(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4076974号
(P4076974)
(45)発行日　平成20年4月16日(2008.4.16)　(24)登録日　平成20年2月8日(2008.2.8)

(51)Int.Cl.　F I
H04L 12/56 (2006.01)　H04L 12/56　400Z
H04L 12/28 (2006.01)　H04L 12/28　200M

請求項の数 27　外国語出願　(全 27 頁)

(21)出願番号　特願2004-151668 (P2004-151668)
(22)出願日　平成16年5月21日 (2004.5.21)
(65)公開番号　特開2004-350296 (P2004-350296A)
(43)公開日　平成16年12月9日 (2004.12.9)
審査請求日　平成17年1月21日 (2005.1.21)
(31)優先権主張番号　60/472549
(32)優先日　平成15年5月21日 (2003.5.21)
(33)優先権主張国　米国(US)

前置審査

(73)特許権者　504090400
イクシア
アメリカ合衆国・カリフォルニア州　９１３０２・カラバサス・ダブリュー　アグーラ　ロード　２６６０１
(74)代理人　110000176
一色国際特許業務法人
(72)発明者　ディエゴ　デュガトキン
アメリカ合衆国・カリフォルニア州　９１３０２・カラバサス・ダブリュー　アグーラ　ロード　２６６０１　イクシア内
(72)発明者　クリフォード　ハンネル
アメリカ合衆国・カリフォルニア州　９１３０２・カラバサス・ダブリュー　アグーラ　ロード　２６６０１　イクシア内
最終頁に続く

(54)【発明の名称】ネットワーク・トラフィックの自動特性記述

(57)【特許請求の範囲】
【請求項１】
観測される製品ネットワーク・トラフィックに基づいて出力ネットワーク・トラフィックを自動的に生成するためのシステムであって、
ネットワーク・トラフィックを自動的に取り込み、ネットワーク・トラフィック・データを編集するためのデータ・コレクターと、
前記ネットワーク・トラフィックおよび前記ネットワーク・トラフィック・データに基づいてネットワーク・トラフィック特性記述データを自動的に作成するための特性記述エンジンと、
前記ネットワーク・トラフィック特性記述データに基づいて、特定の種類のネットワーク・トラフィックを生成するための複数のスクリプトを、前記種類ごとに自動的にユーザーの介在なしで作成するためのスクリプト・ジェネレーターと、
前記複数のスクリプトによってモデル化された異なるタイプのネットワーク・トラフィックを表すデータ単位のグループを多重化して、前記出力ネットワーク・トラフィックを自動的に生成するためのトラフィック・ジェネレーターと、
を含むシステム。
【請求項２】
前記ネットワーク・トラフィック特性記述データが、ネットワーク・トラフィックの統計、トラフィック・モデルおよびトラフィック・プロファイル・データを含み、
前記特性記述エンジンが、

前記ネットワーク・トラフィック・データに基づいて、前記ネットワーク・トラフィックの統計を作成するための整列・統計エンジンと、
前記ネットワーク・トラフィックの統計に基づいて、前記トラフィック・モデルを作成するためのモデル化エンジンと、
前記システムに格納された前記トラフィック・モデルおよびトラフィックの原型に基づいて前記トラフィック・プロファイル・データを生成するためのトラフィック・プロファイラと、を含んでいる、請求項１に記載のシステム。
【請求項３】
前記コレクターが、フィルターに基づいて前記ネットワーク・トラフィックをフィルターし、かつ統一された書式の要求仕様に基づいて前記ネットワーク・トラフィックを変換するように構成されている、請求項１に記載のシステム。
【請求項４】
前記フィルターが、ユーザーが設定したものおよびシステムが設定したもののうちの少なくとも一方であり、送信元アドレス、宛先アドレス及び通信プロトコルを含むグループのうち１つ以上に基づいている請求項３に記載のシステム。
【請求項５】
前記特性記述エンジンが、前記ネットワーク・トラフィック・データと前記統計指標との公表することが適当でない情報を削除するように構成されている、請求項１に記載のシステム。
【請求項６】
公表することが適当でない情報を削除することが、個人識別情報、パスワード、銀行口座番号、およびクレジットカード情報のうちの少なくとも１つを削除することを含む、請求項５に記載のシステム。
【請求項７】
前記ネットワーク・トラフィック・データが、プロトコル分布データ、長さ分布データ、トランザクション分布データ、ヘッダー情報、およびペイロード・データのうちの少なくとも１つを含む、請求項１に記載のシステム。
【請求項８】
前記特性記述エンジンが、前記トラフィック・モデルをユーザーが編集できるようにするためのモデル微調整ユニットを含む、請求項２に記載のシステム。
【請求項９】
前記特性記述エンジンが、前記トラフィック・プロファイル・データをユーザーが編集できるようにするためのプロファイル編集ユニットを含む、請求項２に記載のシステム。
【請求項１０】
前記データ・コレクターが、前記システムがサポートする複数の通信プロトコルのそれぞれに対して、少なくとも１つのデータ収集ユニットを含む、請求項１に記載のシステム。
【請求項１１】
前記スクリプト・ジェネレーターが、前記システムがサポートする複数の通信プロトコルのそれぞれに対して、少なくとも１つのスクリプト作成ユニットを含む、請求項１に記載のシステム。
【請求項１２】
前記トラフィック・ジェネレーターが、前記システムがサポートする複数の通信プロトコルのそれぞれに対して、少なくとも１つのトラフィック生成ユニットを含む、請求項１に記載のシステム。
【請求項１３】
前記システムが、複数の通信プロトコルをサポートする、請求項１に記載のシステム。
【請求項１４】
前記複数の通信プロトコルには、少なくとも、イーサネット、ユーザ・データグラム・プロトコル（ＵＤＰ）、伝送制御プロトコル（ＴＣＰ）、およびハイパーテキスト転送プ

ロトコル（ＨＴＴＰ）が含まれる、請求項１３に記載のシステム。
【請求項１５】
観測される製品ネットワーク・トラフィックに基づいて、出力ネットワーク・トラフィックを自動的に生成するためのシステムであって、
ネットワーク・トラフィックを自動的に取り込み、ネットワーク・トラフィック・データを編集するためのデータ・コレクターと、
前記ネットワーク・トラフィック・データに基づいて、ネットワーク・トラフィックの統計を自動的に作成するための整列・統計エンジンと、
前記ネットワーク・トラフィックの統計に基づいて、トラフィック・モデルを自動的に作成するためのモデル化エンジンと、
前記トラフィック・モデルおよび前記システムに格納されたトラフィックの原型に基づいて、トラフィック・プロファイル・データを自動的に作成するためのトラフィック・プロファイラと、
前記トラフィック・プロファイル・データに基づいて、特定の種類のネットワーク・トラフィックを生成するための複数のスクリプトを、前記種類ごとに自動的にユーザーの介在なしで作成するためのスクリプト・ジェネレーターと、
前記複数のスクリプトによってモデル化された異なるタイプのネットワーク・トラフィックを表すデータ単位のグループを多重化して、前記出力ネットワーク・トラフィックを生成するためのトラフィック・ジェネレーターと、を含むシステム。
【請求項１６】
前記データ・コレクターが、フィルターに基づいて前記ネットワーク・トラフィックをフィルターし、かつ統一された書式の要求仕様に基づいて前記ネットワーク・トラフィックを変換するように構成されている、請求項１５に記載のシステム。
【請求項１７】
前記モデル化エンジンが、前記ネットワーク・トラフィック・データと前記統計指標との公表することが適当でない情報を削除するように構成されている、請求項１５に記載のシステム。
【請求項１８】
公表することが適当でない情報を削除することが、個人識別情報、パスワード、銀行口座番号、およびクレジットカード情報のうちの少なくとも１つを削除することを含む、請求項１５に記載のシステム。
【請求項１９】
前記ネットワーク・トラフィック・データが、プロトコル分布データ、長さ分布データ、トランザクション分布データ、ヘッダー情報、およびペイロード・データのうちの少なくとも１つを含む、請求項１５に記載のシステム。
【請求項２０】
前記モデル化エンジンが、前記トラフィック・モデルをユーザーが編集できるようにするためのモデル微調整ユニットを含む、請求項１５に記載のシステム。
【請求項２１】
観測される製品ネットワーク・トラフィックに基づいて出力ネットワーク・トラフィックを自動的に生成するための方法であって、
製品ネットワーク・トラフィックを取り込むステップと、
前記ネットワーク・トラフィックに基づいてネットワーク・トラフィック・データを編集するステップと、
前記ネットワーク・トラフィックおよび前記ネットワーク・トラフィック・データに基づいて、ネットワーク・トラフィック特性記述データを作成するステップと、
前記ネットワーク・トラフィック特性記述データに基づいて、特定の種類のネットワーク・トラフィックを生成するための複数のスクリプトを、前記種類ごとに自動的に作成するステップと、
前記複数のスクリプトによってモデル化された異なるタイプのネットワーク・トラフィ

ックを表すデータ単位のグループを多重化して、前記出力ネットワーク・トラフィックを生成するステップと、を含む方法。

【請求項２２】

前記ネットワーク・トラフィック特性記述データが、ネットワーク・トラフィックの統計、トラフィック・モデルおよびトラフィック・プロファイル・データを含み、

ネットワーク・トラフィック特性記述データを作成するステップが、

前記ネットワーク・トラフィック・データに基づいて前記ネットワーク・トラフィックの統計を作成するステップと、

前記ネットワーク・トラフィックの統計に基づいて前記トラフィック・モデルを作成するステップと、

前記トラフィック・モデルとシステムが用意するトラフィックの原型とに基づいて前記トラフィック・プロファイル・データを作成するステップと、を含む、請求項２１に記載の方法。

【請求項２３】

前記ネットワーク・トラフィックを取り込むステップが、フィルターに基づいて前記ネットワーク・トラフィックをフィルターするステップを含み、

前記ネットワーク・トラフィック・データを編集するステップが、統一された書式の要求仕様に基づいて前記ネットワーク・トラフィックを変換するステップを含む、請求項２１に記載の方法。

【請求項２４】

製品ネットワーク・トラフィックに基づいて出力ネットワーク・トラフィック・スクリプトを自動的に作成するためのシステムであって、

前記製品ネットワーク・トラフィックに基づいてネットワーク・トラフィック・データを受信するためのコレクターと、

前記ネットワーク・トラフィック・データに基づいてネットワーク・トラフィック特性記述を作成するための特性記述エンジンと、

前記ネットワーク・トラフィック特性記述に基づいて、特定の種類のネットワーク・トラフィックを生成するための複数のスクリプトを、前記種類ごとに自動的にユーザーの介在なしで作成するためのスクリプト・ジェネレーターと、を含むシステム。

【請求項２５】

前記ネットワーク・トラフィック特性記述が、ネットワーク・トラフィックの統計、トラフィック・モデルおよびトラフィック・プロファイル・データを含み、

前記特性記述エンジンが、

前記ネットワーク・トラフィック・データに基づいて、前記ネットワーク・トラフィックの統計を作成するための整列・統計エンジンと、

前記ネットワーク・トラフィックの統計に基づいて、前記トラフィック・モデルを作成するためのモデル化エンジンと、

前記システムに格納された前記トラフィック・モデルおよびトラフィックの原型に基づいて前記トラフィック・プロファイル・データを生成するためのトラフィック・プロファイラと、を含んでいる、請求項２４に記載のシステム。

【請求項２６】

前記データ・コレクターが、前記システムがサポートする複数の通信プロトコルのそれぞれに対して、少なくとも１つのデータ収集ユニットを含む、請求項２４に記載のシステム。

【請求項２７】

前記コレクターが、ネットワーク・トラフィックを取り込み、該取り込まれたネットワーク・トラフィックに基づいて追加のネットワーク・トラフィック・データを編集するように構成されている、請求項２４に記載のシステム。

