(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5520231号
(P5520231)
(45)発行日　平成26年6月11日(2014.6.11)　(24)登録日　平成26年4月11日(2014.4.11)

(51)Int.Cl.　　F I
H04L 12/70 (2013.01)　　H04L 12/70　100Z
H04L 12/66 (2006.01)　　H04L 12/66　B

請求項の数 17　(全 16 頁)

(21)出願番号　特願2010-539443 (P2010-539443)
(86)(22)出願日　平成20年12月12日 (2008.12.12)
(65)公表番号　特表2011-507453 (P2011-507453A)
(43)公表日　平成23年3月3日 (2011.3.3)
(86)国際出願番号　PCT/US2008/013694
(87)国際公開番号　WO2009/082439
(87)国際公開日　平成21年7月2日 (2009.7.2)
審査請求日　平成23年8月9日 (2011.8.9)
(31)優先権主張番号　12/000,910
(32)優先日　平成19年12月18日 (2007.12.18)
(33)優先権主張国　米国(US)

(73)特許権者　510171531
ソーラーウィンズ　ワールドワイド、エルエルシー
アメリカ合衆国、テキサス州　７８７４６、オースティン、ビルディング　２、サウス　モパック　エクスプレスウェイ　３７１１、
(74)代理人　100064414
弁理士　磯野　道造
(72)発明者　ニューマン、グレッグ
アメリカ合衆国、テキサス州　７８７４６、オースティン、サウス　モパック　エクスプレスウェイ　１３０１

審査官　山田　倍司

最終頁に続く

(54)【発明の名称】フロー情報に基づくネットワークデバイスのＡＣＬ構成方法

(57)【特許請求の範囲】
【請求項１】
ネットワークトラフィックを受信して、前記ネットワークトラフィックを記述した複数のフローレコードを生成するネットワーク機器と、
前記ネットワーク機器から前記フローレコードを受信し、前記フローレコードを記憶するフローレコード記憶装置と、
前記フローレコード記憶装置にアクセスし、前記記憶されたフローレコードを読み出し、前記フローレコードの一つ一つを所定の基準にしたがって評価して、動的にアドレスを特定するデータ分析ツールとを備えた複数のネットワーク通信を動的に制御するシステムであって、
前記データ分析ツールは、ネットワーク利用に関する問題を解決する、複数の統計モデルを実装し、前記複数のフローレコードと前記複数の統計モデルを使用して、前記フローレコード記憶装置に記憶される統計結果を生成し、
前記複数のフローレコードの一つ一つは、そのフローレコードを特定する連続番号、送信元ノードアドレス、送信先ノードアドレス、送信元ポートアドレス、送信先ポートアドレス、及び対応する一つ一つのフローにおいて送信されたバイト数またはパケット数を有し、
前記所定の基準は、前記送信元ノードアドレス、前記送信先ノードアドレス、前記送信元ポートアドレスまたは前記送信先ポートアドレスのそれぞれへの前記対応するフローにおいて送信された全バイト数を含んでおり、

前記ネットワーク機器は、前記特定されたアドレスを受信し、前記特定されたアドレスをアクセス制御リストに加えて、前記特定されたアドレスに対応するトラフィックの転送を遮り、
前記システムは、さらに、前記データ分析ツールから受信した前記特定されたアドレスをユーザに表示する入出力装置を備えており、
前記データ分析ツールは、前記ユーザが前記特定されたアドレスを承認する入力を行った場合にのみ、前記特定されたアドレスを前記ネットワーク機器に転送し、前記ネットワーク機器が前記特定されたアドレスを前記アクセス制御リストに追加することを特徴とするシステム。
【請求項２】
前記特定されたアドレスを記憶し、前記特定されたアドレスを前記ネットワーク機器に提供するアクセス制御リスト記憶装置をさらに備えることを特徴とする請求項１に記載のシステム。
【請求項３】
前記複数のフローレコードは、前記送信元ノードアドレス、前記送信先ノードアドレス、前記送信元ポートアドレス及び/または前記送信先ポートアドレスごとに集計されることを特徴とする請求項１に記載のシステム。
【請求項４】
前記入出力機器は、さらに、前記特定されたアドレスに対応するフローレコードデータを入手し、表示することを特徴とする請求項３に記載のシステム。
【請求項５】
ネットワークのコンポーネントを通過するトラフィックを監視するステップと、
前記コンポーネントから、前記トラフィックを記述するフローレコードを受信するステップと、
前記フローレコードを分析し、１つのアドレスに対応する総バイト数の最大限度を含む所定の基準を満たすアドレスを特定するステップと、
ユーザに、その特定されたアドレスを表示するステップと、
前記ユーザが前記特定されたアドレスを承認した後に、前記特定されたアドレスを前記ネットワークコンポーネントの一つに転送するステップと、を有するネットワーク管理方法であって、
前記コンポーネントは、前記特定されたアドレスを、対応するアクセス制御リストに追加し、
前記アクセス制御リストは、前記コンポーネントが前記特定されたアドレスに対応するトラフィックの転送を妨げるように、前記コンポーネントに命令することを特徴とするネットワーク管理方法。
【請求項６】
所定の時間が経過した後は、前記特定されたアドレスは前記アクセス制御リストから自動的に削除されることを特徴とする請求項５に記載の方法。
【請求項７】
前記アドレスは、発信元ノード、送信先ノード、発信元ポート及び送信先ポートの少なくとも一つを特定することを特徴とする請求項５に記載の方法。
【請求項８】
前記アドレスは、発信元ノードを特定することを特徴とする請求項７に記載の方法。
【請求項９】
前記特定されたアドレスに対応する前記フローレコードのデータを前記ユーザに表示するステップをさらに含むことを特徴とする請求項５に記載の方法。
【請求項１０】
ネットワークトラフィックを記述するフローレコードを提供するフローレコード生成機器と、
前記フローレコードを受信し、記憶するフローレコード記憶システムと、

