2-6　実ネットワークトラフィック可視化システムNIRVANAの開発と評価

2-6 Development and Evaluation of NIRVANA: Real Network Traffic Visualization System

鈴木宏栄　衛藤将史　井上大介
SUZUKI Koei, ETO Masashi, and INOUE Daisuke

要旨

情報通信セキュリティ研究センターインシデント対策グループは、nicterシステムの一部である世界地図攻撃可視化システムAtlasを応用して、実ネットワークトラフィック可視化システムNIRVANA（nicter real-network visual analyzer）を開発した。NIRVANAはネットワークを流れる実トラフィックをリアルタイムで可視化し、組織のネットワーク管理者がネットワークの利用状況やボトルネック、機器の設定ミスや不正な通信等を速やかに把握することを目的としたシステムである。

We have developed a real network traffic visualization system named “NIRVANA”. The NIRVANA is based on a visualization engine in the nicter called Atlas, which animates darknet traffic on a world map in a real-time manner. The NIRVANA visualizes livenet traffic, namely traffic in real operating networks, and significantly helps network administrators to promptly grasp comprehensive network status and network troubles such as bottlenecks, configuration errors and irregular communications.

[キーワード]
ネットワークモニタリング，ネットワーク管理，可視化
Network monitoring, Network administration, Visualization

1　はじめに

仮想化技術の発達、クラウドコンピューティングの普及などにより、我々をとりまくネットワーク環境は日々複雑化している。ネットワーク管理者にとって、それらの複雑化したネットワークを安定運用するためには、トラフィックの状況を迅速に把握することが重要である。そのため、ネットワーク管理者は高度なスキルを要求され、運用管理がさらに困難となっているのが実状である。

情報通信セキュリティ研究センターインシデント対策グループでは、nicterシステム[1][2]の開発を通じて、広域のネットワークモニタリングによってセキュリティインシデントの早期検知と、迅速な原因究明の手法について研究を行った。その中で開発された各種の可視化システムは、分析者が攻撃の状況をリアルタイムかつ直観的に理解するためのシステムとして有効に活用された[3][4]。

nicterの可視化システムの多くはダークネット（未使用IPアドレスブロック）に届くトラフィックを可視化したものであるが、これを実ネットワーク（ユーザ端末やサーバ等が実際に接続されたネットワーク）に応用することで、ネットワーク管理者の迅速な対応を可能にする強力な支援ツールとなり得る。本稿では、nicterの世界地図攻撃可視化システムAtlasを応用して開発された、実ネットワークトラフィック可視化システムNIRVANAについて詳説する。

以下、**2**で世界地図攻撃可視化システムAtlasの特徴について述べ、**3**でNIRVANAを構築する目的とその要件についてまとめる。**4**でNIRVANAの概要を示し、**5**でシステムの性能評価と実運用による効果について述べる。**6**でまと

めと今後の課題について述べる。

2 世界地図攻撃可視化システム Atlas

2.1 Atlas の特徴

nicter は、広域のネットワークトラフィックを観測することによってイベントを解析しインシデントを検出・分析するマクロ解析システムと、マルウェアの検体を収集・解析して、それらの挙動を抽出するミクロ解析システム、これら2つの解析結果を分析し、インシデントとマルウェアの挙動を対応づけする相関分析システムによって構成される。

世界地図攻撃可視化システム Atlas は、マクロ解析システムの中に位置し、分析者が観測対象のネットワークに到達する攻撃トラフィックをリアルタイムで描画することにより、攻撃の地理的な傾向を把握するためのシステムである（図1）。攻撃トラフィックは、パケット毎に1つのパケットオブジェクト（円錐などの3D図形）として表現され、送信元国から送信先国へ軌道を描きながら移動するアニメーションとして描画される。これにより、例えば世界中からの分散サービス妨害攻撃（DDoS攻撃）や、ボットネットがその感染を広げる様子（大規模スキャン）などを直感的に把握し、その後の詳細な分析へと進むことができる。

2.2 Atlas の実ネットワークへの適用時の課題

Atlas は、ダークネットを観測し、飛来するパケットの地域性を世界地図上で表現する目的に最適化されており、実ネットワークトラフィックを可視化するためには以下4つの課題があった。

課題1：柔軟な背景画像の切り替え

Atlas は、世界各国からの攻撃の地域性を把握することに特化したシステムであるため、システム設計上、背景画像の切り替えを頻繁に行うことを想定していなかった。実ネットワークへの適用を考えた場合、システム毎に様々なネットワークトポロジが存在し、さらにそのトポロジが頻繁に変化することから、システムに応じた背景画像のカスタマイズとプログラムの書き換えが必要であった。

課題2：障害調査時のノイズトラフィックの除去

ダークネットに飛来するトラフィックは正・不正で区別する必要がなく、大半のパケットを不正なものと見なすことが出来るが、これに対して実ネットワークにおいては、その殆どが正常なトラフィックである。実ネットワークに何らかの障害