【発明の詳細な説明】

【技術分野】

【０００１】
本発明は、ネットワークおよびネットワーク・トラフィックに関係する。
【背景技術】
【０００２】
<<関連出願情報>>
本出願は、２００３年５月２１日に出願された米国仮出願第６０／４７２，５４９号の利益を主張するものであり、それを本明細書に援用する。本出願は、２００３年８月２１日に出願された「実世界トラフィック（REAL WORLD TRAFFIC）」と称する米国特許出願に関連している。
【０００３】
<<関連技術の説明>>
インターネットのようなネットワークは、サーバ、ルータ、ハブ、スイッチ、および他のデバイスを含む、様々なネットワーク・デバイスを使用して通信される様々なデータを提供する。ネットワークを使用する前に、ネットワーク（そこに含まれるネットワーク・デバイスを含む）は、正常動作を確実にするために、試験されることがある。ネットワーク・デバイスは、例えば、それらが目的通りに機能し、サポートされるプロトコルに準拠し、予測されるトラフィックの要求に耐えられることを確実にするために、試験されることがある。
【０００４】
ネットワークおよびネットワーク・デバイスの構築、設置およびメンテナンスを補助するために、ネットワークは、ネットワーク解析装置、ネットワーク適合システム、ネットワーク・モニタリング装置、およびネットワーク・トラフィック・ジェネレーター（全て本明細書ではネットワーク試験システムと呼ぶ）を用いて拡張することができる。ネットワーク試験システムは、ネットワーク通信を送ること、取り込むことおよび／または解析することができるようにする。
【０００５】
現在のネットワーク・トラフィック解析ツールおよびトラフィック生成システムは、別個の構成要素として存在している。ネットワーク・データを収集して解析するためのいくつかの技術が存在する。これらの技術には、記録されたデータを直接再生することや、パケット・ベースのトラフィックを合成して生成することが含まれる。現在のシステムは、統計的解析およびモデル化と、自動スクリプト作成およびトラフィック生成機能とを兼ね備えてはいない。
【０００６】
いくつかのネットワーク試験システムでは、ネットワーク・トラフィック・データを収集、解析およびモデル化する作業、そのネットワーク・トラフィック・データに基づいてスクリプトを作成する作業、および合成ネットワーク・トラフィックを生成する作業には、広範囲に渡って人の関与が必要とされている。この労働集約的な作業には、多くの製品を使用する技術を身につけた高度に訓練された人員が必要とされる。現在のネットワーク試験システムのユーザーは、試験プロセスを通して使用される、システムの独立した構成要素のそれぞれの入出力仕様を理解しなければならない。ネットワーク試験用にいくつかの製品を使用する不便さは、試験プロセス中のいくつもの段階での人為的なミスの危険性により悪化する。現在のネットワーク試験システムを使用することから生じるミス、現在のネットワーク試験システムを運営しまたは管理し、あるいはそれら両方を行うのに必要とされる人員、および現在のネットワーク試験システムを動作させるのに要求される人員が、結果として大きな運営コストの原因となる。加えて、人がもたらすミスを減らしかつユーザーに要求される知識を減らす目的で現在のネットワーク試験システムを単純化する際には、現在のネットワーク試験システムの機能は削減されてきた。
【発明を実施するための最良の形態】
【０００７】
<<発明の詳細な説明>>

本明細書全体を通して、示した実施形態および実施例は、特許が請求される構成要素を限定するものではなく、代表例として考えられるべきである。

【０００８】

本明細書に記載されているように、ネットワーク・トラフィックの統計的解析および統計収集、ネットワーク・トラフィックのモデル化、ネットワーク・トラフィック・スクリプトの作成またはネットワーク・トラフィックの生成あるいはその両方を自動化し、ネットワークの試験、ネットワーク装置の試験およびネットワーク・アプリケーションの試験へのユーザーの関与を減少させ、それらの試験を改善する。このネットワークの解析、モデル化およびプロファイリングは、ネットワークにおける実トラフィックの挙動を統計的に反映するネットワーク・トラフィック・スクリプトまたはネットワーク・トラフィックあるいはそのいずれもを自動的に生成することを可能にする。

【０００９】

<<環境>>

図１を参照すると、本発明による環境のブロック図が示してある。この環境は、専用線またはネットワーク１５０を介して互いに結合されたネットワーク試験シャーシー１１０および１２０と、複数のネットワーク対応デバイス１３０と、ネットワーク試験シャーシーのそれぞれを結合しうるネットワーク１４０と、を含んでいる。

【００１０】

ネットワーク１４０は、ローカルエリアネットワーク（ＬＡＮ）、ワイドエリアネットワーク（ＷＡＮ）、ストレージエリアネットワーク（ＳＡＮ）、またはこれらの組合せでもよい。ネットワーク１４０は、有線、無線、またはこれらの組合せでもよい。ネットワーク１４０は、インターネットを含んでもまたはそのものでもよい。ネットワーク１４０は、公衆のものでも私設のものでもよく、さらには分離された試験ネットワークでもよい。ネットワーク１４０は、データが移動する多数の物理的および論理的経路を与える多数のノードを備えてもよい。

【００１１】

ネットワーク１４０での通信は、フレーム、セル、データグラム、パケットまたは他の情報単位を含む様々な形態を取ることができ、それら全てを本明細書中でデータ単位と呼ぶ。ネットワーク試験システム１００およびネットワーク対応デバイス１３０は互いに同時に通信することができ、所与のネットワーク対応デバイス１３０を用いたネットワーク試験シャーシー１１０と１２０の間に複数の論理的通信リンクがあってもよい。ネットワーク上で通信されるそれらのデータ単位を、本明細書中でネットワーク・トラフィックと呼ぶ。

【００１２】

ネットワーク試験シャーシー１１０および１２０は、トラフィック・ジェネレーター、性能解析装置、適合性確認システム、ネットワーク解析装置、ネットワーク管理システム、またはその他のものあるいはいずれものうちの１つ以上を含んでもまたはそのものでもよい。ネットワーク試験シャーシーは、例えば各バージョンのLinux（登録商標）、Unix（登録商標）およびMicrosoft Windows（登録商標）等のオペレーティング・システムを有してもよい。ネットワーク試験シャーシー１１０および１２０は、１枚以上のネットワーク・カード１１４および１２４と、バックプレーン１１２および１２２とを含んでもよい。ネットワーク試験シャーシー１１０および１２０、または１枚以上のネットワーク・カード１１４および１２４、あるいはそのいずれもは、１つ以上の接続１１８および１２８を介してネットワーク１４０に結合してもよい。接続１１８および１２８は、有線でも無線でもよい。ネットワーク試験シャーシー１１０および１２０は、通信のために直接互いにライン１５０を通して結合してもよい。またネットワーク試験シャーシー１１０および１２０は、ネットワーク１４０を通して互いに通信することもできる。

【００１３】

ネットワーク試験シャーシー１１０および１２０は、図１に示すようにカード・ラックの形でも、一体化されたユニットでもよい。代わりに、それぞれのネットワーク試験シャ

ーシーは、協働してトラフィック生成、トラフィックまたはネットワークあるいは両方の解析、ネットワーク適合性試験、および他の作業を提供するための、複数の独立したユニットを備えてもよい。

【００１４】

ネットワーク試験シャーシー１１０および１２０と、ネットワーク・カード１１４および１２４とは、例えば、ユーザ・データグラム・プロトコル（ＵＤＰ）、伝送制御プロトコル（ＴＣＰ）、インターネット・プロトコル（ＩＰ）、インターネット制御メッセージ・プロトコル（ＩＣＭＰ）、ハイパーテキスト転送プロトコル（ＨＴＴＰ）、アドレス解決プロトコル（ＡＲＰ）、逆アドレス解決プロトコル（ＲＡＲＰ）、ファイル転送プロトコル（ＦＴＰ）、簡易メール転送プロトコル（ＳＭＴＰ）等の、１つ以上の周知の高レベル通信規格またはプロトコルをサポートすることができ、さらに、例えば、１０ギガビット・イーサネット規格、ファイバ・チャネル規格、および１つ以上のさまざまなＩＥＥＥ802イーサネット規格、非同期転送モード（ＡＴＭ）、Ｘ．２５、統合サービスデジタル通信網（ＩＳＤＮ）、トークンリング、フレーム・リレー、ポイントツーポイント・プロトコル（ＰＰＰ）、光ファイバ分散データ・インターフェイス（ＦＤＤＩ）等の、１つ以上の周知の低レベル通信規格またはプロトコルをサポートすることができ、独自のプロトコルをサポートすることができ、さらに他のプロトコルをサポートすることもできる。

【００１５】

ネットワーク・カードという用語は、ライン・カード、テスト・カード、解析カード、ネットワーク・ライン・カード、ロード・モジュール、インターフェイス・カード、ネットワーク・インターフェイス・カード、データ・インターフェイス・カード、パケット・エンジン・カード、サービス・カード、スマート・カード、スイッチ・カード、リレー・アクセス・カード、ＣＰＵカード、ポート・カード等を包含している。ネットワーク・カードは、ブレードと呼ぶこともある。ネットワーク・カード１１４および１２４は、１つ以上のコンピュータ・プロセッサー、フィールド・プログラマブル・ゲート・アレイ（ＦＰＧＡ）、特定用途向け集積回路（ＡＳＩＣ）、プログラマブル論理回路（ＰＬＤ）、プログラマブル論理アレイ（ＰＬＡ）、プロセッサーおよび他の種類のデバイスを含んでもよい。ネットワーク・カードは、例えばランダム・アクセス・メモリ（ＲＡＭ）等の記憶装置を含んでもよい。加えて、ネットワーク・カード１１４および１２４は、ソフトウェアまたはファームウェアあるいはそれらいずれもを含んでもよい。

【００１６】

ネットワーク試験システム１１０および１２０のそれぞれにおける少なくとも１枚のネットワーク・カード１１４および１２４は、ネットワークを通した通信を可能にする回路、チップまたはチップセットを、１つ以上のネットワーク対応デバイスとして含んでもよい。ネットワーク対応デバイスは、ネットワーク１４０を通して通信できる任意のデバイスである。ネットワーク・カード１１４および１２４は、電線、光ファイバ・ケーブル、無線でのものや別のもののこともある１つ以上の接続１１８および１２８を介してネットワーク１４０に接続することができる。接続１１８および１２８をそれぞれ１つだけ示しているが、ネットワーク試験シャーシー１１０および１２０ならびにネットワーク・カード１１４および１２４から、ネットワーク１４０との複数の接続が存在してもよい。それぞれのネットワーク・カード１１４および１２４は、単一の通信プロトコルをサポートしてもよく、複数の関連するプロトコルをサポートしてもよく、または複数の関連のないプロトコルをサポートしてもよい。ネットワーク・カード１１４および１２４は、ネットワーク試験システム１１０および１２０に恒久的に取り付けても、取り外し可能としても、またはそれらの組合せでもよい。１枚以上のネットワーク・カード１１４および１２４は、例えばあるバージョンのLinuxオペレーティング・システム等の、常駐オペレーティング・システムを有していてもよい。それぞれのネットワーク試験シャーシー１１０および１２０は、該シャーシーをコンピュータ・ワークステーションとしても機能させられるＣＰＵカードを備えてもよい。

【００１７】

バックプレーン１１２および１２２は、ネットワーク・カード１１４および１２４用のバスまたは通信媒体として機能しうる。またバックプレーン１１２および１２２は、電力をネットワーク・カード１１４および１２４に供給することもできる。

【００１８】

ネットワーク対応デバイス１３０は、ネットワーク１４０を通して通信可能などんなデバイスでもよい。ネットワーク対応デバイス１３０は、例えばワークステーション、パーソナル・コンピュータ、サーバ、ポータブル・コンピュータ、携帯情報端末（ＰＤＡ）、演算タブレット等の演算機器、例えばプリンタ、スキャナ、ファクシミリ装置等の周辺機器、例えばネットワークアタッチトストレージ（ＮＡＳ）およびＳＡＮデバイスといったディスク・ドライブを含むネットワーク対応記憶装置、さらには、例えばルータ、リレー、ファイア・ウォール、ハブ、スイッチ、ブリッジ、トラフィック・アクセラレータ、および多重化装置といったネットワーキング・装置でもよい。加えて、ネットワーク対応デバイス１３０は、例えばネットワークを通して通信可能な冷蔵庫、洗濯機等の他、住宅向けまたは業務用の暖房、換気および空調システム、アラーム・システム、ならびに、その他の装置またはシステム等の機器をも含みうる。１つ以上のネットワーク対応デバイス１３０が、試験すべきデバイスとなり得て、被試験デバイスと呼ぶことができる。

【００１９】

それぞれのネットワーク試験シャーシー１１０および１２０の他、１枚以上のネットワーク・カード１１４および１２４も、本明細書に記載された技術を実現するように動作するソフトウェアを含むことができる。本明細書中で用いられる、「ソフトウェア」という用語は、なんらかの種類のコンピュータ・プロセッサー上で実行され得る、いかなる命令をも含意するものである。このソフトウェアは、いかなるコンピュータ言語で実行してもよく、またオブジェクト・コードとして実行してもよく、アセンブリまたは機械語、これらの組合せ等でもよい。「アプリケーション」という用語は、１つ以上のソフトウェア・モジュール、ソフトウェア・ルーチンまたはソフトウェア・プログラムおよびそれらの組合せのことを意味している。「スイート」は、１つ以上のソフトウェア・アプリケーション、ソフトウェア・モジュール、ソフトウェア・ルーチンまたはソフトウェア・プログラムおよびそれらの組合せを含む。本明細書中に記載された技術は、１つ以上のアプリケーションおよびスイートの形でソフトウェアとして実施することができ、低レベルのドライバー、オブジェクト・コード、および他の低レベルのソフトウェアを含んでもよい。