前記フローレコード記憶システムにアクセスし、前記記憶されたフローレコードに、所定の基準に基づいてアクセスするデータ分析機器と、を備えるネットワークにおけるトラフィックを動的に制御するシステムであって、
前記データ分析機器は、前記所定の基準を満たす少なくとも一つのアドレスを動的に特定し、
前記少なくとも一つのアドレスは、前記トラフィックに対応するポートまたはノードアドレスを含み、
前記特定された少なくとも一つのアドレスは、アクセス制御リストに加えられ、前記ネットワーク内のコンポーネントは、前記アクセス制御リスト内のアドレスに対応するトラフィックを転送せず、
前記フローレコードの一つ一つは、タイムスタンプを含み、前記所定の基準は、 タイムウィンドウであることを特徴とするシステム。
【請求項１１】
前記フローレコード記憶システムは、前記フローレコードを集計することを特徴とする請求項１０に記載のシステム。
【請求項１２】
前記特定されたアドレスをユーザに表示するユーザインターフェースをさらに備え、
前記ユーザが前記特定されたアドレスを承認した場合にのみ、前記特定されたアドレスが前記アクセス制御リストに追加されることを特徴とする請求項１０に記載のシステム。
【請求項１３】
前記ユーザインターフェースは、前記特定されたアドレスに対応するフローレコード・データを前記ユーザに表示することを特徴とする請求項１２に記載のシステム。
【請求項１４】
ネットワーク内のコンポーネントを通過するトラフィックを監視するステップと、
前記コンポーネントから、前記トラフィックを記述するフローレコードを受信するステップと、
前記アクセス制御リストに記載されているアドレスに対応する前記受信したフローレコードのうちの任意のフローレコードを所定の基準に基づいて分析するステップと、
前記アドレスが予め定義された基準を満たした場合、前記アクセス制御リスト内に記載されている前記アドレスを更新するステップと、
前記アドレスをユーザに表示するステップとを含む、アクセス制御リストに記載されているアドレスの評価方法であって、
前記アドレスの前記更新ステップは、前記ユーザが前記アドレスを承認した後に実行されることを特徴とする、アドレスの評価方法。
【請求項１５】
前記アドレスに対応するフローレコードデータを前記ユーザに表示することを特徴とする請求項１４に記載の方法。
【請求項１６】
前記アドレスは、発信元ノード、送信先ノード、発信元ポート、送信先ポートの少なくとも一つを特定することを特徴とする請求項１４に記載の方法。
【請求項１７】
前記アドレスは、予め定義された時間が経過した後、自動的に前記アクセス制御リストから削除されることを特徴とする請求１４に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワークルータからエクスポートされたネットワークフローデータを使用して、デバイスに転送されるトラフィックやデバイスから転送するトラフィックの情報を提供する技術に関するものである。ネットワークルータは、２つのネットワークデバイ

ス（そのデバイスのトラフィックはルータを介して移動する）間の様々なタイプのネットワークトラフィックの通過を許可もしくは拒否するように構成することができる。提示する方法は、ネットワークルータからエクスポートされたネットワークフロー情報から得られた情報により動的にアクセス制御リストを生成し、そのアクセス制御リストをルータに適用するものである。

【背景技術】

【０００２】

ネットワーク利用データは、契約者への課金、マーケティング及びカスタマーケア、製品開発、ネットワークオペレーション管理、ネットワークとシステムの処理能力計画、セキュリティなどの多くの重要なビジネス機能に役に立つものである。ネットワーク利用データは、通信者同士のコミュニケーション・セッションにおいて送受信された実際のデータを含んでいるわけではなく、一つ以上のタイプのメタデータ（つまり、「データ」に関する「データ」）を含む「フローレコード」として知られる、多数の詳細な利用データを含むものである。公知のネットワーク・フローレコード・プロトコルとしては、Ｎｅｔｆｌｏｗ（登録商標）、ｓＦｌｏｗ（登録商標）、ｊＦｌｏｗ（登録商標）、ｃＦｌｏｗ（登録商標）Ｎｅｔｓｔｒｅａｍ（登録商標）などが挙げられる。本明細書で使用されるとおり、フローレコードは、ある時間間隔の間、同じ発信元、送信先パラメータを共有する複数のＩＰパケットのストリームによる、一方向のネットワーク利用を測定する際の小さい一単位として定義されている。

【０００３】

一つ一つのフローレコードに含まれるメタデータのタイプは、関連するサービスやネットワークのタイプに応じて、また、ある場合では、フローレコードを提供する個別のネットワークデバイスに応じて様々である。一般的に、フローレコードは、接続開始時間、接続停止時間、転送されたデータの発信元、そのデータの送信先や受信者、転送されたデータ量などの、ある特定のイベントや通信者間の通信接続に関する詳細な利用情報を提供するものである。フローレコードは、非常に短い時間（数ミリ秒から数秒、時々数分）で、利用情報をまとめている。関連するサービスやネットワークのタイプによっては、フローレコードは、転送プロトコル、転送されたデータのタイプ、提供されたサービスのタイプ（ＴｏＳ）などに関する情報を含む場合もある。電話網においては、利用情報を構成するフローレコードは、通話情報（ＣＤＲｓ）と呼ばれる。

【０００４】

ネットワークの監視においては、有意味な分析結果を生成するために、複数のネットワークフローレコードが収集、保存、分析される。ネットワーク利用分析システムが、これらの複数のフローレコードを分析処理し、様々なビジネス機能をサポートするレポートや要約データファイルを生成する。ネットワーク利用分析システムは、ネットワークサービスがどのように使用されているかや誰に使用されているかに関する情報を提供する。また、ネットワーク利用分析システムは、ネットワークの混雑やネットワークセキュリティの悪用などにより起こる問題などの、顧客満足度に関する問題を特定（または予測）するために使用することもできる。一例においては、契約者の利用行動の一つの機能として、ネットワークの利用と処理能力を監視して、ユーザの経験を追跡したり、将来のネットワーク容量を予測したり、ネットワークの悪用、詐欺、盗用などを示す利用行動を特定したりすることが出来る。

【０００５】

コンピュータ・セキュリティにおいては、アクセス制御リスト（ＡＣＬ）は、ある対象に与えられた許可リストである。より具体的には、ネットワークの構築において、ＡＣＬは、トラフィック・フィルタリング・ルールを列挙したルールのリストである。ＡＣＬは、ネットワークデバイスを介したトラフィックの通過を許可または拒否することが出来る。　ネットワークＡＣＬを有することができるのは、ルーターとファイアウォールのみである。アクセス制御リストは、一般的に、インバウンドトラフィックとアウトバンドトラフィックの両方を制御可能である。

