイナミックにプログラムする（ブロック４３０）。

【００８８】

特に、ポリシーサーバは、機能アプレットがストアされる場所を決定し、ストアされた機能アプレットから呼処理複合すなわちソフトスイッチへのパスを決定する。その後、ポリシーサーバは、前記したパスに沿ってネットワーク要素を決定する。特に本発明の実施形態によれば、ネットワーク制御のソフトスイッチにおけるネットワーク要素はディレクトリサーバに登録する。これにより、いわゆるディレクトリ可能ネットワークの提供が容易にできる。

【００８９】

このようなディレクトリ可能ネットワークにおいて、ポリシーサーバはディレクトリサーバに問い合わせて、登録されたネットワーク要素がネットワークにおける関連するパスに沿っていること、登録された様々な特性、及びこのようなネットワーク要素の性質を確かめる。本発明の実施形態によれば、このようなネットワーク要素は、初期化並びに新たなレート制御及び接続制御ポリシーを実現することによって再プログラミングされる。

【００９０】

特に、このようなレート制御及び接続制御ポリシーは、機能アプレットによって接続可能なネットワークエンティティのタイプ、及び、どの指定通信に対しても許される時間周期におけるメッセージの数を指定する。したがって、本発明の実施形態によれば、与えられたポリシーは、よく知られている通信プロトコルにより、そのポリシーを識別されたパスを介してネットワーク要素に送信することによって実行される。

【００９１】

さらに、指定コードフラグメント、いわゆるポリシー・エンフォースメント・ポイント（ＰＥＰ）はこのような送信を受信する。ＰＥＰはよく知られているソフトウェアフラグメントであり、２つのいわゆる「側面」を持っている。ＰＥＰフラグメントの一方の側面は送信されたポリシーをよく知られている通信プロトコルで受け取る。ＰＥＰフラグメントの他方の側面は指定デバイスに制御信号をその指定デバイスの範囲で送る。

【００９２】

例えば、よく知られているパケット音声ゲートウェイ（ＰＶＧ）又はルータに対するＰＥＰは、ポリシーサーバからのポリシーを受信して、必要なサーバに指定されているコマンドのシーケンスにそのポリシーを変換し、このコマンドをそのデバイスに送信する。

【００９３】

下記の様々な方法でこのコマンドの送信が行われることは高く評価される。すなわち、（ａ）ＰＥＰはデバイス自身で実行するので送信は内部処理通信（ＩＰＣ）の形式を採ることができる。又は（ｂ）ＰＥＰはネットワーク上のホストマシンで実行し、よく知られているシンプル・ネットワーク・マネージメント・プロトコル（ＳＮＭＰ）のようなコマンドプロトコルを介してコマンドシーケンスを送る。そのプロトコルはデバイスすなわちネットワーク要素によってサポートされている。又は（ｃ）ＰＥＰはネットワーク上の固有のホストマシンで実行し、ネットワーク要素上でリモートログインセッションを開いて、よく知られているコマンド・ライン・インターフェース（ＣＬＩ）を用いて、コマンドシーケンスをネットワーク要素に送る。

【００９４】

前記の説明は、ポリシーサーバとＰＥＰとの間、及びＰＥＰとネットワーク要素との間の通信である本質的に「一方の方向」の通信、すなわち、ポリシーサーバからＰＥＰへの通信、及びＰＥＰからネットワーク要素への通信に集中したが、他の方法においても情報が流れることはもちろんである。すなわち、本発明における上記実施形態によれば、通信はネットワーク要素からＰＥＰ及びポリシーサーバに流れることも可能である。

【００９５】

このような情報は「イベント」として特徴づけられる。したがって、ネットワーク要素はＰＥＰに対して開示される複数のイベントを発生する。例示するならば、このようなイベントに対するネットワークを監視して、デバイスによってストアされ更新された情報を周期的に読み出し、又は、よく知られているプロトコルを用いてネットワーク要素からこのようなイベントを受信する。