【００２０】

ソフトウェアは、例えば、限定はされないが、磁気媒体（例えば、ハードディスク、テープ、フロッピーディスク）、光媒体（例えば、ＣＤ、ＤＶＤ）、フラッシュメモリ製品（例えば、メモリースティック、コンパクトフラッシュ等）、ならびに揮発性および不揮発性のシリコンメモリ製品（例えば、ランダム・アクセス・メモリ（ＲＡＭ）、プログラマブル読取り専用メモリ（ＰＲＯＭ）、電気的消去可能プログラマブル読取り専用メモリ（ＥＥＰＲＯＭ）等）といった任意のローカルまたはリモートの機械可読媒体上に記憶すること、およびそれから実行することができる。記憶装置は、機械可読媒体からの読取りまたはそれへの書込み、あるいは両方を可能にする任意のデバイスである。

【００２１】

ネットワーク試験シャーシー１１０および１２０は、それぞれパーソナル・コンピュータおよびコンピュータ・ワークステーションを含むがこれらに限定されない、ネットワーク・カードをその中に有する１つ以上の演算機器により拡張することまたはそれと置換えることができる。

【００２２】

図２は、本発明による第２の環境のブロック図である。ネットワーク試験シャーシー２１０および２２０は、専用通信回線２５２および２５４を介してコンピュータ・ワークステーション２５０に接続することができる。コンピュータ・ワークステーション２５０は、任意の演算機器であってよい。コンピュータ・ワークステーション２５０は、本明細書に記載された技術を実現するソフトウェアが記憶された記憶媒体にアクセスするための記

憶装置を含むことができる。本明細書に記載された技術を実現するソフトウェアは、ワークステーション２５０からネットワーク試験シャーシー２１０および２２０ならびにそれに含まれるネットワーク・カードへとダウンロードすることができる。ワークステーション２５０は、ネットワーク試験シャーシー２１０および２２０に物理的に隣接して設置しても遠くに設置してもよい。同様に、ネットワーク試験シャーシー２１０および２２０は、互いに物理的に隣接して設置しても遠くに設置してもよい。

【００２３】

ネットワーク試験シャーシー２１０は、１つ以上の接続２６８を介して製品ネットワーク２６０に結合できる。本明細書中で用いられる「製品ネットワーク」という用語は、立ち上がって、通常の仕事中に稼働しているネットワークを意味している。したがって、製品ネットワークは、製品ネットワーク２６０に接続される、または他の方法でそれを通して通信する他のネットワーク対応デバイス２７０のみならず、一般使用者および他の顧客のデバイスや、ウェブサーバおよびアプリケーション・サーバのようなサーバから発せられるネットワーク・トラフィックおよびそれらの間のネットワーク・トラフィックを含んでいる。ネットワーク試験シャーシー２１０は、製品ネットワーク２６０上のトラフィックを傍受し、かつ製品ネットワーク２６０からネットワーク・トラフィックを取り込み、または評価することができる。

【００２４】

ネットワーク試験シャーシー２２０は、１つ以上の接続２２８を介して試験ネットワーク２８０に結合することができる。本明細書中で用いられる「試験ネットワーク」という用語は、試験すべき任意のネットワークを意味しており、私設の分離されたネットワークや公衆アクセス可能なネットワークも含まれる。試験ネットワーク２８０は、試験されうる、被試験デバイスと呼ぶことができる１つ以上のネットワーク対応デバイス２９０を含んでもよい。ネットワーク試験シャーシー２２０は、試験ネットワーク２８０を通してネットワーク対応デバイス２９０に向けられたデータ単位を送るもしくは他の方法で伝えるすなわち通信することができる。

【００２５】

ネットワーク試験シャーシー２１０および２２０のそれぞれは、シャーシーをコンピュータ・ワークステーションとして機能させられるＣＰＵカードを備えてもよい。ハードディスク・ドライブのような記憶装置および記憶媒体を、試験シャーシー２１０および２２０に備えても、またシャーシー、ＣＰＵカードおまたはその中に含まれるネットワーク・カードあるいは両方に備えまたは結合し、あるいは備えかつ結合してもよい。

【００２６】

図３は、本発明による第３の環境のブロック図である。ネットワーク試験シャーシー３１０は、製品ネットワーク３６０上のデバイス３７０からネットワーク・トラフィックを受信し、評価し、または取り込む、あるいはおよび取り込むように通信回線３６８を介して結合することができる。ネットワーク試験シャーシー３１０は、試験ネットワーク３８０上のデバイス３９０に、ネットワーク・トラフィックを送るように通信回線３３８を介して結合することができる。

【００２７】

ネットワーク試験シャーシー３１０には、ディスプレイ３１６、およびキーボード３１２やマウス３１４といったユーザー入力デバイスの他、例えばペンやトラックボールを含む他のユーザー入力デバイス（全て、シャーシー内に備えられたＣＰＵカードに結合できる）が付属していることもありえる。ハードディスク・ドライブまたは他の記憶装置を、本明細書に記載された技術を実現するソフトウェアを格納するために、ネットワーク試験シャーシー３１０に備えてもよい。本明細書に記載された技術を実現するソフトウェアは、ＣＰＵカードからネットワーク試験シャーシー３１０に備えられたネットワーク・カードに伝えることができる。ネットワーク試験シャーシー３１０は、製品ネットワーク３６０内のデバイス３７０および試験ネットワーク３８０内のデバイス３９０に、物理的に隣接して設置しても遠くに設置してもよい。

【００２８】
<<概観>>
図４Ａは、本発明による動作ユニットの機能ブロック図である。図４Ｂは、本発明による図４Ａに示した動作ユニットでとられる動作のフローチャートである。ネットワーク試験システム４００は、ブロック４１２に示すように、ネットワーク４６０から収集されたネットワーク・トラフィックを取り込み、収集し、フィルターし、またそれに他の操作を行うためのコレクター４１０を備えることができる。コレクターは、ネットワーク・トラフィック・データを編集してもよい。コレクターは、特性記述ユニット４２０に結合し、収集およびフィルターされたネットワーク・トラフィックをそこに送り出すことができる。特性記述ユニット４２０は、ブロック４２２に示すように、収集およびフィルターされたネットワーク・トラフィックまたはネットワーク・トラフィック・データあるいは両方に対し、解析、モデル化、プロファイリング、整列、および他の操作を行い、ネットワーク・トラフィック特性記述を作成することができる。
【００２９】
特性記述ユニット４２０でフィードバック４７０を用い、特定の種類またはタイプのネットワーク・トラフィックに関して追加の種類またはタイプのデータをコレクター４１０が収集することを要求することができる。特性記述ユニット４２０は、ネットワーク・トラフィック・データの解析に基づいて、コレクター４１０により収集および編集されたネットワーク・トラフィック・データを自動的に調整してもよい。すなわち、特性記述ユニット４２０は、ネットワーク・トラフィックに関する追加の情報をコレクター４１０が収集または保持することを、フィードバック４７０によって要求してもよい。また特性記述ユニット４２０は、収集される情報を特定の種類またはタイプのネットワーク・トラフィックに関する情報にコレクター４１０が制限することをフィードバック４７０によって要求してもよい。特性記述ユニット４２０がネットワーク・トラフィックについての追加の情報を記憶するため、特性記述ユニット４２０は、より限られたセットまたは種類のデータ単位についてのより詳細な情報を、フィードバック４７０によって続けて要求することができる。
【００３０】
特性記述ユニット４２０は、スクリプト・ジェネレーター４３０に結合することができる。スクリプト・ジェネレーター４３０は、ブロック４３２に示すように、ネットワーク・トラフィック特性記述に基づいてトラフィック送信スクリプトを作成することができる。スクリプト・ジェネレーター４３０は、トラフィック・ジェネレーター４４０に結合することができる。トラフィック・ジェネレーター４４０は、ブロック４４２に示すように、スクリプト・ジェネレーター４３０により作成されたスクリプトにしたがって、試験ネットワーク・トラフィックをネットワーク４６０上に生成することができる。この試験ネットワーク・トラフィックは、ネットワーク４６０に結合された、または違った形でネットワーク４６０からアクセス可能であるネットワーク対応デバイスを試験するのに使用でき、またネットワーク対応デバイスに入れられたソフトウェア（アプリケーション・ソフトウェアを含む）を試験するのに使用することができる。
【００３１】
マネージャ４５０は、コレクター４１０、特性記述ユニット４２０、スクリプト・ジェネレーター４３０およびトラフィック・ジェネレーター４４０のそれぞれに結合することができる。マネージャ４５０は、収集されたネットワーク・トラフィックおよびネットワーク・トラフィック・データに関する情報、スクリプト、および他の構成要素のそれぞれによりユーザーがアクセスできるようにされた他の情報に、ユーザーがそれによってアクセスできるユーザ・インターフェイスを提供することができる。加えて、マネージャ４５０は、コレクター４１０が収集およびフィルター可能な種類またはタイプのネットワーク・トラフィックを定めるインターフェイスをユーザーに提供することができ、ユーザーがネットワーク・トラフィック特性記述を編集または拡張できるようにすることができ、ユーザーがコンパイラー４３０によって生成されたスクリプトを編集または拡張できるよう

にすることができ、またユーザーが他の作業を行うことができるようにすることができる。

【００３２】

加えて、マネージャ４５０は、トラフィック・ジェネレーター４４０の機能を知るために、トラフィック・ジェネレーター４４０に照会することができる。トラフィック・ジェネレーター４４０のトラフィック生成機能に基づいて、マネージャ４５０は、初期設定を与え、また別の方法でネットワーク・トラフィックのコレクター４１０によってシーク、収集されかつ取り込まれるネットワーク・トラフィックおよびネットワーク・トラフィック・データのスコープ、幅および深さを制御することができる。またマネージャは、トラフィック・ジェネレーター４４０の機能に基づいて、スクリプト・ジェネレーター４３０によって作成されたスクリプトのスコープ、幅および深さを制御することもできる。

【００３３】

図５は、本発明による動作ユニットの第２の機能ブロック図である。コレクター５１０は、ネットワーク５６０からネットワーク・トラフィックを取り込み、収集することができる。またコレクター５１０は、ローカルのまたはリモートのネットワーク試験システム、パケット・スニファ、および他のデバイスおよびシステムでもありえるネットワーク試験システム５００の外部の他のコレクター（不図示）から、ネットワーク・トラフィック・ファイル５１２またはネットワーク・トラフィック・データ５１４あるいは両方を受信することができる。外部コレクターは、ネットワーク・トラフィックの取込グループからのデータ単位を含むトラフィック・ファイル５１２を与えることができ、またネットワーク・トラフィックの取込グループからのデータ単位のトラフィック・データ５１４を与えることができる。加えて、コレクター５１０は、ローカルまたはリモートのネットワーク試験システム、およびサーバ、ルータ、ゲートウェイ等を含むネットワーク対応デバイスからログファイルを受信しまたは取り出し、あるいは受信しかつ取り出すことができる。コレクター５１０は、パスワード、その他ログファイルへのアクセスを認証する手段を提示することでログファイル５１６にアクセスできる。コレクター５１０は、ネットワーク・トラフィック・ファイル５１２、ネットワーク・トラフィック・データまたはログファイル５１６あるいはいずれもを直に特性記述ユニット５２０に送り出す外部コレクター（不図示）で置き換えてもよい。

【００３４】

コレクター５１０は、ネットワーク・トラフィック・データを作成し、該ネットワーク・トラフィック・データを特性記述ユニット５２０に送り出すことができる。またコレクター５１０は、ネットワーク・トラフィック・データ５１８を、ネットワーク試験システム５００に対してローカルにまたはリモートに設置可能な外部レポート・ジェネレーター５５２に、送り出すまたは他の方法でネットワーク・トラフィック・データ５１８を利用可能とさせることもできる。外部レポート・ジェネレーター５５２は、ネットワーク試験システムであることもまたはそれを含むこともある演算機器で走るソフトウェア・プログラムでもよい。外部レポート・ジェネレーター５５２は、ネットワーク試験管理者等のユーザーが、グラフィカル・ユーザ・インターフェイスまたは他のユーザ・インターフェイスによってネットワーク・トラフィック・データを視認できるようにすることができる。

【００３５】

特性記述ユニット５２０は、コレクター５１０からネットワーク・トラフィック・データを受信し、ネットワーク・トラフィックの統計およびネットワーク・トラフィック・モデルを含むネットワーク・トラフィック特性記述５２２を作成することができる。特性記述５２０は、ネットワーク・トラフィック特性記述をスクリプト・ジェネレーター５３０に送り出すまたは他の方法で利用可能とさせることができる。加えて、特性記述ユニット５２０は、ネットワーク・トラフィック特性記述５２２を外部レポート・ジェネレーター５５２に送り出すまたは他の方法で利用可能とさせることができる。外部レポート・ジェネレーター５５２は、ネットワーク試験管理者等のユーザーが、グラフィカル・ユーザ・インターフェイスまたは他のユーザ・インターフェイスによってネットワーク・トラフィ