【０００６】
ＡＣＬは、望ましくないアドレスもしくはポートへのユーザやデバイスのアクセス、望ましくないアドレスもしくはポートからのユーザやデバイスへのアクセスを制限することによって、ネットワーク・トラフィックを制御する一つの方法である。ＡＣＬは、他のデバイスがパケットをフィルタすることもできるが、通常はルーター・インターフェースで、発送されたパケットを転送したりブロックすることにより、ネットワーク・トラフィックをフィルタリングしている。ルータは、アクセスリストに規定された基準に基づいて、一つ一つのパケットを検査してそのパケットを転送するか拒否するかを決定する。アクセス制御リストの基準としては、トラフィックの発信元アドレス、送信先アドレス、目標ポート、プロトコル、またはそれらの組み合わせ等が挙げられる。通常は、インターネットプロトコル（ＩＰ）アドレスが、ＩＰベースのネットワークにおいて発信元デバイスの識別子として機能する。アクセス制御リストは、ネットワーク内におけるこのＩＰ識別子に基づいて、アクセスの差別化を可能にしている。
【０００７】
ＡＣＬは有用な機能を提供するが、ＡＣＬの作成は、多大な時間と労力がかかる場合がある。特に、ＡＣＬは現在、人がプログラムすることで作成されている。さらに、ＡＣＬに列挙される複数のＩＰアドレスの選択は、恣意的で、予測不可能な場合もある。
【０００８】
特に、自律ＩＰネットワークや企業ＩＰネットワークは、規模が大きく、複雑で動的であり、それらのネットワークを管理するのは難しい。まず、ネットワークにおけるトラフィックの監視、ネットワークのパフォーマンスの分析、パフォーマンスの改善のためのネットワークの再構築などのようなネットワーク管理業務は、ネットワークに関する情報を必要とする。ところが、規模の大きなＩＰネットワークは極めて動的なため、数多くのネットワーク管理業務に有用な情報を得ることが困難である。規模の大きなＩＰネットワークは、何万ものノードと何百ものルーター、ゲートウェイを有することがあることを考えてほしい。大企業のネットワークは、３０万のノードと２千５百のルータを有する場合もある。ルーター、ゲートウェイ、スイッチ、その他のネットワークデバイスは、時々、故障したり、オフラインになったり、（ネットワークに）復帰したりする。リンクは、よく、故障したり、（ネットワークに）復帰したり、性能が低下したりする。例えば、マイクロ派リンクや衛星リンクは、その帯域を減少させる電波妨害にあうことがある。ＯＳＰＦやＢＧＰなどの、大規模なＩＰネットワークにおいてトラフィックの道順を決めるのに使われるプロトコルは、動的であり、ネットワークの状況の変化に応じて、大規模なネットワークにおいてルーティングパスを変更する。比較的安定したネットワークにおいてさえ、経路収束の状態に達するには長い時間がかかる。一回の接続期間内においてさえ、意図的に、ＩＰネットワークにおける２つのコンピュータ間の通信経路が変わるようにすることも出来る。上述した要素と後述する他の要素により、ネットワーク管理ツールが、幾分か完全で正確なネットワーク像を、時間の経過に沿って表す情報を得ることは困難であった。
【０００９】
ネットワークが複雑になると、技術力のある人間のオペレータが介入することを必要とするため、ネットワークの管理が高額になる。大規模なＩＰネットワークの構成と管理を自動化するのは困難であった。徹底的な人間の管理が必要なことにより、多くのオペレータは、ネットワークを頻繁に再構築してネットワークの性能を最適化することよりも、ネットワークの安定性を優先させる保守的な方針を採用してきた。そのため、ネットワーク管理の技術分野におけるもう一つの問題は、ＩＰネットワークが、必要な期間よりも長い間、準最適ネットワーク構成を維持し、それにより、高額な帯域容量を効率的に使えなかったり、準最適ネットワーク構成を長い間維持しない場合に生じるコミュニケーション・レイテンシーよりも潜在的に高い値のコミュニケーション・レイテンシーを引き起こしたりすることである。（ネットワークの）管理や構成の自動化のためのツールは、広範に採用されることはなかった。

【００１０】
ＡＣＬの監視やメンテナンスを含むネットワーク管理のためのツールは存在するが、それらのツールは単純で、数多くの欠点がある。ほとんどのネットワーク管理ツールは、単純に、機能しているネットワークデバイスを発見してポーリングし、マップ、カウンタ値、平均値、高トラフィックのエリアなどを含むレポートを生成するだけである。現在のツールは、個々のネットワークデバイスから局所的に取られた、中央部に集まる潜在的に相反するデータに注意を集中し、ネットワークの行動の全体的な動態を無視する傾向にある。現在のツールは、ネットワークにおいてある特定のトラフィックのセットが使用するパスを発見したり、なんらかの状況を仮定したシナリオによってネットワークの行動を調査したり、故障や故障からの復帰があった際のネットワークの変化を監視したり、具体的なアプリケーションやサービスに関連することからネットワーク・トラフィックを分析したりすることなどの、潜在的に有用な様々なタスクを、オペレータが実行しやすいようになっていない。

【００１１】
上述したとおり、個々のユーザコンピュータでネットワーク・トラフィックを測定しようとする試みはあったが、ホスト・トラフィックデータは、範囲が制限されており、大体の場合、ＩＰネットワークにおける特定の経路を進むトラフィックフローに関する情報を明らかにすることが出来ない。ホストやエンドシステムによるネットワーク測定は、ネットワークトポロジに関する有用な情報を提供できない。例えば、シスコシステムズ社製のＮｅｔｆｌｏｗ（登録商標）などの、ルータやスイッチなどのネットワーク機器におけるＩＰトラフィックデータを集計するツールもある。しかしながら、これらの手法は、不透明な（例えば、暗号化されたり、トンネル化された）トラフィック、複雑なアプリケーション通信のパターン、サンプリング加工物、監視によるルーターの負荷やその他の数多くの理由により、不十分であることが明らかとなっている。

【００１２】
さらに、ウィルスを特定する公知の技術には、限界がある。一般的に、それらの公知の技術は、ネットワークリソースの利用を監視し、不自然なほど大量のネットワークリソースを要求するアプリケーションを特定するなど、ウィルスの二次的影響を探すものである。しかし、ウィルスと、大量のネットワークリソースを要求する正当なアプリケーションとを区別することは困難な場合もある。また、ウィルスはより賢くなって、検出を免れるようになってきている。例えば、ウィルスは、システム内にしばらくの間休止状態で居座って、起動信号を待っている場合もある。例えば、悪質なウィルスは、機密データを手に入れるまで休止状態で居座っていることもある。したがって、ウィルスが起動まで待機しているうちは、最小限の副次的な作用しか生成しないため、ウィルスの検出が困難である。

【発明の概要】
【００１３】
上述したものと他の必要性に応じて、本発明の実施形態は、ネットワークルータからエクスポートされたネットワークフローレコードを使用して、デバイスが受信/発信するトラフィックに関する情報を提供するシステム及び方法を提供する。ネットワークルータは、２つのネットワークデバイス（そのデバイスのトラフィックはルータを介して移動する）間の様々なタイプのネットワークトラフィックの通過を許可もしくは拒否するように構成することができる。提示する方法は、ネットワークルータからエクスポートされたネットワークフロー情報から得られた情報によりアクセス制御リストを生成し、そのアクセス制御リストをルータに適用するものである。

【００１４】
（本発明の）システムは、動的にネットワークを制御するものであり、ネットワークから複数のフローレコードを受信して、その複数のフローレコードを集計するフローレコード記憶装置と、集計されたフローレコードを受信して、その集計されたフローレコードを所定の基準に基づいて分析し、一つ以上のネットワークアドレスやポートを特定するデー

タ分析ツールと、特定されたネットワークアドレスを受信して、その特定されたネットワークアドレスやポートをアクセス制御リストに加えるネットワークデバイスとを備える。オプションとして、システムは、特定されたネットワークアドレスやポートを記憶し、その特定されたネットワークアドレスやポートをネットワークデバイスに提供するアクセス制御リスト記憶装置を備えていても良い。オプションとして、複数のフローレコードの一つ一つは発信元アドレスを有しており、複数のフローレコードを、発信元アドレスに基づいて集計してもよい。別の場合では、フローレコードは、対応する各フローにおいて転送されたバイトサイズを含んでおり、所定の基準は、発信元アドレスの一つ一つに対応するフローにおいて転送された総バイト数を含んでいてもよい。オプションとして、所定の基準を定義するために、データ入力デバイスがユーザからの入力を受け付けてもよい。