【００９６】

このようにして、ＰＥＰはポリシーサーバに対してこれらのイベントを順番に開示する。そのポリシーサーバの中でこのようなイベントは複数の動作を開始する。これらの動作は、ネットワーク要素の再プログラミングを要求するＰＥＰに対して複数のポリシーを送信することになる。したがって、ネットワーク要素において発生されたイベントは、新たなポリシーに対応して再プログラムされるネットワーク要素を生じる。これにより要素の動きが交替する。

【００９７】

例えば、２つのイベントＡ及びＢがネットワーク要素１及び２においてそれｚれ発生され、それぞれポリシーサーバに対して開示されたとする。この実施形態によるポリシーサーバは、その２つのイベントを相互に関連させて、そのネットワーク要素を再プログラムするために新たなポリシーを発行することになる。

【００９８】

ポリシーサーバによってサポートされたその相関は、（ａ）複数のイベントの結合、（ｂ）複数のイベントの分離、（ｃ）反復するイベントのシーケンス、（ｄ）いわゆる「ワイルドカード」及びある特定イベントを含むイベントのシーケンス、又は（ｅ）複数のイベントの空白、を含むことになる。したがって、この実施形態において、イベントは、許容される論理的順序であれば、上記掲げた（ａ）乃至（ｅ）のどのような結合ででも表現できる。

【００９９】
したがって、以下のことは高く評価される。すなわち、複合イベントセットは、このようなイベント表現で取得して記述することが可能であり、そのイベント表現は様々なネットワーク要素において発生する異なる条件セットを識別するのに使用することができる。それゆえ、本発明によるポリシーサーバは、様々な条件を理解するために位置づけされ、また、ネットワーク要素を選択するために指定された新たなポリシーを送信することによって、修正できる動作又は割込できる動作を取るために位置づけされる。
【０１００】
例えば、後で記述する実施形態のように、ポリシーサーバは、図１のＳＳ７ネットワーク１２０のように特定のネットワークにおいてファイアウォールをプログラムして、このネットワークにアクセスするレート制御が実行されるのを保証する。よく知られているように、ファイアウォールは、様々な安全措置を提供するために使用され、コンピュータウィルスの侵入のような、外部からの安全侵害からネットワークを保護する。
【０１０１】
本来この安全体系は分離したコンピュータシステムに配置する。すなわち、ファイアウォールは、私設ネットワークと例えばインターネット等の公衆ネットワークとの間に配置する。これらのファイアウォールはソフトウェア基盤のゲートウェイであり、一般的には、アウトサイダーすなわち無許可のユーザによる攻撃からローカルエリアネットワーク（ＬＡＮ）のコンピュータを保護するためにインストールされる。
【０１０２】
ファイアウォールは、私設ネットワークからの及び私設ネットワークへの通信上の制御を維持する。本来、ファイアウォールは私設ネットワークを使用している全てのユーザに安全措置の義務を負わせるものである。例えば、ファイアウォールは、新たなインターネットサービス又はワールドワイドウェブ（ｗｗｗ）の新たなサイトにアクセスするのをブロックする。現在のファイアウォール構成によっては安全の因果関係が分からないし、捉えることができないからである。
【０１０３】
したがって、本発明によれば、ポリシーサーバは「インターエイリア」を保証するために関連するファイアウォールをプログラムする。すなわち、独立ソフトウェアベンダー（ＩＳＶ）が機能アプレットに応対するサーバ等のホストエンティティへのレート制御されたアクセスを有すること、又はあるネットワーク（例えば、ＳＳ７ネットワーク）において応対された機能アプレットがネットワーク資源の所定のセットへのレート制御されたアクセスを有すること、又は応対されたアプレットが呼コーディネータへのアクセスを有することを保証するために、関連するファイアウォールをプログラムする。
【０１０４】
ポリシーサーバによるレート制御及び接続制御のダイナミックプログラムが終了した場合には、すでに詳述したように、呼処理複合部１５５は、セッションワイドアクセス制御を実行し、呼処理要求において関係している全てのネットワーク資源からの呼制御基本命令を受け入れる（図４のブロック４４０）。ソフトスイッチによって実行されたセッションワイドアクセス制御は、呼処理が完了するまで持続する（図４のブロック４５０）。呼処理が完了した場合には、通信セッションは終了する（図４のブロック４６０）。
【０１０５】
図５は、本発明によるネットワーク安全機能を具備したネットワーク・マネージメント・シナリオ５００の例を示している。このシナリオ５００は、ホストサーバ５１０で応対された機能アプレット５０５から始める。この場合、ホストサーバ５１０は、呼処理複合部５１５内に存在しているデバイスサーバ５３０に接続することを試みる。
【０１０６】
すでに詳述したように、応対されたアプレットは特定の呼セッションにおいて利用され、その呼セッションによって要求された呼処理機能を提供する。本発明によれば、機能アプレット５０５とデバイスサーバ５３０との接続はポリシーサーバ５３５によって制御され