ック特性記述を視認できるようにすることができる。

【００３６】

また特性記述ユニット５２０は、コレクター５１０で用いられるフィルターのタイプおよび種類を制御しかつ定めることもできる。そうすることによって、特性記述ユニット５２０は、コレクター５１０によって収集、取込および評価されたネットワーク・トラフィックおよびネットワーク・トラフィック・データのスコープ、幅および深さを改善することができる。上記特性記述ユニット４２０およびフィードバック４７０と同様に、フィードバック５７０を特性記述ユニット５２０で用いて、コレクター５１０がネットワーク・トラフィックの特定の種類またはタイプに関するデータを収集することを要求することができる。特性記述ユニット５２０は、ネットワーク・トラフィック・データの解析に基づき、フィードバック５７０を用いて、コレクター５１０により収集および編集されたネットワーク・トラフィック・データを自動的に調整してもよい。特性記述ユニット５２０がネットワーク・トラフィックについての追加の情報を記憶するため、特性記述ユニット５２０は、ネットワーク・トラフィックのより限られたセットまたは種類のデータ単位についてのより詳細な情報を、フィードバック５７０によって続けて要求することができる。

【００３７】

スクリプト・ジェネレーター５３０は、ネットワーク・トラフィック特性記述に基づいてネットワーク・トラフィック生成スクリプトを作成することができる。スクリプト・ジェネレーターは、ネットワーク・トラフィック生成スクリプト５３２をネットワーク試験システム５００に含まれるトラフィック・ジェネレーター５４０に送り出すまたは他の方法でネットワーク・トラフィック生成スクリプト５３２を利用可能とさせることができる。トラフィック・ジェネレーター５４０は、ネットワーク・トラフィック生成スクリプトに基づいて、ネットワーク５６０上に出力ネットワーク・トラフィックを生成し、送信することができる。またスクリプト・ジェネレーターは、ネットワーク・トラフィック生成スクリプト５３２を、ネットワーク試験システム５００に対してローカルにまたはリモートに設置可能な外部トラフィック・ジェネレーター５４２に、送り出すまたは他の方法でネットワーク・トラフィック生成スクリプト５３２を利用可能とさせることもできる。外部トラフィック・ジェネレーター５４２は、ネットワーク試験システムであることもまたはそれを含むこともある演算機器で走るソフトウェア・プログラムでもよい。トラフィック・ジェネレーター５４０は、外部トラフィック・ジェネレーター５４２で置き換えてもまたは拡張してもよい。外部トラフィック・ジェネレーター５４２は、ネットワーク・トラフィック生成スクリプト５３２に基づいて、トラフィック・ジェネレーター５４０とは独立して、ネットワーク５６０上に出力ネットワーク・トラフィックを生成し、送信することができる。

【００３８】

<<システム>>

図６は、本発明によるネットワーク試験システム６００のブロック図である。ネットワーク試験システム６００は、製品ネットワーク６０２と試験ネットワーク６５２の間に結合することができる。ネットワーク試験システムは、入力側の製品ネットワークトラフィック・シャーシー６０４および出力側の試験ネットワーク・シャーシー６５４とを含むことができる。１つ以上のシャーシー６０４および６５４に含まれるネットワーク・カードは、ネットワーク試験システム６００の機能を実現するソフトウェアを実行することができる。ネットワーク試験システム６００の機能ユニットには、１つ以上のデータ・コレクター６１２、特性記述エンジン６２０、スクリプト・ジェネレーター６３０、トラフィック・ジェネレーター６４０およびマネージャ６６０が含まれうる。

【００３９】

データ・コレクター６１２は、ネットワーク・トラフィックを評価して、製品ネットワーク６０２上のネットワーク・トラフィックに関するネットワーク・トラフィック・データを収集する。本明細書中でデータ・コレクターは、取込グループ内のネットワーク・トラフィックおよびネットワーク・トラフィック・データを評価し、取り込みまた別の方法

で取得することができる。ここで、取込グループとは、システムにより定められた期間（例えば３分、３０分、３時間）にわたって、メモリ記憶領域がいっぱいになるまで、またはユーザーもしくはシステムにより指定された閾値に達するまで収集することができる、データ単位または該データ単位に関するネットワーク・トラフィック・データのグループである。

【００４０】

ネットワーク・トラフィック・データには、収集されたネットワーク・トラフィックから選り集められたプロトコル分布データ、長さ分布データ、トランザクション分布データ、ヘッダー情報、およびペイロード・データが含まれうる。

【００４１】

プロトコル分布データは、収集されたネットワーク・トラフィック内に存在するプロトコルを一覧表にすることができる。一グループのプロトコルのそれぞれに対するデータ単位の生のカウントを、プロトコル分布データを編集するために保持しておいてもよい。簡単なヒストグラムをマネージャ６６０のビューア６７０によって示し、ネットワーク・トラフィックのプロトコル分布を図表によって示すことができる。プロトコル分布データの編集には、いろいろなデータ通信プロトコルに従って伝えられるネットワーク・トラフィックの比率を評価するために、複数の取込グループの反復する収集または反復するパスのような複数セグメントの解析を含んでもよい。

【００４２】

長さ分布データは、ネットワーク・トラフィックで収集されるデータ単位の、各プロトコルについて、あるサイズのデータ単位について、あるペースすなわち速度特性について編集することができる。トランザクション分布データは、収集されたネットワーク・トラフィックを構成するデータ単位内に含まれる最も一般的な種類またはタイプのトランザクションのカウントに基づいて編集することができる。例えば、Ｎで最も一般的なトランザクションのデータ単位を、１つ以上のプロトコル・データ単位についてカウントでき、ここでＮは４、８、１０、１６、２０、３２、またはその他の数である。送信元または宛先アドレス、ポート割当て、および他のヘッダーデータ等のヘッダー情報は、最も一般的なアドレス、ポートまたは最も一般的なヘッダー情報が保持されるように、カウントまたは保持することができる。またペイロード・データも、ネットワーク・トラフィックによって表される異なるネットワーク・アプリケーションを分類するように保持することができる。データ・コレクター６１２は、最も一般的なネットワーク・アプリケーションのカウントを保持することができる。ヘッダーまたはペイロード属性あるいは両方の特定の組合せを有するデータ単位を保持してもよい。

【００４３】

特性記述エンジン６２０によるネットワーク・トラフィックの統計的なプロファイリングを支援するために、データ・コレクター６１２は、製品ネットワーク６０２からネットワーク・トラフィックを取り込み、データ単位の数、データ単位当たりのバイト数を実時間でカウントすることができ、さらにネットワーク・トラフィックに関する他の生のデータを保持することができる。データ・コレクター６１２は、ＦＰＧＡのようなハードウェアやファームウェアにおいて、カーネル・レベルで直接ネットワーク・トラフィック・データ収集を行うことが出来る。これにより、ネットワーク・トラフィック・データの迅速な収集が可能となる。実時間データ収集は、ライン速度でまたはそれに近い速度で、実行中に統計的に妥当な情報を生成するのに利用できる。本明細書中で、ライン速度とは、ネットワーク・トラフィックが、それが伝えられているところの物理層（ＰＨＹ）を移動する速度を意味している。ワイヤ・スピードはライン速度の同義語である。

【００４４】

データ・コレクター６１２は、ネットワーク・トラフィックを構成する異なる種類のデータ単位に関するデータを取得するのにそのそれぞれを特化しうる、１つ以上のユニット、システムまたはプラグイン・モジュールから構成できる。収集されるネットワーク・トラフィックの豊富さと、その収集されたネットワーク・トラフィックから選り集められる

ネットワーク・トラフィック・データとを増加させるために、またはデータ・コレクター６１２の性能を向上させるために、あるいはその両方のために、複数のデータ収集ユニットを用いてもよい。状況によっては、トラフィック・ミックスを決定するために第１のデータ収集ユニットを最初に用い、複数の特別なデータ収集ユニットを順々に適用してもよい。複数の特別なデータ収集ユニットは、それぞれ、ネットワーク層プロトコル、アプリケーション、宛先アドレス等のような特定の特性を有するデータ単位に的を絞ることができる。また、複数のデータ・コレクター６１２を、異なる種類のデータ単位の内容を評価するのに、または同じ種類のデータ単位の異なる部分を評価するのに、並行してすなわち同時に適用することもできる。

【００４５】

複数のデータ収集ユニットを使用することで、システムの全体の複雑さを増すことになる可能性がある。単一のデータ収集ユニットでも、統計を与えるのに十分な情報を収集することができる。単純化のため、単一のデータ収集ユニットを用いてもよい。

【００４６】

データ・コレクター６１２では、製品ネットワーク６０２のネットワーク・トラフィックに含まれるデータ単位についての生の統計を収集するために、データ単位スキャナを備えた１枚以上の特別なネットワーク・カードを用いてもよい。データ単位スキャナは、ＦＰＧＡのようなハードウェアにおいて、またファームウェアにおいて、オペレーティング・システム・レベルで実行できる。データ単位スキャナによって、データ・コレクター６１２は、ライン速度でまたはそれに近い速度で、ネットワーク・トラフィックに含まれるデータ単位の複数の特性を同時に収集することができる。ネットワーク・トラフィックのこれら複数の特性は、整列・統計エンジン６２２により計算される統計の幅または深さあるいはそのいずれもを増大させるのに、またモデル化エンジン６２４によるネットワーク・トラフィックのモデル化の精度を向上させるのに利用できる。

【００４７】

フィルター６１４およびトランスレータ６１６をデータ・コレクター６１２に含めてもよい。データ・コレクター６１２が複数のデータ収集ユニットを備える場合には、データ収集ユニットのそれぞれが異なる書式で出力を示してもよい。トランスレータ６１６をデータ・コレクター６１２に含め、ネットワーク・トラフィック・データを統一された書式に変換することができる。この統一された書式のネットワーク・トラフィック・データは、データ・コレクター６１２が結合される特性記述エンジン６２０に送り出すことができる。

【００４８】

データ・コレクター６１２に含まれるトランスレータ６１６は、製品ネットワーク６０２のデータ単位が、例えばＩＰセキュリティ（ＩＰＳｅｃ）、セキュア・ソケット・レイヤー（ＳＳＬ）、トランスポート・レイヤー・セキュリティ（ＴＬＳ）等といった保護プロトコルを使用する場合に適用できる。トランスレータ６１６は、暗号化された情報を抽出し、それを適切に変換してもよい。

【００４９】

フィルター６１４は、システムが定めたものまたはユーザーが定めたものあるいはその両方でありうる。フィルター６１４は、例えば、データ単位内で指定されている送信元または宛先アドレス、プロトコル、またはその他のデータ・フィールドに基づいて、収集されたネットワーク・トラフィックを制限するためといった、様々な目的で使用できる。使用されるフィルター６１４は、トラフィック・ジェネレーター６４０の機能により導き出される。フィルター６１４は、ネットワーク・トラフィックの収集を、トラフィック・ジェネレーター６４０が送信できるような種類またはタイプのデータ単位に限定できる。データ・コレクター６１２内に含まれるすなわちその中で働く種類およびタイプのフィルター６１４は、トラフィック・ジェネレーター６４０の機能にある程度基づいて、マネージャ６６０により制御できる。またフィルター６１４は、データの収集を特定のネットワーク・トラフィック・パターンに限定するのにも使用できる。

【００５０】
マネージャ６６０は、データ・コレクター６１２で使用されるフィルターをユーザーが作成または修正あるいはいずれもできるようにするためのインターフェイスを提供できる。これは、コンピュータ端末または他の演算機器によってユーザーにユーザ・インターフェイスを提供するマネージャ６６０によって実現できる。またユーザ・インターフェイスは、データ・コレクター６１２によってまたはこれと組み合わせて提供してもよい。
【００５１】
またマネージャ６６０は、リモート・サーバ、ルータ、およびその他のネットワーク・デバイスについてのネットワーク・トラフィックに関連したデータを含むログファイルまたは他のフィールドの内容を、ユーザーが見られるようにするインターフェイスを提供することもできる。見ることができるログファイルには、サーバ・ログ、経路選択テーブルおよびログ等が含まれうる。このアクセスを実現するために、マネージャ６６０またはネットワーク試験システム６００あるいはそのいずれもでは、サーバ、ルータ、および他のネットワーク・デバイスのログを見る許可を得るためのパスワードや他の認証手段を用いてもよい。
【００５２】
特性記述エンジン６２０は、整列・統計エンジン６２２、モデル化エンジン６２４、およびトラフィック・プロファイラ６２６を含みうる。整列・統計エンジン６２２は、ネットワーク・トラフィックに関する標準化された書式のネットワーク・トラフィック・データや基本的な統計（例えば、データ単位の生のカウント、特定のプロトコル・タイプのデータ単位の生のカウント等）をデータ・コレクター６１２から受信することができ、また１セットのネットワーク・トラフィックの統計を作成することができる。
【００５３】
整列・統計エンジン６２２は、ネットワーク・トラフィックの統計をモデル化エンジン６２４に送り出すことができ、またネットワーク・トラフィックの統計をマネージャ６６０に送り出すこともできる。整列・統計エンジン６２２は、統計を集めて、トラフィック・データ解析を施し、ユーザーが読むことができる、ウェブでアクセス可能ともできるレポートを作成することができる。
【００５４】
整列・統計エンジン６２２は、マネージャ６６０、またはネットワーク・プロトコル・アナライザのような他の外部要素へのインターフェイスを提供し、ユーザーが実時間でまたは他のやり方でネットワーク・トラフィックの統計を吟味できるようにすることができる。このインターフェイスは、ＴＣＰのようなタイプのトラフィックに対してlibpcapまたはtcpdumpを用いることで、与え、または拡張することができる。整列・統計エンジン６２２は、マネージャ６６０にインターフェイスを提供し、ユーザーが応用層の情報を見られるようにすることができる。
【００５５】
モデル化エンジン６２４は、モデルの形でネットワーク・トラフィックの単一の取込グループまたは複数の取込グループの記述を作成することができる。観測されるトラフィック・パターンのモデルとしての数学的表現は、取り込んだネットワーク・トラフィックの特性記述を与える。モデル化エンジン６２４への入力は、整列・統計エンジン６２２からの一連の集められたネットワーク・トラフィックの統計である。この統計は、１つのファイル名だけを整列・統計エンジン６２２からモデル化エンジン６２４に送り出せばよいように、１つのファイルで送り出すことができる。
【００５６】
モデル化エンジン６２４の出力は、ネットワーク・トラフィックの統計から編集されたパラメータの集まりとして表すことのできる、モデルである。このパラメータには、アドレス、プロトコル、フラグ、データ単位のサイズ、ペイロードのサイズ、データ単位に含まれるアプリケーション等に関する平均標準偏差等を含む、ネットワーク・トラフィック・データに関するまたはそれから導き出される、どのような統計または他の情報も含まれ