【００１５】

ネットワーク上のトラフィックに関する複数のフローレコードをコンポーネントから受信することにより、ネットワーク内のコンポーネントを監視することが出来る。オプションとして、データを定義するアクセス制御基準を受信し、そのアクセス制御基準を使用して複数のフローレコードを分析してもよい。アクセス制御基準を満たした送信先及び発信元ネットワークアドレスやレンジ及び/または送信先及び発信元ポートは特定されて、ユーザに提示される。ユーザは、特定されたアドレスやレンジ及び/またはポートを確認し、その後、それらをネットワークコンポーネントの１つに転送するように選択することができる。転送された場合、コンポーネントは、特定されたネットワークアドレス及び/またはポートを対応するアクセス制御リストに追加する。そして、そのアクセス制御リストが、特定されたネットワークアドレス及び/又はポートにトラフィックが到達することを防ぐ。 オプションとして、自動的に入力されたＡＣＬの入力事項を削除することを可能にする時間を、それぞれのアクセス制御リストについて設定することも出来る。

【００１６】

このように、ＡＣＬは、ルーターもしくはファイヤーウォールに適用されるトラフィック・フィルタリング・ルールである。ＡＣＬには、発信元ＩＰアドレスによってのみトラフィックを拒否または許可する標準ＡＣＬと、発信元及び送信先ＩＰアドレス、発信元及び送信先ポートによってトラフィックを拒否する拡張ＡＣＬの２種類のＡＣＬがある。したがって、本発明の実施形態は、特定されたアドレス又はポートを記憶する処理を含んでいる。

【００１７】

ネットワークトラフィックを動的に制御するシステムにおいて、そのシステムは、記憶システムにアクセスして、フローレコードを提供するフローレコード生成デバイスと、フローレコードを受信して記憶するフローレコード記憶装置と、記憶システムにアクセスし、所定の基準に基づいて、記憶された複数のフローレコードを評価するデータ分析デバイスとを備えている。もしフローレコードが所定の基準を満たした場合、そのアドレス/ポートは、確認とＡＣＬへの追加の承認を得るために、ユーザに転送してもよい。ユーザを支援するため、特定されたアドレス/ポートに対応するフローレコードデータもユーザに表示してもよい。

【００１８】

別の実施形態では、本明細書で開示される技術は、ＡＣＬに記載されたアドレス/ポートを評価する方法に関するものである。特に、ＡＣＬに記載されたアドレス/ポートに対応するフローレコードを、所定の基準に基づいて、評価することができる。それらのフローレコードが所定の基準を満たした場合、そのアドレス/ポートは、確認と承認のためにユーザに転送して、ＡＣＬ内で更新することも出来る。別の場合では、それらのフローレコードが所定の基準を満たさない場合、そのアドレス/ポートは、確認と承認のためにユーザに転送して、ＡＣＬから削除することも出来る。

【図面の簡単な説明】

【００１９】

本発明のある典型的な実施形態における、上述した目的と他の目的、特徴、利点は、添

付の図面と下記の詳細な説明により、より明らかになるであろう。
【００２０】
【図１Ａ】本発明のネットワークの実施形態による典型的なネットワークを示す図である。
【図１Ｂ】公知のフローレコード分析システムを示す図である。
【図２】典型的な公知のフローレコードを示す図である。
【図３】本発明の実施形態によるフローレコードを記憶する典型的な公知のテーブルを表す図である。
【図４】本発明の実施形態による集計されたフローレコードを記録する典型的なテーブルを表す図である。
【図５】本発明の実施形態によるフローデータを使用してＡＣＬを生成するためのシステムを示す図である。
【図６】本発明の本発明の実施形態によるネットワークノード、アクセス制御システム、フローレコード記憶システム間の通信を説明するサービスフロー図である。
【図７】本発明の実施形態による、フローレコードを使用してＡＣＬを生成する方法におけるステップを示したフロー図である。
【発明を実施するための形態】
【００２１】
図１Ａには、本発明の実施形態によるネットワーク１００が図示されており、一実施形態による、本発明のネットワークを表すブロック図が示されている。図示されているように、クライアントデバイス１０８ａ－１０８ｎは、ネットワークファブリック１１２を介して、サーバ１１０ａ－１１０ｎに接続されている。ネットワークファブリック１１２は、互いに接続されて複数のネットワークリンクを形成する、多数のルーティングデバイス１０６ａ－１０６ｎを含んでいる。クライアントデバイス１０８ａ－１０８ｎは、ルーティングデバイス１０６ａ－１０６ｎを介して、より詳しくは、ルーティングデバイス１０６ａ－１０６ｎによって形成された複数のネットワークリンクを通って、選択的にサーバ１１０ａ－１１０ｎにアクセスし、サービスを得る。当業者であれば理解していることであろうが、残念なことに、サーバ１１０ａ－１１０ｎにクライアントデバイス１０８ａ－１０８ｎがアクセスしやすいようにしたネットワークリンクは、同じネットワークリンクであっても、サーバ１１０ａ－１１０ｎを一つ以上のクライアントデバイス１０８ａ－１０８ｎによって不正使用されたり、悪用されやすくしてしまう可能性がある。例えば、一つ以上のクライアントデバイス１０８ａ－１０８ｎは、個別に、もしくは、協同して、サービス妨害攻撃などの攻撃を行ったり、そうでなければ、一つ以上のサーバ１１０ａ－１１０ｎ、ルーティングデバイス１０６ａ－１０６ｂ、複数のコンピュータエレメントを相互に接続する複数のリンクを被害に合わせたりする。本発明によると、多数のセンサ１０４ａ－１０４ｎによって補完されたディレクタ１０２を使用して、そのようなネットワークリンクの不正使用や悪用を検出して阻止する。その処理については、以降に詳述する。図示した実施形態では、センサ１０４ａ－１０４ｎは、分散して配置されている。別の実施形態においては、センサ１０４ａ－１０４ｎのいくつかもしくは全てをルーティングデバイス１０６ａ－１０６ｂと一体にして配置してもよい。
【００２２】
ネットワーク１１２は、多国籍企業の企業ネットワークやインターネットなどの、私的および公的ネットワークや相互接続型ネットワークなど、広い意味範囲でのネットワークを表している。クライアント１０８ａ－１０８ｎやサーバ１１０ａ－１１０ｎなどのネットワークノードは、個々のユーザマシン、ｅコモースのサイトなどを含む、当技術分野において知られている広い範囲のこれらの要素を表している。前記したように、ルーティングデバイス１０６ａ－１０６ｎは、ネットワークトラフィックを転送する広い範囲の機器を表しており、それらに限定されるわけではないが、従来のルータ、スイッチ、ゲートウェイ、ハブなどを含んでいる。
【００２３】