る。ポリシーサーバ５３５はこの通信システム内において分離したエンティティである。
【０１０７】
さらに、呼コーディネータ５２０は、機能アプレット５０５によって初期化されたイベントで、機能アプレット５０５によって呼コーディネータ５２０内に生じたどんな悪影響でも緩和するためにデバイスサーバ５３０やデバイスサーバ５２５に多重化されたイベントを制御する。さらに、上記したように、呼コーディネータ５２０はセッションワイドアクセス制御を実行し、通信セッションにおいて関係している内部交換ネットワーク（ＩＸＣ）５５５等の全てのネットワーク資源からの呼制御基本命令を受け入れる。
【０１０８】
シナリオ５００によれば、機能アプレット５０５はまた、ＩＳＶ５４０内に存在するデバイスサーバ５４５に接続することを試み、デバイスサーバ５４５が不当な目的を持っている場合には、そのデバイスサーバに関連しているデバイスゲートウェイに対するサービスを否定するようにそのデバイスサーバに命令する。
【０１０９】
上記したように、本発明によるポリシーサーバは、「インターエイリア」を保証するためにＩＳＶ５４０に関連するファイアウォールをプログラムする。すなわち、ＩＳＶ５４０が機能アプレットに応対するホストエンティティ（例えば、ホストサーバ５１０）へのレート制御されたアクセスを有すること、又は機能アプレットが必要な資源の所定のセットへのレート制御されたアクセスを有することを保証する。
【０１１０】
さらに、シナリオ５００によれば、デバイスサーバ５４５は、呼の所望のルーティングを指示するために、呼コーディネータ５２０に接続することを試みる。前と同じように、ポリシーサーバ５３５は、ＩＳＶ５４０、呼処理複合部５１５、ＩＸＣネットワーク５５５内に存在するファイアウォールをプログラムして「インターエイリア」を保証する。すなわち、レート制御されたアクセス及び接続制御であるネットワーク安全性が通信セッション内に実現される。
【０１１１】
さらに、セッションにおける特定の呼処理要求によって要求された機能アプレット５５０は、呼コーディネータ５２０へのアクセスを要求する。機能アプレット５０５と同様に、機能アプレット５５０と呼コーディネータ５２０との接続は、ポリシーサーバ５３５によって制御される。さらに、呼コーディネータ５２０は機能アプレット５５０によって初期化されたイベントで、機能アプレット５５０の実行によって呼コーディネータ５２０内に生じたどんな悪影響でも緩和するために、デバイスサーバ５３０やデバイスサーバ５２５に多重化されたイベントを制御する。
【０１１２】
優れた本発明によれば、次世代呼処理システムにおけるネットワーク破壊に対する保護は、接続制御及びレート制御をともに強化するために、様々なネットワークルーティング要素をダイナミックにプログラムすることと結合したより高いレベルの呼処理プロトコル基本命令の意味制限を用いて実現される。
【０１１３】
上記したように、本発明は、複数の方法及びこれらの方法を実現する複数の装置の形で実施される。本発明はまた、具体的な媒体で実施されるプログラムコードの形で実施される。例えば、フロッピーディスク、ＣＤ－ＲＯＭ、ハードディスク、又はその他の機械で読み取り可能な記憶媒体において、その中のプログラムコードが機械内にロードされてその機械によって実行される場合には、例えばコンピュータ等からなるその機械は、本発明を実現する装置になる。
【０１１４】
本発明はまた、何らかの通信媒体で送信されるプログラムコードの形で実施され、例えば、電線、ケーブル、光ファイバ、又は電波を介して送信されたそのプログラムコードが機械内にロードされてその機械によって実行された場合には、例えばコンピュータ等からな