る。モデル化エンジン６２４は、ネットワーク・トラフィックの統計に基づいてトラフィックの特性を表す、パラメータ表示モデルを抽出する。モデル化エンジン６２４は、パラメータ表示モデルをトラフィック・プロファイラ６２６に送り出す。モデル化エンジン６２４は、パラメータ表示モデルを、マネージャ６６０を介してユーザーに伝える。モデル化エンジン６２４は、ユーザーがパラメータ表示モデルをマネージャ６６０によって修正できるようにすることができる。

【００５７】

モデル化エンジンは、フィードバック６２８を介して、データ・コレクター６１２およびフィルター６１４によってネットワーク・トラフィック・データ内に含まれる情報の種類およびタイプを制御するための、また整列・統計エンジン６２２によって編集、計算される情報のスコープ、幅および深さを制御するためのフィードバック・コントローラー６２３を含んでもよい。例えば、フィードバック・コントローラー６２３は、最初に全てのトランスポート層（レイヤ３）データ単位を要求し、それから全てのＴＣＰデータ単位を要求し、それから全てのＨＴＴＰデータ単位を要求し、等々によって、ネットワーク・トラフィックに関する取り出されるべき情報を連続的に改善することができる。このようにして、データ・コレクター、フィルター６１４、および整列・統計エンジン６２２によって取り込まれ、収集されおよび解析されるネットワーク・トラフィック・データの細分性を一連の取込グループ内で増加させることができる。他の連続的な改善は、フィードバック・コントローラー６２３内に含まれるまたはそれに与えられる、システムが定めた命令またはユーザーが定めた命令あるいは両方に基づいて実現できる。

【００５８】

モデル化エンジン６２４は、実際のトラフィックの、パラメータ表示モデルを表現するプロセスに含まれる様々な変数およびパラメータを、ユーザーが調節できるようにするモデル微調整ユニット６２５を含んでもよい。

【００５９】

モデル化エンジン６２４は、全ての私的で微妙な内容の情報をデータから削除することによって、ネットワーク・トラフィックに関してそれが保持している全ての情報の好ましくない部分を削除することができる。例えば、パスワード、ユーザー名、バンキング情報、クレジットカード番号、社会保障番号等といった私的で微妙な内容のデータを、モデル化エンジン６２４によって削除することができる。またモデル化エンジン６２４は、例えばＩＰアドレス、ポート番号、ペイロード・データ等を含む、ネットワーク・トラフィック・データおよびネットワーク・トラフィック・モデルからの他のどんな識別情報をも削除することもできる。

【００６０】

モデル化エンジン６２４は、観測されるトラフィックの特性を記述するネットワーク・トラフィックのパラメータ表示モデルを構築することができる。パラメータ表示モデルは、ネットワークの特定のレイヤに限定することができる。これは、例えば、ネットワークのレイヤ７（アプリケーション層であることもある）に、ネットワーク層であることもあるネットワークのレイヤ３に、等々でありうる。ネットワーク・トラフィックの複数のレイヤは、例えば、ＯＳＩモデルのレイヤ３、４および７、すなわちネットワーク層、トランスポート層、およびアプリケーション層、のように、パラメータで表すことができる。

【００６１】

モデル化エンジン６２４を提供する際、詳細さのレベル、およびネットワーク・トラフィックのパラメータ表示モデルを作成するのに用いられる自由度の数は、ネットワーク試験システム６００の能力に影響されうる。ネットワーク試験システムの、現在および未来のハードウェアの他、現在および未来のデバイスで走るソフトウェアを用いてトラフィックを生成する能力を、モデル化エンジン６２４により参照されるべきパラメータの数および対応する精密さのレベルを選ぶ際に、考慮に入れることができる。すなわち、ネットワーク・トラフィックのパラメータ表示モデルにモデル化エンジン６２４によって含められるパラメータの種類およびタイプは、トラフィック・ジェネレーター６４０の機能にある

程度基づいてマネージャ６６０によって制御できる。

【００６２】

モデル化エンジン６２４は、基本モデル、数学的モデル等を含む、異なる種類のパラメータ表示モデルを作成することができる。

【００６３】

基本モデルには、ネットワーク・トラフィックのプロトコル分布と、ネットワーク・トラフィックに含まれるデータ単位内の各送信元アドレスに対しての、ネットワーク・トラフィックのデータ単位内の特定のフィールド（およびサブフィールド、あるいはまたはサブフィールド）の選ばれたグループとが含まれうる。また基本モデルは、ネットワークの特定の地点からくるトラフィックを記述することもできる。基本モデルの一例には、所与の送信元アドレスについての、パケットサイズ分布に加えて、出力トランスポート層すなわちＩＰパケットの数、ＩＰプロトコルの多変量分布、ポート、フラグ等が含まれうる。他に、基本モデルのアプローチには、単一の送信元アドレスから発した全てのパケットに関する統計を有しうる統計を各ユーザーに対して記述することが必要となることがある。

【００６４】

数学的モデルは、ネットワーク・トラフィックのミックスに対する多項式表現を用いることで得られうる。様々な曲線のフィッティング技法のいずれもが、ネットワーク・トラフィックのミックスの表現を多項方程式として作成するのに利用できる。ネットワーク・トラフィックのミックスに対する多項式表現は、パレート分布、ガウス分布、減衰指数関数分布、および他の技法を用いて作成できる。例えばデータ単位サイズ分布、期間内データ単位、データ単位レイヤ分布、データ単位内に含まれるアプリケーション分布、データ単位プロトコル分布等を含む、ネットワーク・トラフィックの様々な属性を表すのに、複数の数学的モデルを用いることができる。複合数学的モデルは、ネットワーク・トラフィックの複数の属性を考慮に入れることができる。

【００６５】

トラフィック・プロファイラ６２６は、パラメータの形でネットワーク・トラフィック・モデルをモデル化エンジン６２４から受信する。トラフィック・プロファイラ６２６は、モデル化エンジン６２４により作成されたモデルを、トラフィックの原型の形の所定のトラフィック・パターンと照合する。トラフィック・プロファイラ６２６は、パラメータ表示モデルと利用可能なトラフィック原型ミックスとの比較に基づいて、トラフィック・プロファイル・スキーマを作成することができる。例えば財務ミックス、製造ミックス、インターネット・バックボーン・ミックス、およびその他のパターンを含む、トラフィックの原型として予め定めることができる多くの可能なトラフィック・ミックスがある。さらなるトラフィックの原型は、申し出のあった顧客、研究室、および他の出所から得ることができる。トラフィックの原型を集めることの利益には、ユーザーの対応する産業区分またはネットワーク・タイプに対して対応する原型を用いることで、ネットワーク試験システムをネットワーク・トラフィック・ミックスに迅速に擬することができるということが含まれる。

【００６６】

トラフィック・プロファイラ６２６は、プロファイル・エディタ６２７を含むことができる。プロファイル・エディタ６２７は、ユーザーが、トラフィック・ミックスおよびネットワーク・トラフィック・プロファイルの変動をよりよく表すように、トラフィックの原型およびトラフィック・プロファイル・スキーマを修正および調節できるようにすることができる。

【００６７】

スクリプト・ジェネレーター６３０は、トラフィック・プロファイラ６２６により作成されたトラフィック・プロファイル・スキーマを受信し、トラフィック・ジェネレーター６４０がネットワーク・トラフィックを生成するのに用いる複数のスクリプトを作成する。スクリプト・ジェネレーター６３０は、別々の個々のコンパイラーをそれぞれ含む１つ以上のプラグイン、モジュールまたはサブユニットを含んでもよい。それぞれのスクリプ

ト作成コンパイラーは、特定の種類のネットワーク・トラフィックを生成するために特定のタイプのスクリプトを作成できる。スクリプト・ジェネレーターのプラグインは、例えば、ＴＣＰやＨＴＴＰのようなステートレス・ストリーム、パーフスタック（perfstack）やフルスタック（fullstack）等を含む様々な種類のネットワーク・トラフィックに対するスクリプトを作成するのに特化することができる。スクリプト・ジェネレーター・プラグインは、加えることも削除することもできる。それぞれのサポートされたネットワーク通信プロトコルに対して１つのスクリプト作成コンパイラーが存在しうる。

【００６８】

トラフィック・ジェネレーター６４０は、スクリプト・ジェネレーター６３０によって作成されたスクリプトの集合を入力として受け取る。トラフィック・ジェネレーター６４０は、スクリプトによって記述された一連のデータ単位の形で、出力としてネットワーク・トラフィックを生成できる。一連のネットワーク・トラフィックは、１つのストリームであってもよい。ストリームは、何らかの一連の関連するパケットであってもよい。一連のネットワーク・トラフィックは、試験ネットワーク６５２内に送出される。

【００６９】

またトラフィック・ジェネレーター６４０は、データ単位の複数の連なりおよび複数のストリームを生成することもできる。トラフィック・ジェネレーター６４０は、ストリーム多重スケジューラのようなスケジューラを含むことができる。スケジューラは、様々なストリームを、またはその他の、複数のスクリプトによってモデル化された異なるタイプのネットワーク・トラフィックを表すデータ単位のグループを多重化できる。スケジューラは、どんな数のストリームを、またはその他の、ネットワーク・トラフィックのグループを連係して働かせてもよい。例えば、１６０個の別個のストリームを、生成されたネットワーク・トラフィックとして集約してもよい。

【００７０】

データ単位のタイプの数が、例えば１２８、１６０、２５６等といった、システムが定めた最大値よりも大きい場合には、複数のスクリプトを、データ単位のタイプの数を減らすように解析し、そうして試験ネットワーク・トラフィックの分解能を下げることができる。すなわち、複数のスクリプトに含まれるものよりも少ないタイプのデータ単位が送出される。

【００７１】

マネージャ６６０は、入力ネットワーク・トラフィックのデータ単位ミックス、製品ネットワーク６０２の全体のスループット、製品ネットワーク６０２に見られるアプリケーション・スループット、ならびに、製品ネットワーク６０２および該製品ネットワーク６０２を占めるネットワーク・トラフィックの他の特性を記述する、レポート、グラフィック、およびチャートを作成できる。

【００７２】

マネージャ６６０は、１つ以上のデータ・コレクター６１２、整列・統計エンジン６２２、モデル化エンジン６２４およびトラフィック・プロファイラ６２６といった、複数の出所からの情報を受信できる。マネージャ６６０は、１つ以上のデータ・コレクター６１２、整列・統計エンジン６２２、モデル化エンジン６２４およびトラフィック・プロファイラ６２６から、統計データおよび他のデータを受信できる。マネージャ６６０は、人間の使用または機械での使用のために、統計データの書式を設定することができる。マネージャ６６０は、統計データの書式を設定し、それを表示のために整えかつ統計データを出力のために適当な書式に整える、あるいはそれを表示のために整えまたは統計データを出力のために適当な書式に整えることができる。加えて、マネージャ６６０は、ユーザーがリモート・サーバ上のサーバ・ログの内容を見られるようにするインターフェイスを提供できる。