理解しやすいように、一つのディレクタ１０２と、一握りのネットワークノード、クライアント１０８ａ－１０８ｎ、サーバ１１０ａ－１１０ｎ、ルーティングデバイス１０６ａ－１０６ｎ及びセンサ１０４ａ－１０４ｎのみを図示しているが、以下の説明から、当業者は、本願は、２つ以上のディレクタ１０２と図示されている数とは多少異なる数のネットワークノード、ルーティングデバイス１０６ａ－１０６ｎ、センサ１０４ａ－１０４ｎを用いて実施可能であることを理解するであろう。特に、本願は、２つ以上のディレクタ１０２を用いて実施可能である。２つ以上のディレクタ１０２を使用する場合、一つ一つのディレクタ１０２に対して、センサ１０４ａ－１０４ｎの一部に関する責任を課してもよい。そして、２つ以上のディレクタ１０２は、集団で後述する責任を果たすために、ディレクタ１０２の一つが「マスタ」として機能し（その他が「スレーブ」として機能する）マスタ/スレーブ関係でお互いに関連づけたり、お互いにピアとして関係付けてもよいし、階層構造に構成されていてもよい。

【００２４】

ディレクタ１０２の動作は、下記に詳述する。また、ディレクタ１０２は、下記に詳述するように、フローデータ結合システムとアクセス制御デバイスとを備えている。

【００２５】

図１Ｂに図示しているように、既知のネットワーク利用分析システム１１１は、一実施形態において、データ収集システムサーバ１３０とデータ記憶システム１４０を備えている。リスナーとも呼ばれる、データ収集システムサーバ１３０は、記憶、分析のために、全ての様々なネットワークエージェント１２０からフローデータグラム１９０を収集する中央サーバである。データ収集システムサーバ１３０は、フローレコード生成デバイス１２０からフローレコード１９０を受信する。フローレコード生成デバイス１２０は、ＩＰネットワーク１１４の一部であるネットワークデバイスである。一実施形態においては、ネットワーク１１４は、インターネット１１５を含んでいる。

【００２６】

一般的に、フローレコード生成デバイス１２０は、未加工のネットワークトラフィックを「回線速度」で処理し、そのトラフィックからフローレコードを生成することができるほぼ全てのネットワークデバイスを含んでいる。典型的なフローレコード生成デバイス１２０は、ルーター、スイッチ、ゲートウェイなどを含んでおり、場合によっては、アプリケーションサーバ、システム、ネットワーク探査機を含む場合もある。ほとんどの場合において、フローレコード生成デバイス１２０によって生成された複数の小さなフローレコードは、フローレコード１９０のストリームとして、データ収集システムサーバ１３０にエクスポートされる。

【００２７】

ネットワークトラフィック情報とインターネットプロトコルトラフィック情報を収集するために、様々なネットワークプロトコルがネットワーク機器上で機能している。通常、ルーターなどの様々なネットワークエージェント１２０は、フローレコードを生成可能なフロー特徴を有している。フローレコード１９０は、通常、ネットワークエージェント１２０から、ユーザ・データグラム・プロトコル（ＵＤＰ）パケットもしくはストリーム・コントロール・トランスミッション・プロトコル（ＳＣＴＰ）パケットでエクスポートされ、フローコレクタを使用して収集される。より詳しい情報が必要な場合は、 http://www.ietf.org/html.charters/ipfix-chapter.htmlに掲載の、インターネット・プロトコル・フローインフォメーション・エクスポート（ＩＰＦＩＸ）のインターネット・エンジニアリング・タスク・フォース（ＩＥＴＦ）標準を参照されたい。

【００２８】

上述したように、通常、フローレコード１９０は、ＵＤＰもしくはＳＣＴＰを使用して、ネットワークエージェント１２０から送信される。効率性の理由から、ネットワークエージェント１２０は、一度フローレコードがエクスポートされた後は、そのフローレコードは記憶しておかない。ＵＤＰのフローでは、もしフローレコード１９０がネットワークエージェント１２０とデータ収集サーバ１３０との間で、ネットワークの混雑により失わ

れた場合、ネットワークエージェント１２０がフローレコード１９０を再送する方法はないため、そのフローレコード１９０は永遠に失われたままとなる場合がある。ルーターのプロセッサに不必要に負荷をかけてしまうことを避けるため、フローは、インターフェース毎を基本にしてイネーブルしてもよい。したがって、フローレコード１９０は、一般的に、二重カウントを避け、ネットワークエージェント１２０の仕事を省くために、フローがイネーブルされたインターフェースに入力されたパケットに基づいている。また、ネットワークエージェント１２０は、パケットが失われたときのために、複数のフローレコードをエクスポートすることもできる。

【００２９】

ネットワークのフローは多くの方法で定義されてきた。一実施例においては、フローは、５つの要素からなっており、発信元ＩＰアドレス、送信先ＩＰアドレス、発信元ＴＣＰポート、送信先ＴＣＰポート、ＩＰプロトコルを定義する一方向配列のパケットである。通常、ネットワークエージェント１２０は、フローが終了したと判断したとき、フローレコードを出力する。ネットワークエージェント１２０は、既存のフローに対して新しいトラフィックを発見したとき、エイジングカウンタをリセットする、「フローエイジング」によって、これを行なう。また、ＴＣＰフローにおけるＴＣＰセッションの終了によってネットワークエージェント１２０は、フローを終了させる。ネットワークエージェント１２０は、フローが継続していても、定められた間隔でフローレコードを出力するように構成することも可能である。他の方法としては、管理者がネットワークエージェント１２０におけるフロー特性を定義することもできる。

【００３０】

フローレコード１９０は、所与のフロー中のトラフィックに関する様々な情報を含むことが出来る。図２に表されるように、フローレコード２００の典型的な例は下記の値を含んでいる。特に、典型的なフローレコード２００は、使われているフローのタイプを特定するバージョンナンバー２１０を含んでいる。シーケンスナンバー２２０は、フローレコードを特定するものである。

【００３１】

引き続き図２に関して説明すると、入出力インターフェース簡易ネットワーク管理プロトコル（ＳＮＭＰ）指標２３０を使って、ＳＮＭＰを介して動的にネットワークデバイスを特定することができる。ネットワーク管理システムは、管理者が注意する必要のある状態をみつけるために、ＳＮＭＰを使ってネットワークに接続されたデバイスを監視している。また、ＳＮＭＰは、アプリケーション・レイヤー・プロトコル、データベーススキーマ、一セットのデータベースオブジェクトを含む一セットのネットワーク管理の規格で構成されている。ＳＮＭＰは、管理データを管理されるシステムにおける変数の形で表し、その変数がシステムの構成を表している。これらの変数を、管理する側のアプリケーションは、問い合わせる（時々、設定する）ことができる。モジュラーデバイスは、スロット式のハードウェアが取り付けられたり、取り外されたりする度に、そのＳＮＭＰ指標を付けなおすこともできる。ＳＮＭＰ指標値は、通常、起動時に割り当てられ、次回の起動まで同じ指標値が保たれる。