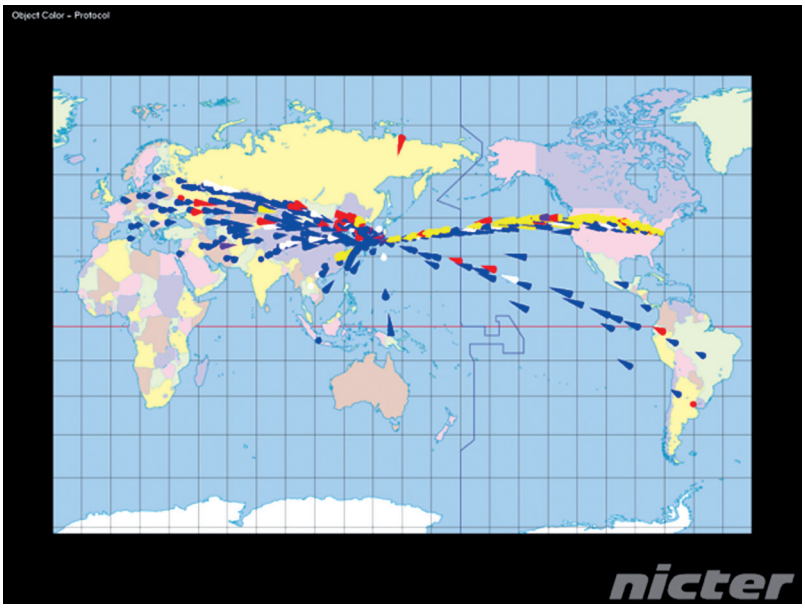

図1 nicter の世界地図攻撃可視化システム Atlas

が発生した場合、ネットワーク管理者は膨大なトラフィックの中から観測対象以外のノイズトラフィックを除外する必要があるが、Atlasはこのような絞り込み機能を有していなかった。

課題3：トラフィック流量の表現

ネットワーク管理者にとって、トラフィックの流量を把握することによりネットワークの使用率を調査し、最適なネットワークを構築することは重要な使命の1つである。これに対して、Atlasはトラフィックの表現として1パケットごとにリアルタイム描画する表現方法をとっているため、トラフィックの種類等を直観的に把握することはできるが、その流量を正確に把握することは難しかった。

課題4：膨大なトラフィックのリアルタイム処理

実ネットワークではダークネットと比較してトラフィック量が膨大となるため、グラフィック描画の性能限界によりパケット単位の描画が困難となることが想定された。そのため、可視化処理をより軽量となるよう工夫をするとともに、実運用に適したトラフィック処理性能を満たすかどうかの精密な評価検証を行う必要があった。

3　NIRVANAの目的と要件

2で述べた世界地図攻撃可視化システムAtlasの課題を踏まえ、ここでは実ネットワークを対象としたトラフィック可視化システムNIRVANAの構築の目的とシステム要件について述べる。

3.1　NIRVANAの目的

NIRVANAは、実ネットワークを流れるトラフィックをリアルタイムで「見える化」することで、ネットワークの輻輳・切断等の障害や、設定ミス等を瞬時に見つけ出すことを可能にし、ネットワーク管理者の負荷を軽減することを目的とする。NIRVANAの導入によって、クラウドサービスプロバイダや通信キャリアなどのネットワーク運用が迅速化・効率化され、管理コストの大幅な低減が期待できる。

3.2　システム要件

Atlasを応用し、実ネットワークの可視化システムを構築するために、**2.2**で述べた課題を考慮し、以下(1)～(4)のシステム機能要件を定義する。

(1) 背景画像切り替え機能

背景画像の切り替えを行う仕組みを持たないという課題(**課題1**)を解決するため、NIRVANAでは背景画像切り替え機能を実装する。様々なネットワークトポロジの可視化に対応するため、プログラムの書き換えなしに、ネットワーク管理者が、自由に背景をカスタマイズ可能とする。

(2) トラフィック絞り込み機能

ノイズトラフィックの除外(**課題2**)に対応するため、トラフィック絞り込み機能を実装する。ネットワークに障害が発生した場合、管理者が膨大なトラフィックの中から、観測したいトラフィックのみを強調、または観測したい対象トラフィック以外のノイズトラフィックを除外できるよう、可視化インタフェースからトラフィックの強調や絞り込みを行うことができるようにする。

(3) パケットの詳細表示機能

さらに課題2の絞り込みを迅速に実現するためには、管理者が目的とするトラフィックの詳細な情報に即時的にアクセスできることも重要である。そのため、可視化画面上からパケットの詳細を参照可能となるように、詳細情報表示のための機能を追加する。

(4) データ流量の可視化機能

トラフィック流量の表現(**課題3**)と、膨大なトラフィックのリアルタイム処理(**課題4**)を実現するため、ネットワーク管理者がトラフィック流量(パケット数、データ量)を把握でき、かつ、トラフィックの可視化を軽量に処理できるよう、機能の追加と処理の高速化を図る。

4　実装

ここでは、**4.1**でNIRVANAシステム全体の構成を述べ、**4.2**以降では、**3.2**で述べたシステム要件を満たすために実装したNIRVANAの各種機能を示す。

4.1　システム構成

・デフォルトシステム構成

NIRVANAは、観測対象ネットワークからトラフィックを収集する「センサシステム」、収集した

トラフィックを集約する「ゲートシステム」、集約されたトラフィックをネットワークトポロジ図上に3Dで可視化する「可視化システム」という3つのサブシステムからなる。ネットワーク管理者は、可視化システム上で稼働する可視化インタフェース（GUI）により、ネットワークの状況を把握する。このように、NIRVANAではネットワークの複数箇所にセンサを設置して複数のネットワークトラフィックを集約し、観測することが可能である。

なお、NIRVANAの（可視化システムを除く）構成要素は、nicterで開発したシステムとの共通化が図られている。NIRVANAの典型的なシステム構成を図2に示す。

・可視化システム単体構成

NIRVANAの可視化システムは、可視化システム自身のネットワークインターフェイスカード（NIC）をキャプチャすることにより、単体で稼働させることも可能である。この機能を用いることで、小型のラップトップPC等を可視化システムとして利用し、障害の発生が疑われるネットワーク機器のミラーポートのトラフィックを直接的にモニタリングするなど、機動的な対応が可能となる。NIRVANAの可視化システム単体構成を図3に示す。