【００７３】

本明細書に記載した全てのネットワーク試験システムについて、追加のあるいはより少ない、ユニット、シャーシー、ブロック、通信回線、モジュールまたは他のソフトウェア

、ハードウェア、ファームウェアおよびデータ構造の配置が、本明細書に記載したシステムおよび技術を実現するのに使用可能である。

【００７４】

<<方法>>

図７は、本発明による方法のフローチャートである。ブロック７１０に示すように、データ単位はネットワークから収集できる。ネットワークは代表的には製品ネットワークである。ブロック７１４に示すように、データ単位はフィルターされる。このフィルタリングは、システムが定めたものまたはユーザーが定めたものあるいはいずれもでありうるフィルターによってなされうる。このフィルターは、データ単位のサイズ、データ単位のレイヤ、データ単位を送るアプリケーション、データ単位に含まれるプロトコル、データ単位の送信元または宛先アドレスあるいは両方、データ単位内で指定されたポート、データ単位内で指定されたフラグ等といった特定の特性に基づくデータ単位の収集および評価を限定することができる。それぞれの収集されたデータ単位から適切な情報を取得し、ネットワーク・トラフィック・データとして保存する（ブロック７１６に示す）。適切な情報は、該適切な情報をそのそれぞれが様々な書式で格納できる、様々なプラグイン、モジュールまたはユニットによって取得できる。ブロック７２０に示すように、データ単位のそれぞれに対する適切な情報は、それから、統一された書式に変換される。それから、ブロック７２４に示すように、ネットワーク・トラフィックに対する統計が編集される。

【００７５】

ブロック７３０に示すように、ネットワーク・トラフィック・データは、データ単位の分布を整列して割り出すことができる。ネットワーク・トラフィックの分布は、データ単位のサイズ、データ単位のプロトコル・タイプ、データ単位のレイヤ、データ単位のアプリケーション、および他のデータ単位の属性によって評価できる。ブロック７３４に示すように、収集されたデータ単位をパラメータ表示モデルとしてパラメータで表すモデルを抽出する。ブロック７３６に示すように、私的で微妙な内容の情報は、ネットワーク・トラフィック・データまたはパラメータ表示モデルあるいはそれらいずれもから削除できる。パラメータ表示モデルは、予め準備されたネットワーク・トラフィックの原型ミックスと照合して、ネットワーク・トラフィックのプロファイルを割り出すことができる（ブロック７４０に示す）。出力データ単位作成スクリプトは、ネットワーク・トラフィック・プロファイルに基づいて作成できる（ブロック７４４に示す）。出力データ単位は、データ単位作成スクリプトに基づいて作成できる（ブロック７５０に示す）。

【００７６】

図８は、本発明による、収集されたネットワーク・トラフィックのフィルタリングのフローチャートである。ブロック８１０に示すように、生のネットワーク・トラフィックを受信する。それから、ブロック８２０に示すように、データ単位の種類を解析する。そのときとられる動作は、評価されているデータ単位の種類に依存しうる。様々な実施において、データ単位の種類が、ブロック８２２に示すようにフレーム・リレーのデータ単位であるか、ブロック８２４に示すようにトークンリングのデータ単位であるか、ブロック８２６に示すようにＩＳＤＮデータの単位であるか、ブロック８２８に示すようにＸ．２５のデータ単位であるか、ブロック８３０に示すようにイーサネットのデータ単位であるか、ブロック８３２に示すようにＦＤＤＩのデータ単位であるか、ブロック８３４に示すようにＡＴＭのデータ単位であるか、ブロック８３６に示すようにＰＰＰのデータ単位であるか、ブロック８３８に示すように「他の」種類のデータ単位であるか、あるいはブロック８４０に示すように「ワイルドカード」のデータ単位であるかに基づいて、様々な動作を取りうる。ここで用いた「他の」とは、既知ではあるが情報の細かい細分性を保つ必要がない種類またはタイプのデータ単位を意味している。ここで用いた「ワイルドカード」とは、ネットワーク・トラフィック内に見られる未知の種類またはタイプのデータ単位を意味している。

【００７７】

データ単位の種類が、ブロック８３０に示すようにイーサネットの場合、データ単位は

ブロック８５０に示すようにそのタイプに基づいて更に分類される。イーサネットのデータ単位のタイプには、ブロック８５２に示すようなＡＲＰデータ単位、ブロック８５４に示すようなＲＡＲＰデータ単位、ブロック８６０に示すようなＩＰデータ単位、ブロック８５６に示すような「他の」タイプのイーサネット・データ単位、およびブロック８５８に示すような「ワイルドカード」または未知のタイプのイーサネット・データ単位が含まれる。イーサネット・データ単位のタイプがＩＰの場合、動作のフローは図９のブロック９１０に続く。他の種類のデータ単位は、特定の種類のデータ単位の属性に基づいて同様の特化された方法でフィルターすることができる。

【００７８】

図９は、ＩＰデータ単位をフィルタリングする際にとられる動作のフローチャートである。ＩＰデータ単位が収集されると（ブロック９１０に示す）、統計がそれに対してとられる適切な情報が、そのＩＰデータ単位の種類に基づいて割り出される（ブロック９２０に示す）。

【００７９】

ブロック９３０に示すように、ＩＰデータ単位の種類がＴＣＰであると、ブロック９３２に示すように、使用されたポートの履歴が保持される。ブロック９３３に示すように、ＴＣＰデータ単位についてのパラメータ表示された情報が作成される。このＴＣＰデータ単位についてのパラメータ表示された情報は、ブロック９３４に示すようにトラフィック要約テーブルに加えられるか、またはネットワーク・トラフィック要約データを格納するのに用いられる他のデータ構造に加えられる。ネットワーク・トラフィック要約テーブルは、取込グループ内のデータ単位のそれぞれについてネットワーク・トラフィック・データを格納することができる。

【００８０】

ブロック９４０に示すように、ＩＰデータ単位の種類がＵＤＰであると、ブロック９４２に示すように、ポート・トラフィックの履歴が保持される。ブロック９４３に示すように、ＵＤＰデータ単位についてのパラメータ表示された情報が作成され、このＵＤＰデータ単位についてのパラメータ表示された情報は、ブロック９４４に示すように、ネットワーク・トラフィック要約テーブルに加えられる。

【００８１】

ブロック９５０に示すように、ＩＰデータ単位の種類がＩＣＭＰであると、ブロック９５２に示すように、ＩＣＭＰデータ単位のタイプの履歴が保持される。ブロック９５３に示すように、ＩＣＭＰデータ単位についてのパラメータ表示された情報が作成され、このＩＣＭＰデータ単位についてのパラメータ表示された情報は、ブロック９５４に示すように、ネットワーク・トラフィック要約テーブルに加えられる。

【００８２】

ブロック９６０に示すように、ＩＰデータ単位の種類が「他の」であると、ブロック９６２に示すように、これら他のＩＰデータ単位の適切なデータ・フィールドの履歴が保持される。ブロック９６３に示すように、他のＩＰデータ単位についてのパラメータ表示された情報が作成され、この他のＩＰデータ単位についてのパラメータ表示された情報は、ブロック９６４に示すように、ネットワーク・トラフィック要約テーブルに加えられる。

【００８３】

ブロック９７０に示すように、ＩＰデータ単位の種類が「未知」であると、それは「ワイルドカード」と見なすことができる。ブロック９７３に示すように、未知の種類のＩＰデータ単位についてのパラメータ表示された情報が作成され、この未知のデータ単位についてのパラメータ表示された情報は、ブロック９７４に示すように、ネットワーク・トラフィック要約テーブルに加えられる。

【００８４】

図７、図８および図９に関して、追加のあるいはより少ないステップを取ることができ、また、示したようなステップは、本明細書に記載された方法を実現するようにして組み合わせ、またはさらに改良することもできる。

【００８５】
<<データ格納>>
図１０は、本発明によるネットワーク・トラフィック要約テーブル１０００である。要約テーブルは、ネットワーク・トラフィックに関する適切な情報を要約する機能を果たす。また要約テーブルは、トラフィック分布テーブルと見なすこともできる。ネットワーク・トラフィックに含まれるデータ単位に関する基本的な生のデータを、１つのテーブルとして見ることができる１つ以上のデータ構造内に保持することができる。１つの要約テーブルを、各取込グループに対して作成することができる。要約テーブルのサイズは、システムにより定められていても、ユーザーがカスタマイズできてもよい。要約テーブルは、特定の取込グループ内のネットワーク・トラフィックのパラメータ表示されたビューを提供し、複数の取込グループに関するデータ、または全ての取り込んだネットワーク・トラフィックの要約を格納するのに使用することができる。
【００８６】
ネットワーク・トラフィック要約テーブル１０００には、データ単位内に含まれる送信元および宛先ＩＰアドレス１０１０および１０１２、そのデータ単位において用いられるプロトコル１０２０のようなプロトコル情報１０１６、そのデータ単位において指定されるポート指示子すなわちポート・タイプ１０２２、およびそのデータ単位において指定されるフラグ１０２４が含まれうる。実例のプロトコルには、ＴＣＰ、ＵＤＰ、ＩＣＭＰ等が含まれる。これらのプロトコルは、図８および図９に関する上記のタイプのプロトコルに対応する。ポート指示子１０２２は、ポートの範囲、ポートのリスト、または単一のポートであってもよい。フラグ１０２４は、プロトコルのタイプ１０２０に基づいて変化しうる。
【００８７】
特定の範囲のサイズを有するデータ単位の数１０３０は、各binによって保持できる。すなわち、特定のＩＰアドレス１００４および／または同じプロトコル情報１０１６を有するデータ単位に対して、サイズによるデータ単位のカウントが保持できる。例えば、第１のbin１０３２は、１～６３バイトのサイズを有するデータ単位の数の生のカウントを含むことができ、第２のbin１０３４は６４～１２８バイトのサイズを有するデータ単位の数の生のカウントを含むことができ、第３のbin１０３６は１２８～２５５バイトのサイズを有するデータ単位の数の生のカウントを含むことができ、第４のbin１０３８は２５６～５１１バイトのサイズを有するデータ単位の数の生のカウントを含むことができ、第５のbin１０４０は５１２～１０２３バイトのサイズを有するデータ単位の数の生のカウントを含むことができ、第６のbin１０４２は１０２４～１５１８バイトのサイズを有するデータ単位の数の生のカウントを含むことができ、そして第７のbin１０４４は最大サイズを有するデータ単位の数の生のカウントを含むことができる。
【００８８】
要約テーブルに保持された情報をより効率的に格納するために、要約テーブルは、例えばハッシュテーブルを用いたり、他のデータ格納技法を用いたりすること等により、メモリ空間を浪費しないようにして実現することができる。
【００８９】
要約テーブルに加えて、またはその代わりに、各タイプのデータ単位に基づく情報のパラメータ表示されたベクトルを保持してもよい。例えば、データ単位のタイプにＴＣＰ、ＵＤＰおよびＩＣＭＰデータ単位が含まれている場合には、パラメータ表示されたＴＣＰ表現ベクトル、パラメータ表示されたＵＤＰ表現ベクトル、およびパラメータ表示されたＩＣＭＰ表現ベクトルが使用でき、他の場合も同様である。
【００９０】
図１１は、本発明によるＴＣＰデータ単位の表現ベクトル１１００である。表現ベクトル１１００には、レイヤ２プロトコル・タイプ１１１０、レイヤ３プロトコル・タイプ１１１２、ＩＰタイプ・サービス１１１４、送信元ＩＰアドレス１１１６、宛先ＩＰアドレス１１１８、送信元および宛先ＴＣＰポートの最小値である最小ＴＣＰポート１１２０、

送信元／宛先ポート・ビット１１２２、スタッフィング・ビット１１２４、ＴＣＰフラグ１１２６、およびデータ単位サイズ１１２８に対するフィールドが含まれる。表現ベクトル１１００は、１２８ビット幅でよい。表現ベクトルのサイズは、取り込むべき情報、および他の理由（ＣＰＵワードサイズ、利用可能な記憶用メモリ等）に基づいて、様々な実施において変化しうる。ネットワーク・カード上のプロセッサーすなわち本明細書に記載の技術を実現するためのソフトウェアを実行するプロセッサーは３２ビットワードを有しうるため、表現ベクトル１１００は、指定された３２ビットの部分で示している。他のワードサイズ（例えば８、１６、６４等）を有する他のプロセッサーもまた使用できる。

【００９１】

図示の表現ベクトル１１００は、一つの例、すなわち標準ＩＰタイプ・サービスを用いて、ＩＰアドレス10.0.0.1からＩＰアドレス10.0.0.2（宛先ＴＣＰポート８０）へと送られるＩＰバージョン４のＴＣＰデータ単位を表している。この例では、レイヤ２プロトコル・タイプは、十六進数コード０ｘ０８００のＩＰｖ４である。この情報を得るには、いくつかの処理が必要とされることがある。例えば、最小のＴＣＰポートは、２つのポート（送信元および宛先）に関する情報を抽出し、最小を見いだすためにそれらを比較することを必要とする。