【００３２】

引き続き図２について説明すると、フローレコード２００の一つ一つは、通常、フロー開始/終了時間のタイムスタンプ２４０を含んだ、データ通信に関する情報を含んでいる。データ通信に関する他の情報として、フローにおけるバイト数とパケット数２５０に関する情報を含んでいる。発信元アドレス及び送信先アドレス、発信元アドレス及び送信先アドレスのポート番号、伝送プロトコル、サービスの種類（ＴｏＳ）を記述したヘッダーデータ２６０などの、データ転送の条件もフローレコード２００には含まれている。通信制御プロトコル（ＴＣＰ）について、フローレコード２００は、フロー中の全てのＴＣＰフラグの集合を記載していてもよい。ＴＣＰについてよく知られているように、データの転送の際には、例えば、応答確認フラグ（ＡＣＫｓ）のペアなどによって、一連の通信確認を行なっている。ＴＣＰフラグの不均衡は、メッセージは送信されたが受信されなかっ

たという、メッセージの送信失敗を表す。

【００３３】

ＵＤＰの転送メカニズムにおいては信頼性がないが、そのことは、抽出されたフローから得られる測定の正確性に深刻な影響を与えるわけではない。例えば、もしフロー・サンプルが失われたとしても、次のポーリングインターバルが経過すれば、新しい値が送信される。したがって、パケットフローサンプルが失われても、若干有効サンプリングレートが下がるだけである。サンプル抽出法が使用された場合、ＵＤＰペイロードは、抽出フロー・データグラムを含んでいる。したがって、それぞれのデータグラムは、フローレコード１９０全体を含む代わりに、フロー・ヴァージョン、データグラムの送信元エージェントのＩＰアドレス、シーケンス番号、データグラムが含むサンプルの数およびフローサンプルなどの情報を提供する。

【００３４】

引き続き図１Ｂについて説明すると、データ収集システムサーバ１３０は、コミュニケーションリンク１７０を介して、フローレコード生成デバイス１２０からストリーミングでフローレコード１９０を受信する。一実施形態においては、フローレコード生成デバイス１２０は、ネットワーク１１４に含まれていてもよい。別の実施形態においては、フローレコード生成デバイス１２０は、機能的にはネットワーク１１４と結合していても、物理的にはネットワーク１１４からは離れた位置に実装してもよい。図１Ｂでは、フローレコード生成デバイス１２０は、データ収集システムサーバ１３０とは分離して配置されているが、別の実施形態においては、フローレコード生成デバイス１２０は、データ収集システムサーバ１３０の一部であってもよい。

【００３５】

データ分析システムサーバ１５０は、フローレコード１９０にアクセスし、それを使用して所定のネットワーク利用統計分析を行なう。一般的に、データ分析システムサーバ１５０は、ネットワークの混雑、ネットワークセキュリティの不正利用、悪用および盗用などの、一つ以上のネットワーク利用に関する問題を解決するために定義された様々な統計モデルを実装している。データ分析システムサーバ１５０は、フローレコード１９０と前記した統計モデルを使用して、分析結果を生成する。その分析結果は、その後データ記憶システム１４０に記憶することもできる。統計結果を記憶する典型的な実施形態は、以降に詳述する。フローデータを分析することにより、データ分析システムサーバ１５０は、ネットワークにおけるトラフィックフローとトラフィック量の実態を表すことが出来る。データ分析システム１５０の用途については、以降に詳述する。

【００３６】

一側面において、データ分析システムサーバ１５０は、フローレコード１９０の双方向的な分析のために、ユーザインターフェース１６０に対応することもできる。ユーザインターフェース１６０は、キーボード、マウス、タッチパッド、ディスプレイスクリーンなど、当技術分野で公知の任意の入出力機器を含んだものでよい。一例においては、統計結果の視覚的表示をユーザインターフェース１６０において表示スクリーンに出力してもよい。

【００３７】

一実施形態においては、データ分析システムサーバ１５０は、発明の様々な実施形態に基づいてネットワーク利用データを分析するために、一つ以上のコンピュータやサーバ上で実行可能なコンピュータソフトウエアプログラムを有している。データ記憶システム１４０は、データ収集システムサーバ１３０やデータ分析システムサーバ１５０の外部に図示されているが、別の場合では、データ記憶システム１４０は、サーバ１３０やサーバ１５０の内部に配置することもできる。データ記憶システム１４０は、当技術分野における任意の揮発性メモリ（例、ＲＡＭ）および/または非揮発性メモリ（例、ハードディスクドライブや他の永続記憶装置）によって構成することができる。

【００３８】

図３には、複数のフローレコード２００を記憶システム１４０に格納するための典型的

な表３００が図示されている。具体的には、図示された表３００は、ｎ個の受信したフローレコード２００の一つ一つを識別するフローレコード識別子を割り当てた列を有している。表３００は、また、各受信フローレコード２００におけるＩＰ送信元アドレス３２０を含む列、各受信フローレコード２００のタイムスタンプ３３０を含む列、受信フローレコード２００に対応するフローのバイトサイズ３４０を含む列を有している。

【００３９】

図３の例では、典型的なフロー表３００は、フローレコード識別子３１０によって示されるとおり、７つのフローを表した７つのフローレコードを有している。この特定例では、７つフローは、３つの固有の送信元アドレス３２０から発信されている。例えば、フローレコード１、２、４、７は、全て同じ送信元から発信されている。図示されているわけではないが、例示したフロー表３００は、図２に図示されているものと同様に、送信先、ＱｏＳ、伝送プロトコルなどのフローレコード２００の他の側面を含んでいてもよい。引き続き図３に示す典型的なフロー表３００を説明すると、タイムスタンプ３３０の値は、各フローに対応する時刻を表し、バイトサイズ３４０の値は、列３１０において識別され、リストアップされたフローレコード１－７に対応するフローの一つ一つのサイズを表している。

【００４０】

次に、図４を参照すると、送信元ＩＰアドレス４２０にしたがって典型的なフローデータ表３００のデータが集計された、集計フロー表４００が図示されている。通常、集計処理は、予め定義された一期間以上の期間にわたって行なわれる。例えば、典型的な集計フロー表４００は、表３００におけるそれぞれの送信元ＩＰアドレス４２０に対応するフローレコードの合計数４１０を記載した列を含んでいる。集計フロー表４００は、さらに、表３００における送信元ＩＰアドレス４２０の一つ一つに対応する複数のフローの合計バイトサイズを記載している。集計フロー表４００の用途については、以降に説明する。当然のことながら、フローレコード表３００と同様に、フローレコード２００は、例えば、図２の典型的なフローレコード２００に記載されている一つ以上のフローレコードのカテゴリに基づいて、任意の方法で合計してもよい。