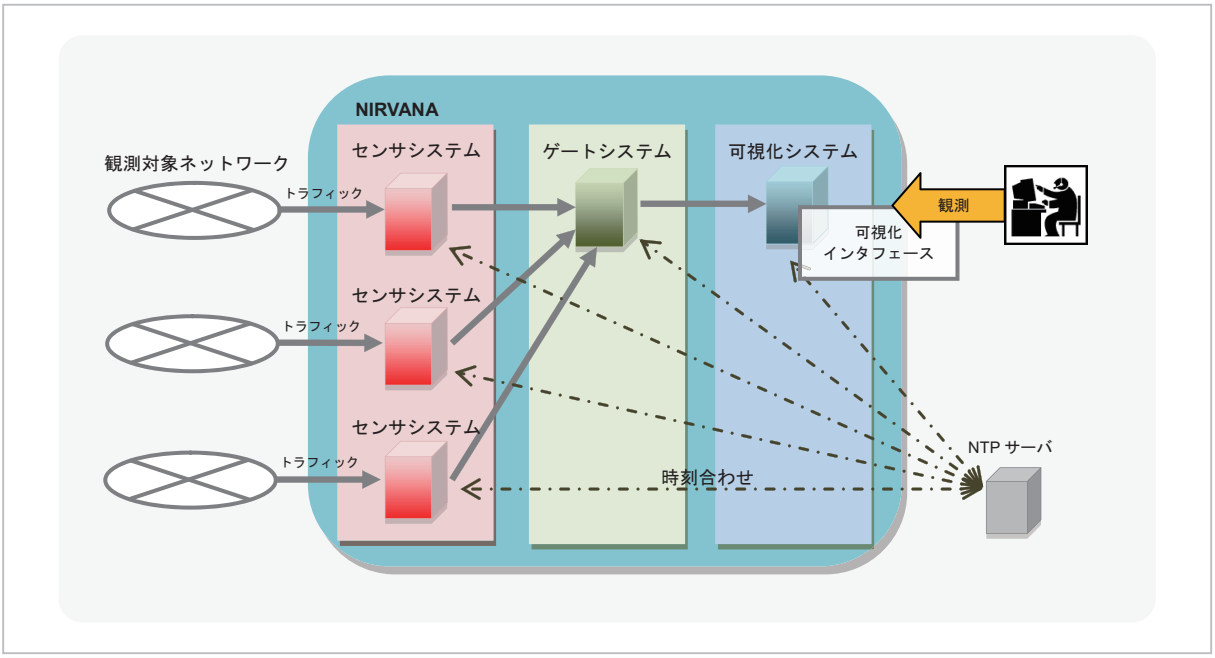

図2 NIRVANAデフォルトシステム構成

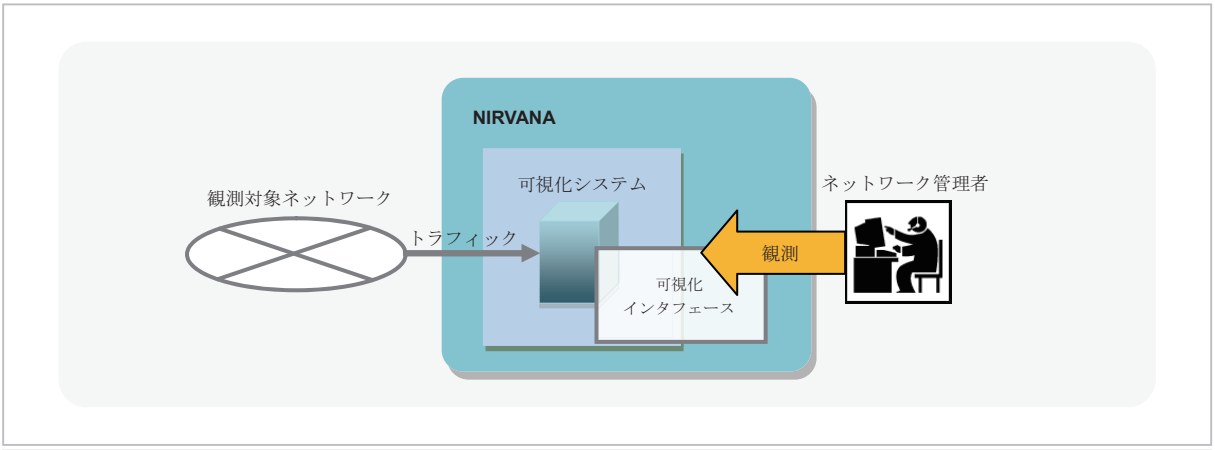

図3 NIRVANA可視化システム単体構成

4.2 背景画像切り替え機能

3.2 のシステム要件(1) 背景画像切り替え機能で定義した機能要件を満たすための実装方法について述べる。

NIRVANAでは、様々なネットワークトポロジの可視化に対応可能とするため、作画ツールによって作成されたネットワーク図を可視化システムが自動的に読み込めるよう実装した。作画ツールには、ネットワーク機器のオブジェクトにIPアドレス等のデータを割り当てられることや、作画の容易性、ツールの普及度などを考慮し、Microsoft Visio 2007を採用した。

NIRVANAでトラフィックを可視化するためには、ネットワークトポロジの背景画像、トラフィックの送信元／送信先となるネットワーク機器のオブジェクトの座標と、座標に対応するIPアドレス(もしくはIPアドレスレンジ)の情報が必要となる。