【００９２】

図１２は、本発明によるＩＣＭＰデータ単位の表現ベクトル１２００である。表現ベクトル１２００は、レイヤ２プロトコル・タイプ１２１０、レイヤ３プロトコル・タイプ１２１２、ＩＰタイプ・サービス１２１４、送信元ＩＰアドレス１２１６、宛先ＩＰアドレス１２１８、ＩＣＭＰタイプ・コード１２２０、スタッフィング・ビット１２２２、およびデータ単位サイズ１２２４に対するフィールドが含まれる。表現ベクトル１２００は、１２８ビット幅でよい。表現ベクトルのサイズは、取り込むべき情報、および他の理由（ＣＰＵワードサイズ、利用可能な記憶用メモリ等）に基づいて、様々な実施において変化しうる。ネットワーク・カード上のプロセッサーすなわち本明細書に記載の技術を実現するためのソフトウェアを実行するプロセッサーは３２ビットワードを有しうるため、表現ベクトル１２００は、指定された３２ビットの部分で示している。他のワードサイズ（例えば８、１６、６４等）を有する他のプロセッサーもまた使用できる。

【００９３】

図示の表現ベクトル１２００は、一つの例、すなわち標準ＩＰタイプ・サービスを用いて、ＩＰアドレス10.0.0.1からＩＰアドレス10.0.0.3へと送られるＩＰバージョン４のＩＣＭＰデータ単位を表している。この例では、レイヤ２プロトコル・タイプは十六進数コード０ｘ０８００のＩＰｖ４であり、レイヤ３プロトコル・タイプはＩＣＭＰを示す１である。

【００９４】

本発明の代表的な実施例を示して説明してきたが、本明細書中に記載された本発明に対するいくつもの変更、改変、または置換であって、本発明の精神から逸脱しないものが可能であることは、当業者には明らかであろう。したがって、全てのそのような変更、改変および置換が、本発明の範囲内にあるものとみなされるべきである。

【００９５】

<<著作権およびトレード・ドレスの告知>>

この特許文献の開示の一部は、著作権保護を受ける材料を含んでいる。この特許文献は、所有者のトレード・ドレスであるかそれになりうる内容を示しかつ／または記述していることがある。この著作権およびトレード・ドレスの所有者は、特許商標庁の特許ファイルまたは記録に現れるそのままの特許の開示の何人による複製に対しても不服はないが、それ以外では全ての著作権およびトレード・ドレス権のいかなるものをも保有するものである。

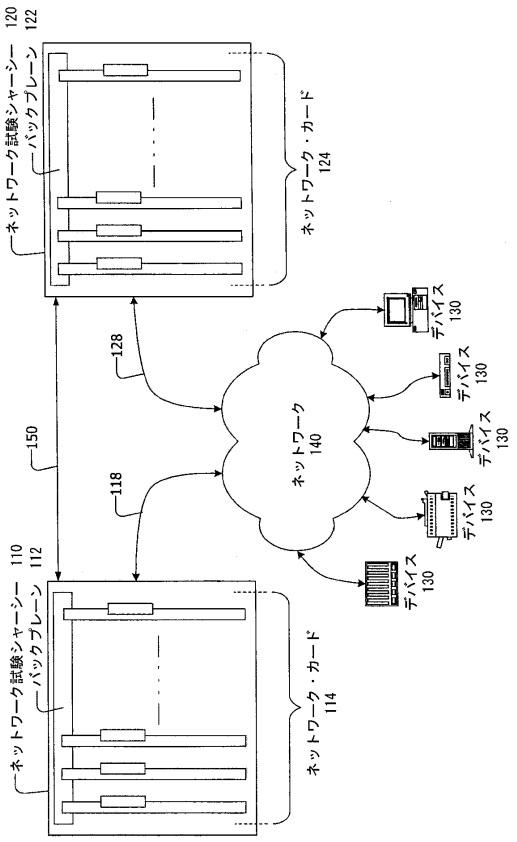
【図面の簡単な説明】

【００９６】

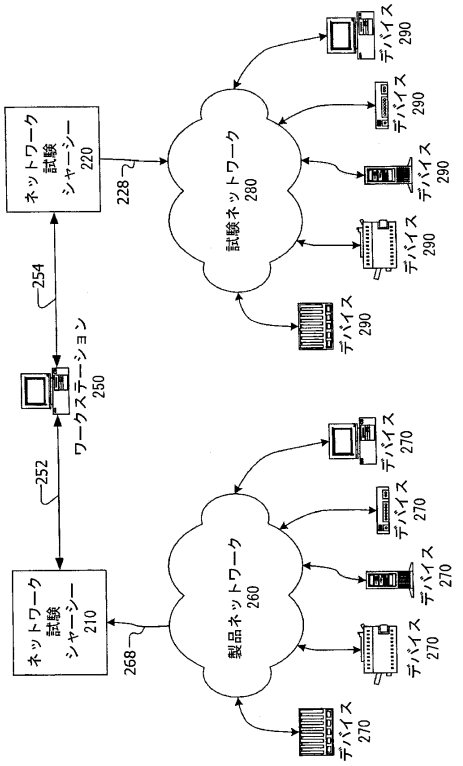
【図１】本発明による環境のブロック図である。

【図２】本発明による第２の環境のブロック図である。
【図３】本発明による第３の環境のブロック図である。
【図４Ａ】本発明による動作ユニットの機能ブロック図である。
【図４Ｂ】図４に示した動作ユニットでとられる動作のフローチャートである。
【図５】本発明による動作ユニットの第２の機能ブロック図である。
【図６】本発明によるネットワーク試験システムのブロック図である。
【図７】本発明による方法のフローチャートである。
【図８】本発明にしたがってネットワーク・トラフィックにフィルターをかける際にとられる動作のフローチャートである。
【図９】本発明にしたがってインターネット・プロトコル・データ単位にフィルターをかける際にとられる動作のフローチャートである。
【図１０】本発明によるネットワーク・トラフィック要約テーブルである。
【図１１】本発明によるＴＣＰデータ単位の表現ベクトルである。
【図１２】本発明によるＩＣＭＰデータ単位の表現ベクトルである。

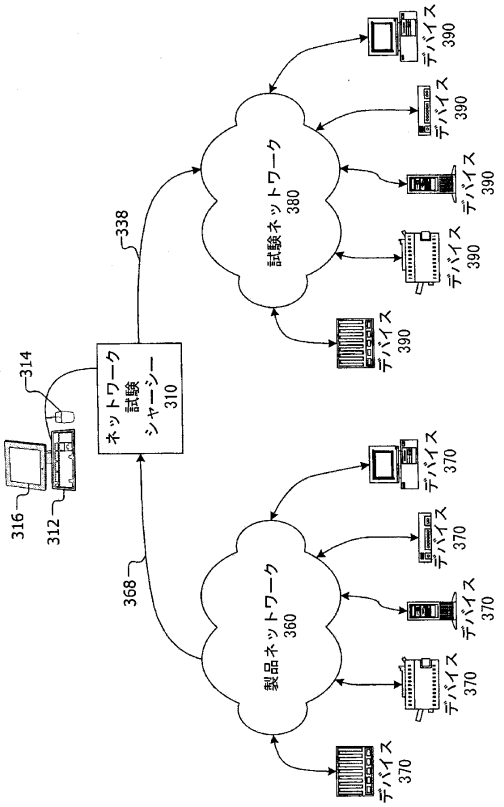
【図１】



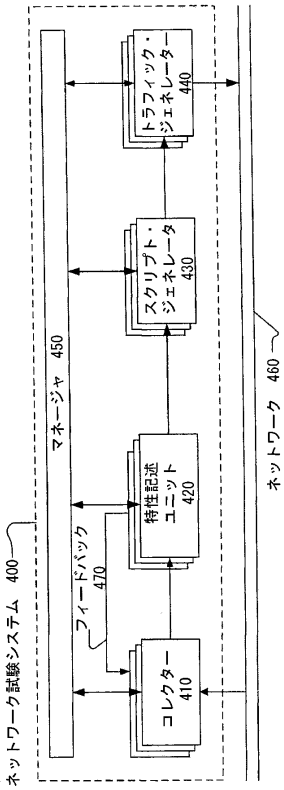
【図２】



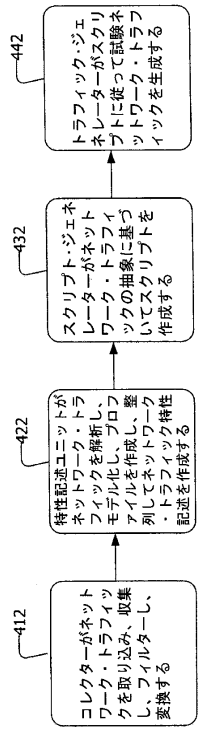
【図３】


ネットワーク試験シャーシー 310
試験ネットワーク 380
製品ネットワーク 360
デバイス 390
デバイス 370
314
316
312
338
368

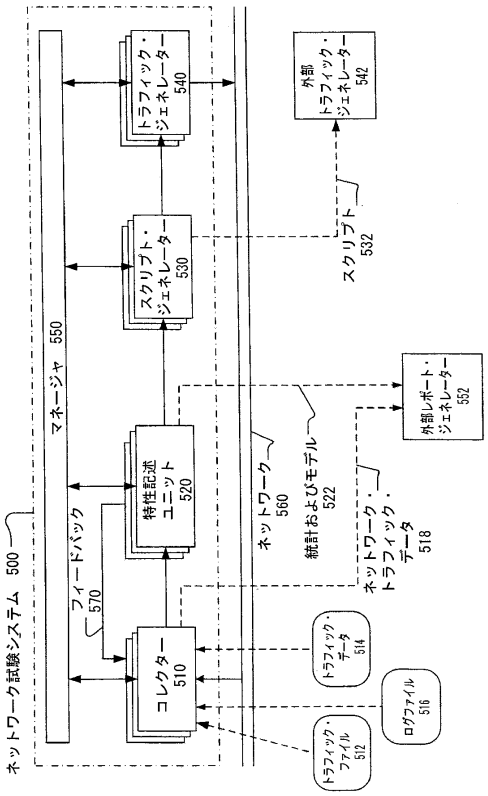
【図４Ａ】


ネットワーク試験システム 400
マネージャ 450
フィードバック 470
コレクター 410
特性記述ユニット 420
スクリプト・ジェネレータ 430
トラフィック・ジェネレーター 440
ネットワーク 460

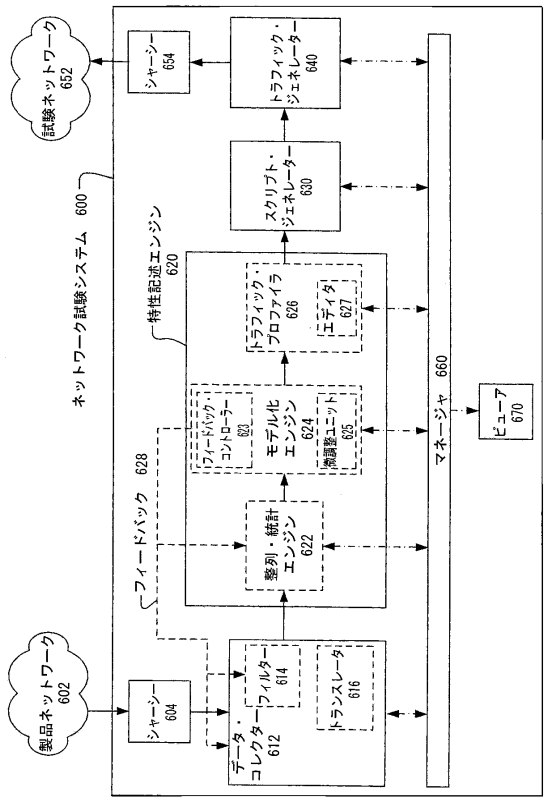
【図４Ｂ】


412
コレクターがネットワーク・トラフィックを取り込み、収集し、フィルター し、変換する
422
特性記述ユニットがネットワーク・トラフィックを解析し、モデル化し、プロファイルを作成し、整列してネットワーク・トラフィック特性記述を作成する
432
スクリプト・ジェネレーターがネットワーク・トラフィックの抽象に基づいてスクリプトを作成する
442
トラフィック・ジェネレーターがスクリプトに従って試験ネットワーク・トラフィックを生成する

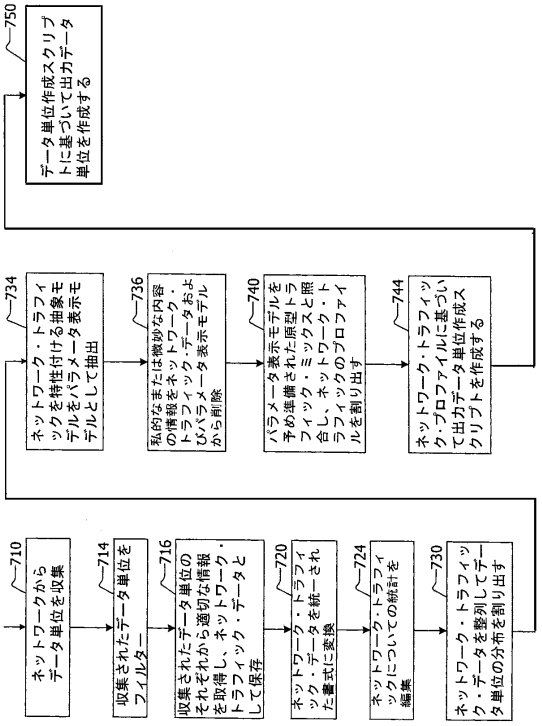
【図５】


ネットワーク試験システム 500
マネージャ 550
フィードバック 570
コレクター 510
特性記述ユニット 520
スクリプト・ジェネレーター 530
トラフィック・ジェネレーター 540
外部トラフィック・ジェネレーター 542
スクリプト 532
ネットワーク 560
統計およびモデル 522
ネットワーク・トラフィック・データ 518
外部レポート・ジェネレーター 552
トラフィック・ファイル 512
トラフィック・データ 514
ログファイル 516