【００４１】

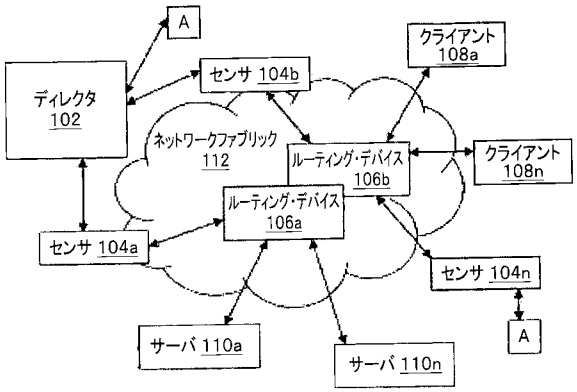
次に、図７を参照して、本発明の実施形態によるアクセス制御方法７００を説明する。ステップ７１０において、上述したように、公知の技術によってネットワークコンポーネントのトラフィックを監視し、ステップ７２０において、フローレコードを収集する。通常、ステップ７１０と７２０は、ルーター、ハブ、サーバなどのほとんどのネットワークコンポーネントに既に備わっている機能を使って実行することが出来、ステップ７１０と７２０を使って、例示したフローレコード表３００などのように、フローレコードを収集して記憶することができる。ステップ７２０で収集されたフローレコードは、ステップ７３０で分析される。例えば、上述したような集計フローレコード表４００を形成するなど、複数のフローレコードを合計することもできる。

【００４２】

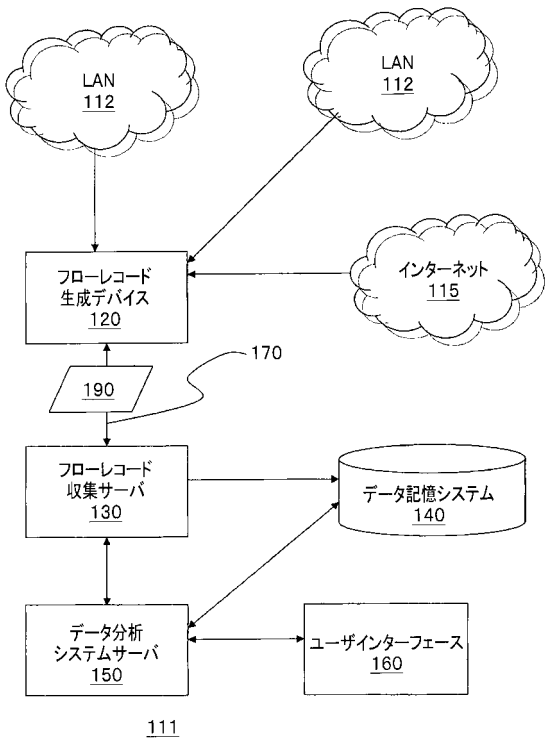
アクセス制御方法７００の説明を続けると、ステップ７４０において、アクセス制御条件が定義される。デフォルトの予め定義されたアクセス制御条件を使用して、フローレコードを評価してもよい。例えば、ある特定の割合を占めるトラフィックやある特定量のトラフィックに関連付けられたアドレスやポートを特定してもよい。一例としては、一番数の多いトランザクション、タイムスタンプ３３０の時刻、転送データ４３０の一番大きいデータ量などに基づいて、送信元ＩＰアドレス４２０に対するアクセスを制限することができる。これらの基準は、ある特定の基準について最大閾値を決めるなどして設けられた、客観的なものであってもよいし、発信元ＩＰアドレスまたは送信先ＩＰアドレスの基準、及び/またはネットワークリソースを最も多く使用する、もしくは最も高い頻度で使用する消費者に対応するポートの基準（もしくは他の基準）などの基準の順位付けに基づく主観的なものであってもよい。必要に応じて、これらの基準は、ユーザが提供することも出来る。

【００４３】
これらの基準を満たした発信元ＩＰアドレス/送信先ＩＰアドレス、またはポートは、ステップ７５０において、簡単なロジックで特定することが出来る。ステップ７６０では、特定された発信元ＩＰアドレスや送信先ＩＰアドレス及び/またはポートの識別子をユーザに提示することが出来る。ユーザに承認されれば、特定されたネットワークデバイスのこれらの送信先ＩＰアドレス（もしくは他のデバイス識別子）を、ステップ７７０において、ＡＣＬに加えて、ネットワークデバイスに、特定されたポートやアドレスに対応するトラフィックを無視または転送拒否するように要求することが出来る。
【００４４】
次に、図５を参照して、本発明の実施形態によるアクセス制御システム５００を説明する。上述した通り、フローデータ記憶システム１４０は、未加工のフローレコード１９０を受信することができる。フローデータ記憶システム１４０は、上述したように、システムの目的を達成するために、様々な方法でフローレコード１９０を集計することも出来るし、フローレコードを未加工の状態で記憶することもできる。データ分析サーバ１５０は、フローレコードにアクセスし、ユーザインターフェース１６０を介して受信及び/または定義された、ＡＣＬに加えるべきネットワークアドレスまたはポートを定める基準に基づいて、フローレコードを評価する。当然のことながら、所定の基準をある期間の間続いて満たさないポート又はアドレスを自動的に特定して、ＡＣＬから削除するようにユーザに提示してもよい。通常、フローレコード内の全てのアドレスや、所定の基準に基づいて動的に特定されたＡＣＬに記載されたアドレスは、管理者が検討できるように、ユーザインターフェースに転送される。そして、管理者は、特定されたポート/アドレスのＡＣＬへの追加もしくはＡＣＬからの削除を承認する。
【００４５】
ＡＣＬ５９０は、ネットワークデバイス５２０上にあってもよいし、また、必要に応じて、ＡＣＬ記憶システム５３０に記憶しておき、ＬＡＮ５１０やインターネットを介してトラフィックを受信するネットワークデバイス５２０に転送するようにしてもよい。ネットワークデバイス５２０は、通常、ＡＣＬがネットワークデバイス５２０またはオプションのＡＣＬ記憶装置５３０に記憶されているＡＣＬにおいて特定された機器に対応するあらゆるトラフィックの転送を拒否する。すなわち、ＡＣＬに記載されたアドレスへのトラフィックや、そのアドレスからのトラフィックは、ネットワークデバイス５２０に到達しても、ネットワーク５１０、１１５を通って転送されないことになる。トラフィックの通信が時間切れになると、その通信は、記憶装置から削除され、指定された送信先へ届くことはない。
【００４６】
次に、図６のサービスフロー図６００を参照すると、ネットワークノード６１０は、ネットワークトラフィックを記述したフローレポート６５０をネットワーク監視システム６２０に転送することが表されている。上述したように、ネットワーク監視システム６２０は、複数のフローレコード６５０を収集して記憶することが出来る。記憶されたフローレコード６６０は、所定の条件に基づいてその記憶されたフローレコード６６０を評価して、自動的にネットワークアドレス/ポートを特定するアクセス制御システム６３０がアクセスすることができる。特定されたアドレスは、ユーザインターフェース６４０に確認のために転送される。特定されたアドレス/ポートがユーザによって（ＡＣＬへの追加について）許可されると、そのアドレス/ポートは、ＡＣＬを実施するためのＡＣＬ更新データ６８０として、ネットワークノード６１０に送信される。
【００４７】
典型的な実施形態を参照して本発明について説明してきたが、本発明の範囲を逸脱することなく、様々な追加、削除、代替および他の修正例が実現可能である。したがって、本発明は、上述の説明により限定されるものではなく、添付の請求の範囲によってのみ制限されるものである。