Microsoft Visio 2007を用いてネットワーク機器のオブジェクトを配置し、配置したオブジェクトのデータフィールドに、IPアドレス(レンジ)を定義する。データフィールドとは、オブジェクトに値を付与することができるラベルであり、これを定義することにより、オブジェクトとIPアドレスとを紐付けることができる。可視化の際には、送信元／送信先IPアドレスを基に、それらに対応するネットワーク機器のオブジェクト間にトラフィックが描画される。

また、データフィールドにはエリアと呼ばれる各ネットワーク機器が属する地域を設定できる。例えば、営業拠点毎のエリア定義や建物のフロア毎のエリア定義などが可能である。可視化時には、設定されたエリア毎にトラフィックの色指定、表示／非表示の切り替えなどを可能とし、トラフィックの切り分けを容易にした。

Visioで作成した図面ファイルは、png形式の画像ファイルとxml形式の座標情報ファイルとして出力し、それぞれNIRVANAの可視化インタフェースに背景画像、オブジェクトの座標とIPアドレスレンジ(ネットワーク範囲)の対応情報として読み込む(図4)。これにより、トラフィックを可視化する背景画像が容易にカスタマイズやメンテナンス可能となり、様々なネットワークトポロジに合わせた可視化が可能となった。

図5～図7にNICTの情報システムチーム(現情報システム室)が、機構内トラフィックのモニタリングのために作成した背景画像を示す。図5は機構と世界の国々とのトラフィックを可視化する

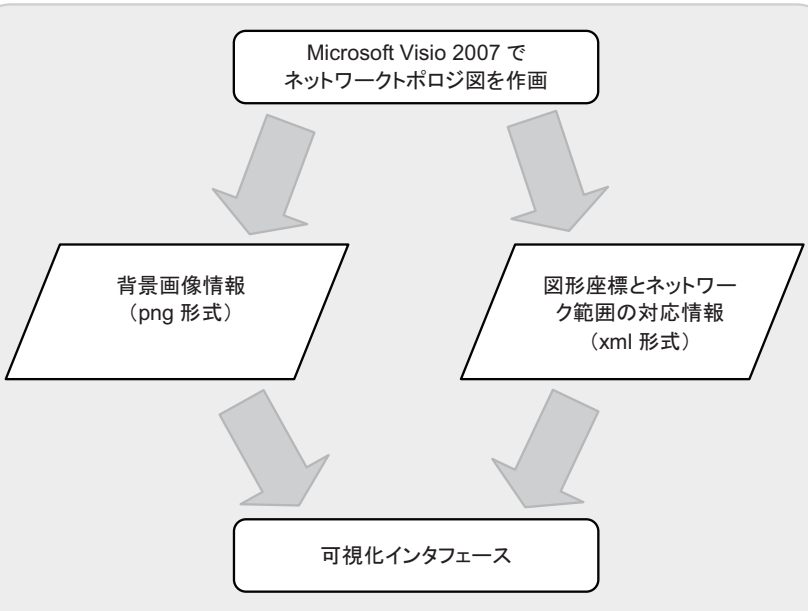

図4 ネットワーク図の設定フロー

図５ 機構と世界の国々とのトラフィックの可視化

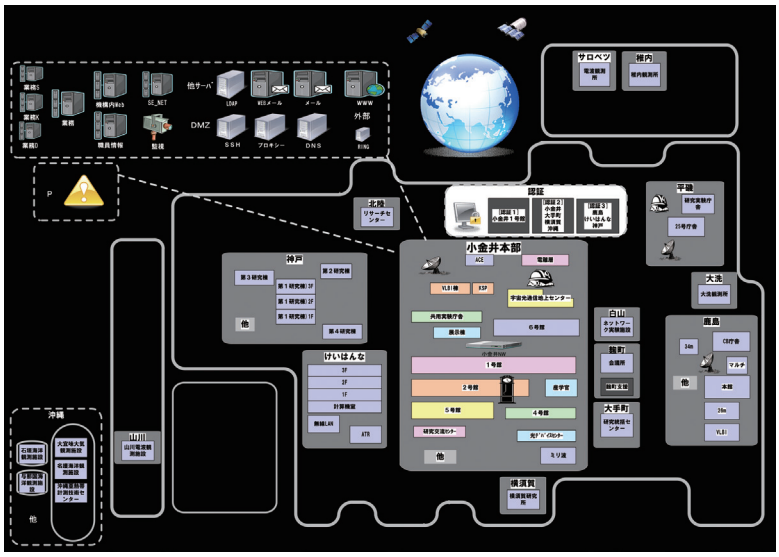

図６ 機構内拠点間トラフィックの可視化

ため、図６は機構内の拠点間のトラフィックを可視化するため、図７は機構に割り当てられているIPアドレスブロック間のトラフィックを可視化するための画像となっている。このように、同一のトラフィックデータを受信した場合でも、論理的な構成図や、物理的な配置図など、様々な視点からの可視化を可能とした。

4.3 トラフィック絞り込み機能

3.2 のシステム要件 (2) トラフィック絞り込み機能にて定義した機能要件を満たすための実装方法について述べる。NIRVANA ではトラフィック絞り込み機能を、パケットオブジェクト色切り替え機能とフィルタ機能を組み合わせて実現した。

4.3.1 パケットオブジェクト色切り替え機能

パケットオブジェクト色切り換え機能とは、トラフィックを描画する際のパケットオブジェクトの色を様々なパラメータによって切り替えることができる機能である。この機能により、トラフィックの強調描写を複数の視点から行うことができる。色と対応させることが可能なパラメータの種類を以下に示す。