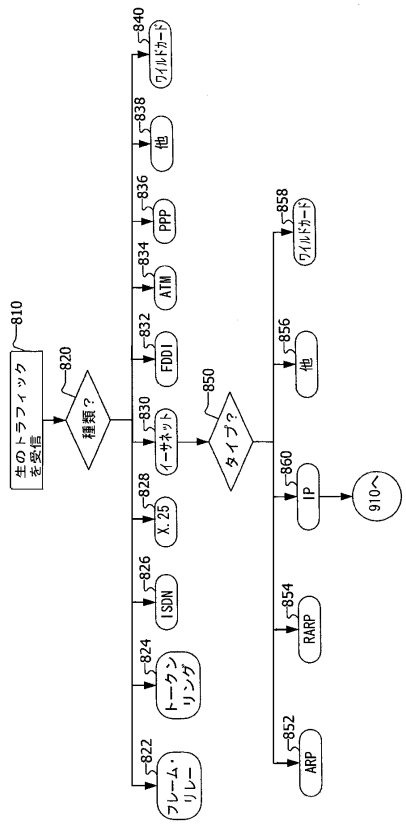
【図６】


製品ネットワーク 602
試験ネットワーク 652
ネットワーク試験システム 600
シャーシー 604
シャーシー 654
フィードバック 628
データ・コレクター 612
フィルター 614
トランスレータ 616
整列・統計エンジン 622
フィードバック・コントローラー 623
モデル化エンジン 624
適調整ユニット 625
特性記述エンジン 620
トラフィック・プロファイラ 626
エディタ 627
スクリプト・ジェネレーター 630
トラフィック・ジェネレーター 640
マネージャ 660
ビューア 670

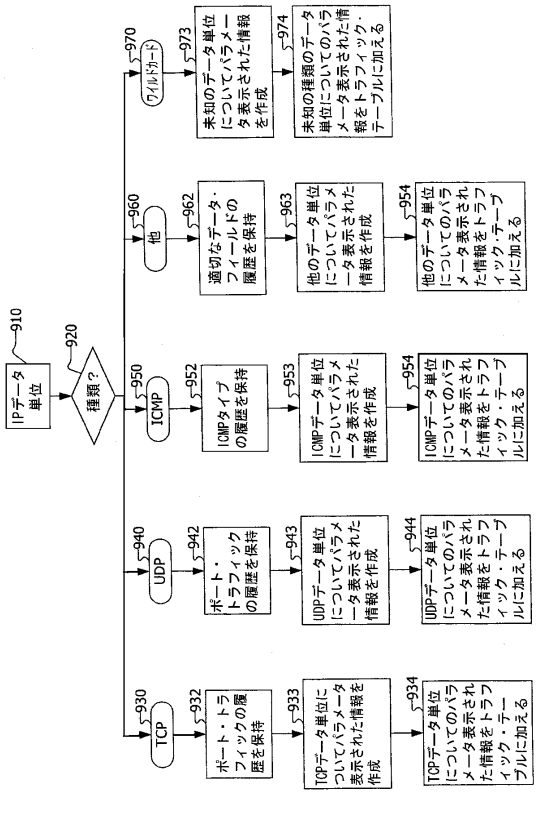
【図７】


750
データ単位作成スクリプトに基づいて出力データ単位を作成する
734
ネットワーク・トラフィックを特性付ける抽象モデルをパラメータ表示モデルとして抽出
736
私的なまたは微妙な内容の情報をネットワーク・トラフィック・データおよびパラメータ表示モデルから削除
740
パラメータ表示モデルを予め準備された原型トラフィック・ミックスと照合し、ネットワーク・トラフィックのプロファイルを割り出す
744
ネットワーク・トラフィック・プロファイルに基づいて出力データ単位作成スクリプトを作成する
710
ネットワークからデータ単位を収集
714
収集されたデータ単位をフィルター
716
収集されたデータ単位のそれぞれから適切な情報を取得し、ネットワーク・トラフィック・データとして保存
720
ネットワーク・トラフィック・データを統一された書式に変換
724
ネットワーク・トラフィックについての統計を編集
730
ネットワーク・トラフィック・データを整列してデータ単位の分布を割り出す

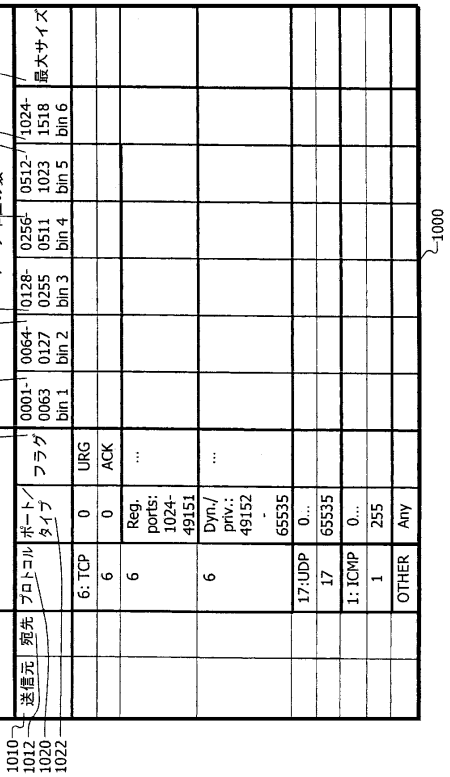
【図８】


生のトラフィックを受信
810
種類？
820
タイプ？
850
S822 フレーム・リレー
S824 トークン・リング
S826 ISDN
S828 X.25
S830 イーサネット
S832 FDDI
S834 ATM
S836 PPP
S838 他
S840 ワイルドカード
S852 ARP
S854 RARP
S856 他
S858 ワイルドカード
S860 IP
910へ

【図９】


IPデータ単位
910
種類？
920
S930 TCP
S932 ポート・トラフィックの履歴を保持
S933 TCPデータ単位についてのパラメータ表示された情報を作成
S934 TCPデータ単位についてのパラメータ表示された情報をトラフィック・テーブルに加える
S940 UDP
S942 ポート・トラフィックの履歴を保持
S943 UDPデータ単位についてのパラメータ表示された情報を作成
S944 UDPデータ単位についてのパラメータ表示された情報をトラフィック・テーブルに加える
S950 ICMP
S952 ICMPタイプの履歴を保持
S953 ICMPデータ単位についてのパラメータ表示された情報を作成
S954 ICMPデータ単位についてのパラメータ表示された情報をトラフィック・テーブルに加える
S960 他
S962 適切なデータ・フィールドの履歴を保持
S963 他のデータ単位についてのパラメータ表示された情報を作成
S954 他のデータ単位についてのパラメータ表示された情報をトラフィック・テーブルに加える
S970 ワイルドカード
S973 未知のデータ単位についてのパラメータ表示された情報を作成
S974 未知の種類のデータ単位についてのパラメータ表示された情報をトラフィック・テーブルに加える

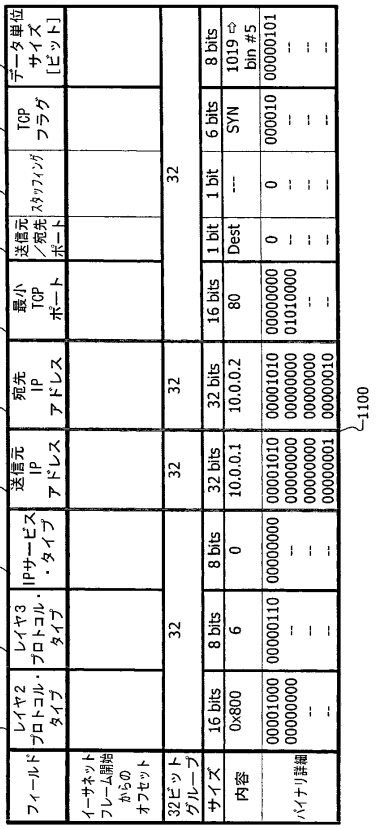
【図１０】



IPアドレス			プロトコル情報			データ単位の数					
送信元	宛先	プロトコル	ポート/タイプ	フラグ	0001-0063 bin 1	0064-0127 bin 2	0128-0255 bin 3	0256-0511 bin 4	0512-1023 bin 5	1024-1518 bin 6	最大サイズ
		6: TCP	0	URG							
		6	0	ACK							
		6	Reg. ports: 1024-49151	...							
		6	Dyn./prv.: 49152-65535	...							
		17:UDP	0...								
		17	65535								
		1: ICMP	0...								
		1	255								
		OTHER	Any								

1000
1004
1010
1012
1016
1020
1022
1024
1030
1032
1034
1036
1038
1040
1042
1044

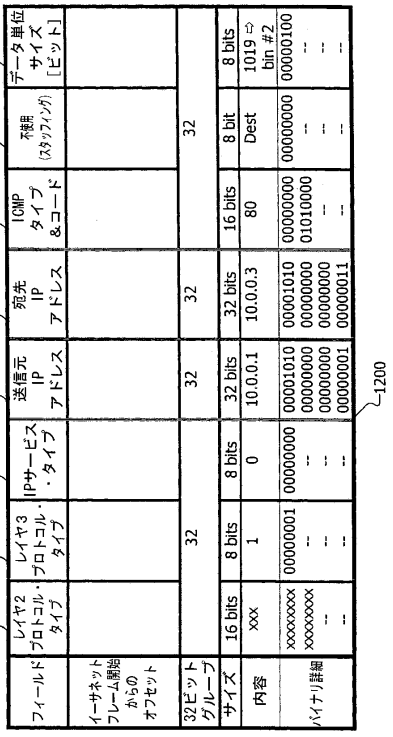
【図１１】



フィールド	レイヤ2プロトコル・タイプ	レイヤ3プロトコル・タイプ	IPサービス・タイプ	宛先IPアドレス	送信元IPアドレス	宛先IPアドレス	最小TCPポート	送信元/宛先ポート	スタッフィング	TCPフラグ	データ単位サイズ[ビット]
イーサネットフレーム開始からのオフセット											
32ビットグループ		32		32	32	32		32			
サイズ	16 bits	8 bits	8 bits	32 bits	32 bits	32 bits	16 bits	1 bit	1 bit	6 bits	8 bits
内容	0x800	6	0	10.0.0.1	10.0.0.2		80	Dest	---	SYN	1019 ⇨ bin #5
バイナリ詳細	00001000 00000000 -- --	00000110 -- -- --	00000000	00001010 00000000 00000000 00000000	00001010 00000000 00000000 00000000	00000010 00000000 00000000 00000000	00000000 01010000 -- --	0 -- -- --	0 -- -- --	000010 -- -- --	00000101 -- -- --

1100
1110
1112
1114
1116
1118
1120
1122
1124
1126
1128

【図１２】



フィールド	レイヤ2プロトコル・タイプ	レイヤ3プロトコル・タイプ	IPサービス・タイプ	送信元IPアドレス	宛先IPアドレス	ICMPタイプ&コード	未使用(スタッフィング)	データ単位サイズ[ビット]
イーサネットフレーム開始からのオフセット								
32ビットグループ		32		32	32			
サイズ	16 bits	8 bits	8 bits	32 bits	32 bits	16 bits	8 bit	8 bits
内容	xxx	1	0	10.0.0.1	10.0.0.3	80	Dest	1019 ⇨ bin #2
バイナリ詳細	xxxxxxxx xxxxxxxx -- --	00000001 -- -- --	00000000 -- -- --	00001010 00000000 00000000 00000001	00001010 00000000 00000000 00000011	00000000 01010000 -- --	00000000 -- -- --	00000100 -- -- --

1200
1210
1212
1214
1216
1218
1220
1222
1224

フロントページの続き

審査官　玉木　宏治

(56)参考文献　San-qi Li et al., MAQ: A Measurement-Based Tool for Traffic Modeling and Queuing Analysis PartI: Design Methodologies and Software Architecture, IEEE Communicaitons Magazine, １９９８年　８月　１日, vol.36,no.8, pp.56-65
San-qi Li et al., MAQ: A Measurement-Based Tool for Traffic Modeling and Queuing Analysis PartII: Network Applications, IEEE Communicaitons Magazine, １９９８年　８月　１日, vol.36,no.8, pp.66-77

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ　１２／５６