【図１Ａ】



【図１Ｂ】



（従来技術）

【図２】

典型的フローレコード
200

フロー・バージョンナンバー	210
シーケンスナンバー	220
入出力インターフェースSNMP指標	230
フロー開始/終了タイムスタンプ	240
フローにおけるバイト数とパケット数	250
発信元IPアドレス及び送信先IPアドレス、発信元及び送信先ポート番号、IPプロトコル、サービスの種類(ToS)を記述したレイヤー3ヘッダ	260
TCPフローに関して、フローが生きている間観察された全てのTCPフラグの集合	270

（従来技術）

【図３】

フローレコード番号 310	発信元IPアドレス 320	タイムスタンプ 330	バイトサイズ 340
1	xxx.xxx.x.1	t_1	10
2	xxx.xxx.x.1	t_2	20
3	xxx.xxx.x.2	t_3	1000
4	xxx.xxx.x.2	t_4	2000
5	xxx.xxx.x.1	t_5	30
6	xxx.xxx.x.3	t_6	10
7	xxx.xxx.x.1	t_7	40

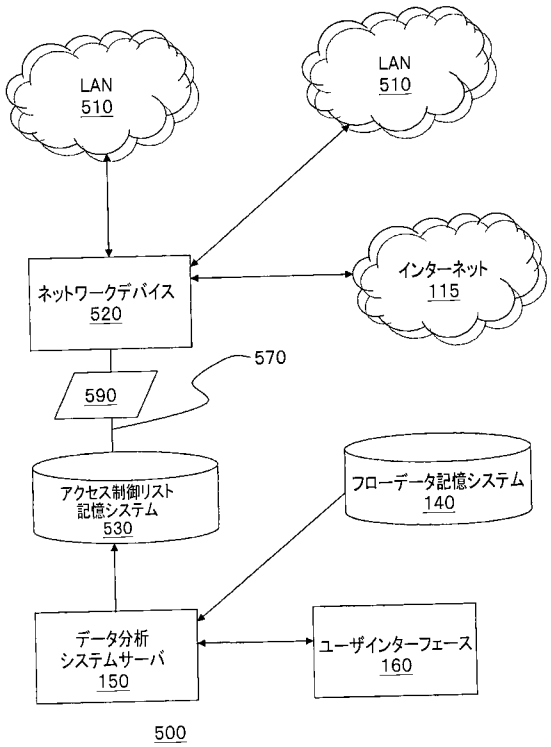
典型的なフロー表 300

【図４】

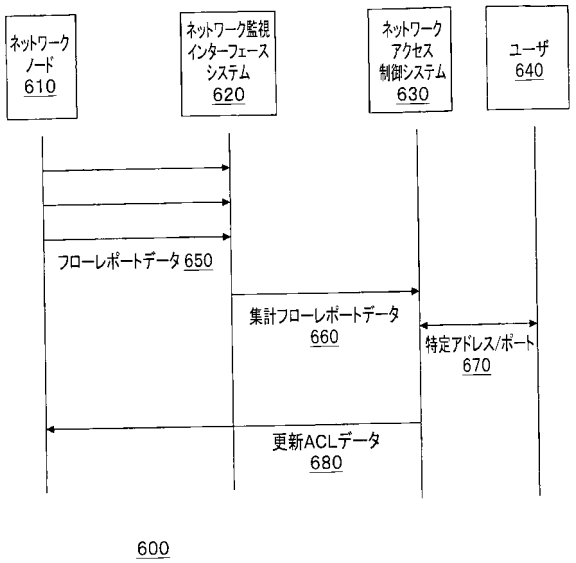
フローレコード合計数 410	発信元IPアドレス 420	総バイトサイズ 430
4	xxx.xxx.x.1	100
2	xxx.xxx.x.2	3000
1	xxx.xxx.x.3	10

集計フロー表 400

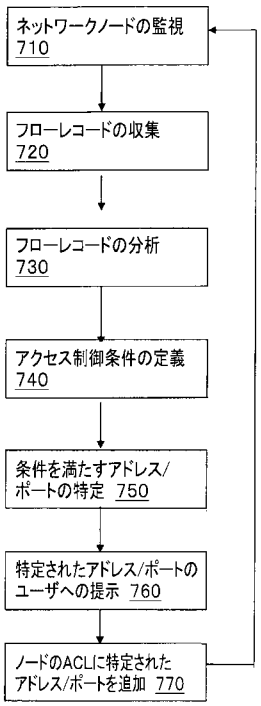
【図５】


LAN
510
LAN
510
ネットワークデバイス
520
インターネット
115
570
590
アクセス制御リスト
記憶システム
530
フローデータ記憶システム
140
データ分析
システムサーバ
150
ユーザインターフェース
160
500

【図６】


ネットワーク
ノード
610
ネットワーク監視
インターフェース
システム
620
ネットワーク
アクセス
制御システム
630
ユーザ
640
フローレポートデータ 650
集計フローレポートデータ
660
特定アドレス/ポート
670
更新ACLデータ
680
600

【図７】


ネットワークノードの監視
710
フローレコードの収集
720
フローレコードの分析
730
アクセス制御条件の定義
740
条件を満たすアドレス/
ポートの特定 750
特定されたアドレス/ポートの
ユーザへの提示 760
ノードのACLに特定された
アドレス/ポートを追加 770

フロントページの続き

(56)参考文献 特開２００４－３０２９５６（ＪＰ，Ａ）
特表２００５－５１８７６４（ＪＰ，Ａ）
特開２００４－３２８３０７（ＪＰ，Ａ）
特開２００５－２１０６０１（ＪＰ，Ａ）
特開２００６－３５２８３１（ＪＰ，Ａ）
特開２００５－０４５６４９（ＪＰ，Ａ）
特開２００６－２５３７５７（ＪＰ，Ａ）
特開２００６－３４５２６８（ＪＰ，Ａ）
米国特許出願公開第２００６／０２８２８９５（ＵＳ，Ａ１）
特開２００５－１９７８２３（ＪＰ，Ａ）
特開２００２－１２４９９６（ＪＰ，Ａ）
米国特許出願公開第２００４／００５４９２５（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ １３／００
Ｈ０４Ｌ １２／００－１２／９５５