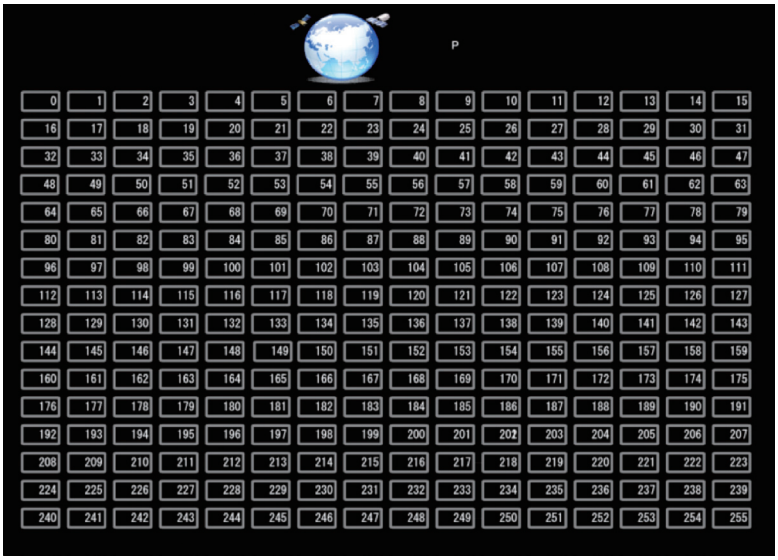

図7　機構内IPアドレス割り当てブロック間トラフィックの可視化

・プロトコル

プロトコルの種類毎にパケットオブジェクトの色を設定する。プロトコル／フラグの種類は、TCP/SYN、TCP/SYN-ACK、TCP/ACK、TCP/PUSH、TCP/RST、TCP/FIN、TCP/OTHER（上記以外）、UDP、ICMPとする。

・エリア

送信先エリア毎にパケットオブジェクトの色を設定する。エリアとは、**4.2**で述べた、背景画像の描画オブジェクトごとに定義できる地域情報である。

・センサID

センサID毎にパケットオブジェクトの色を設定する。センサIDとはセンサシステムに一意に割り当てられるIDである（すなわち、トラフィックの採取ポイントに相当する）。

・IPアドレス

送信元IPアドレスと送信先IPアドレスの組み合わせ（IPアドレスフィルタ）毎にパケットオブジェクトの色を設定する。IPアドレスフィルタはIPアドレスフィルタ機能（**4.3.2**）により作成する。

・ポート番号

送信元ポートと送信先ポートの組み合わせ（ポート番号フィルタ）毎にパケットオブジェクトの色を設定する。ポート番号フィルタは、ポート番号フィルタ機能（**4.3.2**）により作成する。

4.3.2　フィルタ機能

フィルタ項目毎に、フィルタ設定（パケットオブジェクト色の設定、描画ON/OFF設定、間引き設定）を行うことで、画面上に表示するトラフィックのフィルタリングを行うことを可能とした。以下ではまず、フィルタ項目の種類を示し、次に各フィルタ項目で共通的に用いられるフィルタ設定を示す。

フィルタ項目の種類を以下に述べる。フィルタ項目は以下の5種類とした。

・プロトコルフィルタ（図8）

プロトコルフィルタではプロトコル種別毎にフィルタ設定を行うことができる。プロトコル種別として実ネットワークにて主に使用されるTCPとそのフラグ、UDP、ICMPを採用した。表1にTCPフラグの種類と判定条件を示す。図8では、プロトコルフィルタにより、プロトコル種別毎に色分けを行い、トラフィックのプロトコル内容を表示している。

・IPアドレスフィルタ（図9）

IPアドレスフィルタでは送信元IPアドレスと送信先IPアドレスの組み合わせ毎にフィルタ設定を行う。送信元IPアドレスと送信先IPアドレスの組み合わせには、特定のIPアドレス、または全てのIPアドレスを意味する“ANY”が設定できる。図9では、IPアドレスフィルタにより、ある送信

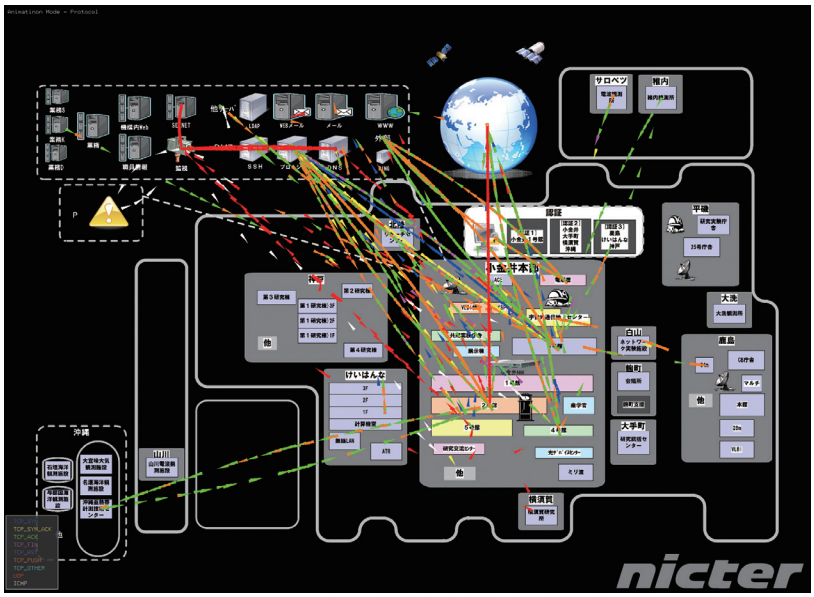

図８ プロトコルフィルタによるトラフィックの表示の例

表１ TCP フラグの種類と判定条件

プロトコルタイプ	判定条件
TCP_SYN	TCP の SYN フラグのみが ON
TCP_SYN_ACK	TCP の SYN フラグと ACK フラグのみが ON
TCP_ACK	TCP の ACK フラグのみが ON
TCP_FIN	TCP の FIN フラグが ON
TCP_RST	TCP の RST フラグが ON
TCP_PUSH	TCP の PSH フラグが ON
TCP_OTHER	TCP の上記以外