るその機械は、本発明を実現する装置になる。汎用プロセッサでプログラムコードが実行される場合には、そのプログラムコードセグメントはそのプロセッサ内に組み込まれて、特定用途の論理回路と類似した動作をするユニークなデバイスを提供する。

【図面の簡単な説明】

【図１】本発明によるネットワーク安全性を実現するＰＳＴＮ／ＩＰネットワークにおけるアーキテクチャの例を示す図。

【図２】図１に示すようなデバイスサーバにおけるネーム空間ツリーを示す図。

【図３】図１に示すような呼コーディネータのネーム空間の例を示す図。

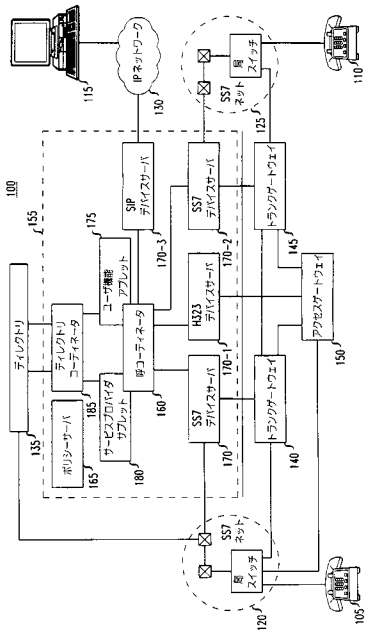
【図４】本発明による通信ネットワークにおけるネットワーク安全性を実現する動作４００を示すフローチャート。

【図５】本発明によって実現されるネットワーク安全性機能を具備するネットワーク管理シナリオの例を示す図。

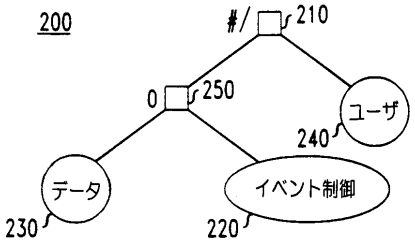
【符号の説明】

１００　ＰＳＴＮ／ＩＰ通信ネットワーク
１０５，１１０　ＰＯＴＳ電話機
１１５　ＩＰ電話機
１２０，１２５　ＳＳ７ネットワーク
１３０　ＩＰネットワーク
１３５　ディレクトリ
１４０，１４５　トランクゲートウェイ
１５０　アクセスゲートウェイ
１５５，５１５　呼処理複合部
１６０，５２０　呼コーディネータ
１６５，５３５　ポリシーサーバ
１７０，１７０－１，１７０－２，１７０－３，５２５，５３０，５４５デバイスサーバ
１７５　ユーザ機能アプレット
１８０　サービスプロバイダ・サブレット
１８５　ディレクトリコーディネータ
２００　ネーム空間ツリー
２１０　ルートノード
２２０　イベント制御
２３０　ノードデータ
２４０　ノードユーザ
３００　呼コーディネータのネーム空間
３１０　ネーム空間
３２０　グローバルイベント制御
３３０　呼ツリーノード
３４０　アクティブ呼ノード
３５０　呼ワイドイベント制御ファイル
３６０　番号ノード
５００　ネットワーク・マネージメント・シナリオ
５０５，５５０　機能アプレット
５１０　ホストサーバ
５４０　独立ソフトウェアベンダー（ＩＳＶ）
５５５　内部交換ネットワーク（ＩＸＣ）