元 IP アドレスと送信先 IP アドレス間の通信のみを表示している。

・**ポート番号フィルタ**（図 10）

ポート番号フィルタでは送信元ポートと送信先ポートの組み合わせ毎にフィルタ設定を行う。送信元ポートと送信先ポートの組み合わせには、ポート番号、または全てのポート番号を意味する“ANY”が設定できる。図 10 では、80 番ポートに通信を行うトラフィックのみを表示している。

・**センサ ID フィルタ**（図 11）

センサ ID フィルタではセンサシステムに一意に割り当てられるセンサ ID 毎に、フィルタ設定を行う。図 11 では、センサ ID フィルタにより、特定のセンサ ID を持つセンサシステムにて採取されたトラフィックを強調表示している。

・**エリアフィルタ**（図 12）

送信先エリア毎にフィルタ設定を行う。図 12 では、エリアフィルタにより、エリアとして定義されたあるサーバへのアクセスのみを強調表示している。

各フィルタ項目で共通的に用いるフィルタ設定

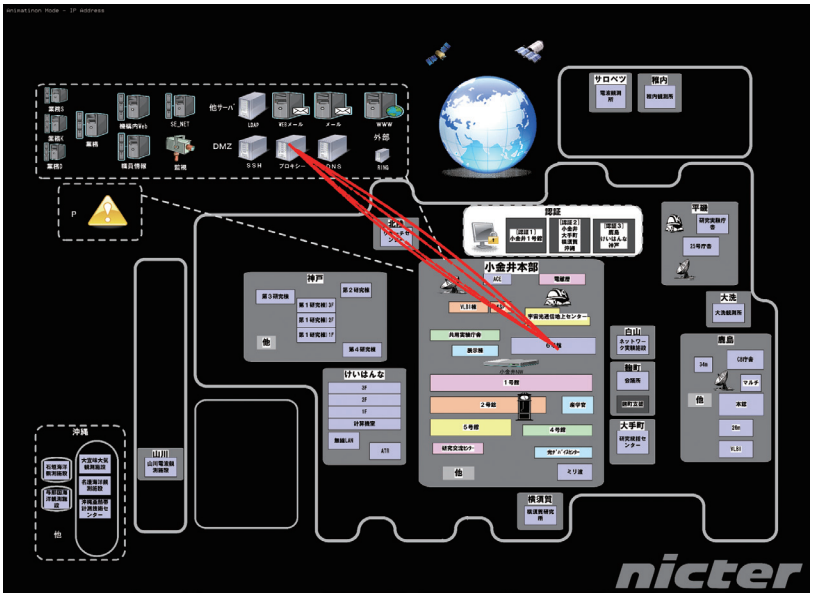

図9 IPアドレスフィルタによるトラフィック表示の例

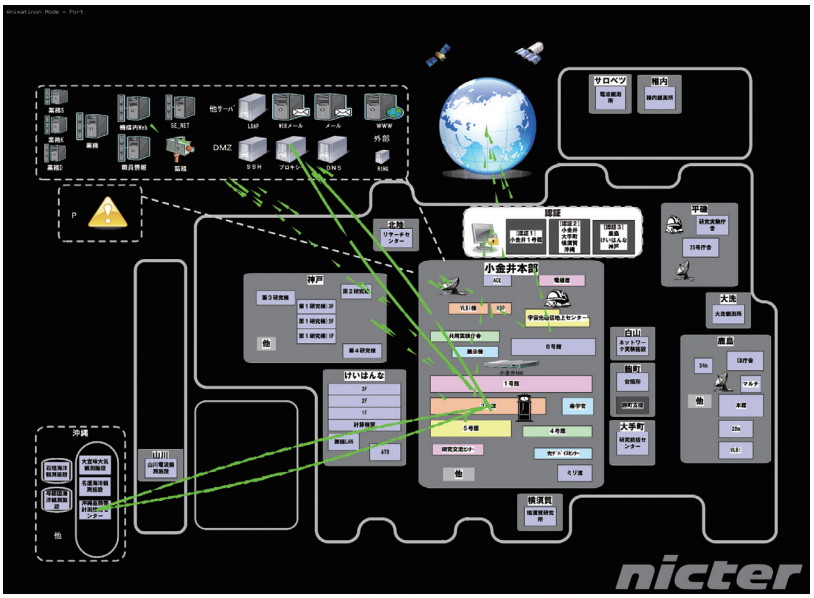

図10 ポート番号フィルタによるトラフィック表示の例

は以下の3種類とした。

・色設定

フィルタ項目毎に、パケットオブジェクトの色を設定し、特定のトラフィックの強調を行うための設定。

・描画ON/OFF設定

全体トラフィックの中から特定のトラフィック以外を非表示にすることにより、トラフィックを絞り込むための設定。

・間引き設定

全体のトラフィックの中から特定のトラフィック以外を間引き（サンプリング）することにより、特定のトラフィック以外を目立たなくするための設定である。

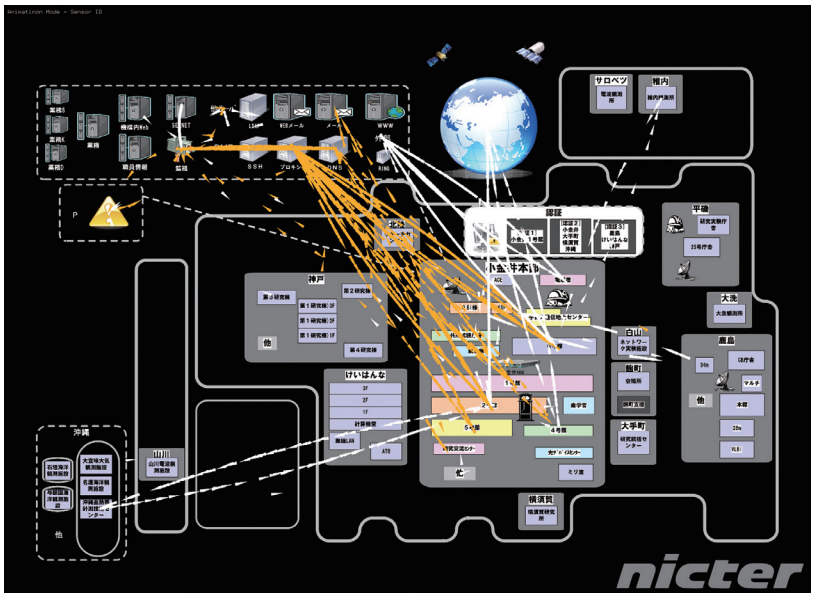