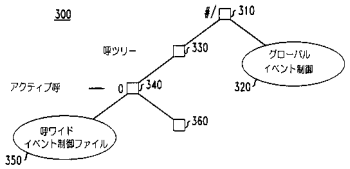
【図１】


IPネットワーク
SS7ネット
呼スイッチ
SIPデバイスサーバ
SS7デバイスサーバ
トランクゲートウェイ
ユーザ機能アプレット
H323デバイスサーバ
アクセスゲートウェイ
ディレクトリ
ディレクトリコーディネータ
呼コーディネータ
ポリシーサーバ
ナビゲーションアプレット

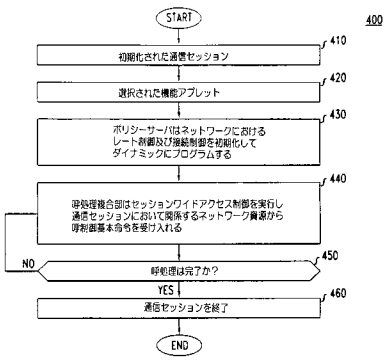
【図２】


200
#/
210
0
250
ユーザ
240
データ
230
イベント制御
220

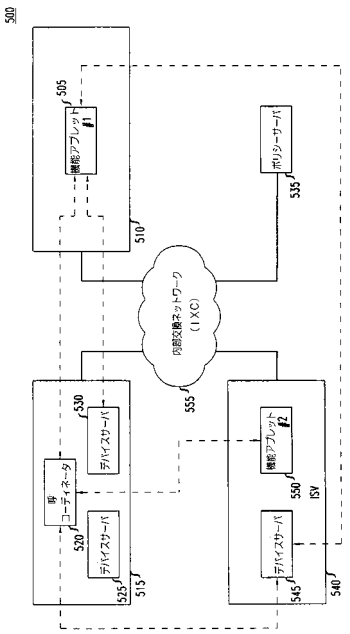
【図３】


300
#/
310
呼ツリー
330
グローバルイベント制御
320
アクティブ呼
0
340
360
呼ワイドイベント制御ファイル
350

【図４】


START
400
初期化された通信セッション
410
選択された機能アプレット
420
ポリシーサーバはネットワークにおける
レート制御及び接続制御を初期化して
ダイナミックにプログラムする
430
呼処理複合部はセッションワイドアクセス制御を実行し
通信セッションにおいて関係するネットワーク資源から
呼制御基本命令を受け入れる
440
NO
呼処理は完了か？
450
YES
通信セッションを終了
460
END

【図５】


500
機能アプレット#1
505
ポリシーサーバ
535
510
内部交換ネットワーク
(IXC)
555
呼コーディネータ
520
デバイスサーバ
530
デバイスサーバ
525
515
機能アプレット#2
550
ISV
デバイスサーバ
545
540

フロントページの続き

(74)代理人 100096943
弁理士 臼井 伸一
(74)代理人 100091889
弁理士 藤野 育男
(74)代理人 100101498
弁理士 越智 隆夫
(74)代理人 100096688
弁理士 本宮 照久
(74)代理人 100102808
弁理士 高梨 憲通
(74)代理人 100104352
弁理士 朝日 伸光
(74)代理人 100107401
弁理士 高橋 誠一郎
(74)代理人 100106183
弁理士 吉澤 弘司
(74)代理人 100081053
弁理士 三俣 弘文
(72)発明者 ムラリ アラバムダン
アメリカ合衆国、０７９７４ ニュージャージー、ムレイ ヒル、マーサー ロード ６
(72)発明者 シャミム エー．ナクビ
アメリカ合衆国、０７９６０ ニュージャージー、モリスタウン、スプリング バレイ ロード １９

審査官 吉村 伊佐雄

(56)参考文献 特開平１１－１１２５０３（ＪＰ，Ａ）
特開平１１－３４１０５３（ＪＰ，Ａ）
特開平１１－３５３２５８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 12/00-12/26、12/50-12/66、
H04M 3/00、 3/16- 3/20、 3/38- 3/58、
7/00- 7/16、11/00-11/10、
H04W 40/34