図 11　センサ ID フィルタによるトラフィック表示の例

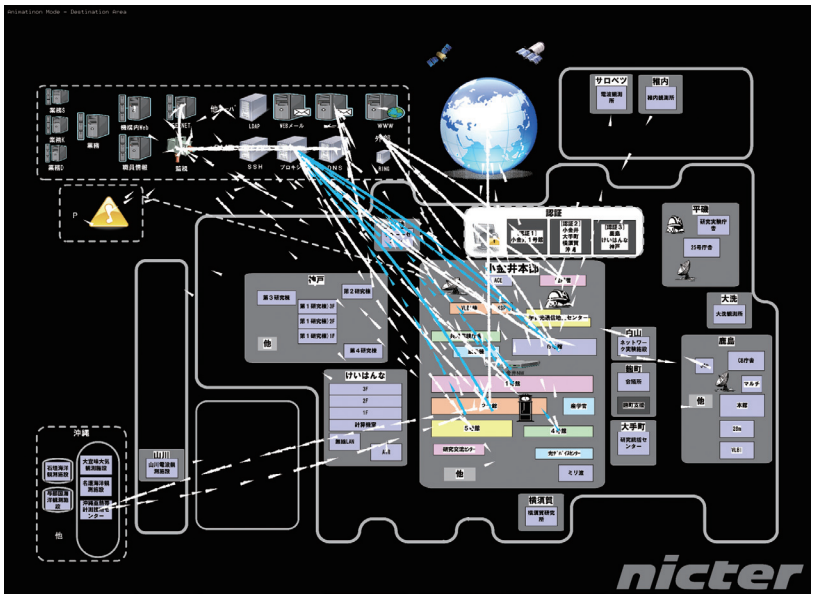

図 12　エリアフィルタによりトラフィック表示の例

4.4　パケットの詳細表示機能

3.2 のシステム要件 (3) パケットの詳細表示機能にて定義した機能要件を満たすための実装について述べる。

NIRVANA は、トラフィックを単に可視化するだけではなく、可視化された 3D オブジェクトに対して直接的な操作を実現している。これにより、従来のログベースのネットワーク管理に比べ、格段に迅速なドリルダウンが可能となった。図 13 は、パケットオブジェクトをマウスクリックし、その詳細情報のためのウィンドウが表示されている例である。ウィンドウの中には、パケットのタイムスタンプや送信元／送信先 IP アドレス、プロトコル、送信元／送信先ポート番号、送信元／送信

先エリア、センサIDが表示されている。

4.5　データ流量の可視化機能

3.2のシステム要件（4）データ流量の可視化機能にて定義した機能要件を満たすための実装について述べる。

データ流量の可視化機能は、**4.5.1**で述べるネットワークセグメント間のデータ流量と、**4.5.2**で述べるネットワークセグメントのデータ送受信量を可視化することによって実現した。

4.5.1　ネットワークセグメント間のデータ流量

ネットワークセグメント間のトラフィックのデータ流量を把握するため、ネットワークセグメントを表す図形間のデータ流量（パケット数、データ量）を弧線で表現する（図14）。データ流量を表す弧線は、送信元IPアドレスが登録されている図形から、送信先IPアドレスが登録されている図形へ描画され、色、高さ、太さ、透明度、グラデーションでデータ流量を表現する。弧線の頂点に円錐のオブジェクトを描画し、トラフィックの方向を示す。また、弧線の頂点にはデータ流量のカウント数を表示する。表示するカウント数の種類を表2に示す。

以下に弧線のデータ流量を表す項目について述

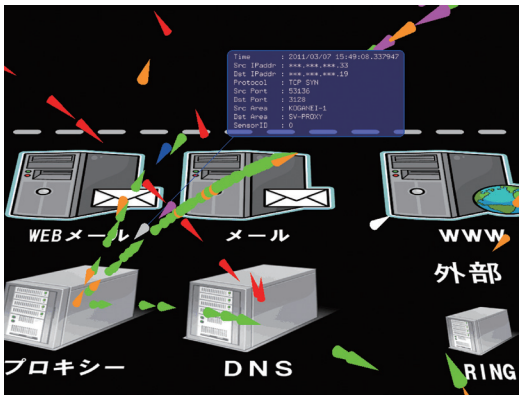

図13　パケットの詳細情報表示の例

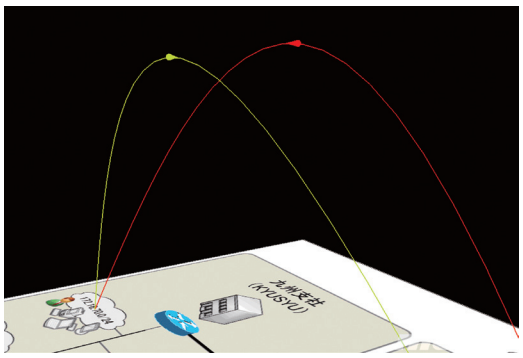

図14　データ流量の弧線

表2　データ流量カウント数の種類

フローカウンタモードの種類	意　味
パケット数カウント	ネットワークオブジェクト間のパケットカウント数の積算を表示する。
パケット数カウント割合	ネットワークオブジェクト間のパケットカウント数積算の全体に対しての割合をパーセンテージで表示する。 パーセンテージ表示は小数点以下2桁まで表示する。
データ量カウント	ネットワークオブジェクト間のデータ量の積算*を表示する。 表示単位はMbitで、小数点以下3桁まで表示する。
データ量カウント割合	ネットワークオブジェクト間のデータ量積算*の全体に対しての割合をパーセンテージで表示する。 パーセンテージ表示は小数点以下2桁まで表示する。

＊データ量は、パケットのIPヘッダ以降のデータ長を積算する。

べる。

・**弧線の色**（図 15）

弧線の色は、流量のカウント数をもとに決定され、最もカウント数が多い弧線が赤で表現される。その他の色は、その最大カウンタ数を基準に、相対的に色が決定される。最大カウンタ（赤）から相対的にカウンタが小さくなるにつれて、赤から紫へのグラデーションで表現する。

・**弧線の高さ**（図 16）

弧線の高さは、流量のカウント数をもとに決定され、カウント数が多いほど高く表現される。流量の多い箇所を把握しやすくするため、高さ比率の設定を可能としている。高さ比率の設定値が小さいほど、すべての描画線の高さの比は小さくなる。比率の設定値が大きいほど、カウンタ数が多い弧線とカウンタ数が少ない弧線の高さの比が大きくなり、カウンタ数が多い弧線がより際立つようになる。

・**弧線の太さ**（図 17）

弧線の太さは、流量のカウント数をもとに決定され、カウント数が多いほど太く表現される。流量の多い箇所を把握しやすくするため、太さ比率の設定を可能としている。太さ比率の設定値が小さいほど、すべての弧線の太さの比は小さくなる。比率の設定値が大きいほど、カウンタ数が多い弧線とカウンタ数が少ない弧線の太さの比が大きくなり、カウンタ数が多い弧線がより際立つようになる。

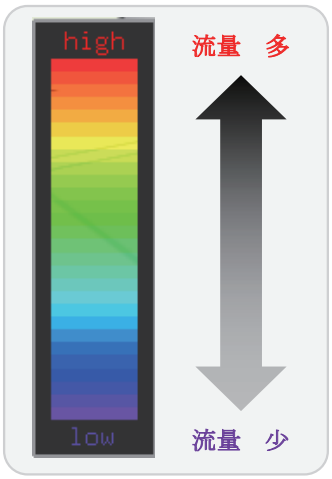

図 15　データ流量弧線の色

・**弧線の透明度**（図 18）

弧線の透明度は、流量のカウント数をもとに決定され、カウント数が多いほど濃く表現される。流量の多い箇所を把握しやすくするため、透明度比率の設定を可能としている。透明度比率の設定値が小さいほど、すべての弧線の透明度の比は小さくなる。比率の設定値が大きいほど、カウンタ数が少ない弧線がより透明に表示され、カウンタ数が多い弧線がより際立つようになる。

・**弧線のグラデーション**（図 19）

弧線のグラデーションは、現在の流量が多い弧線ほど、多くトラフィックが流れているように表

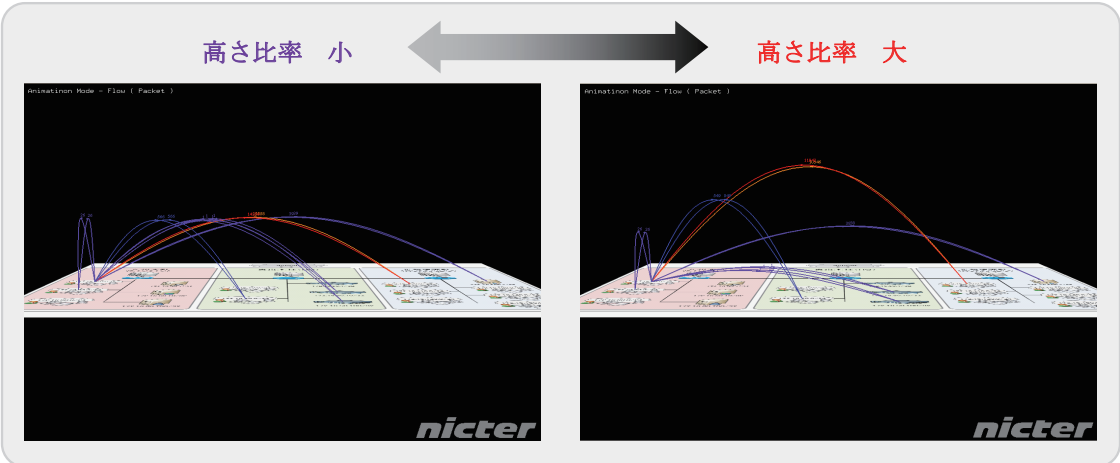

図 16　データ流量弧線の高さ

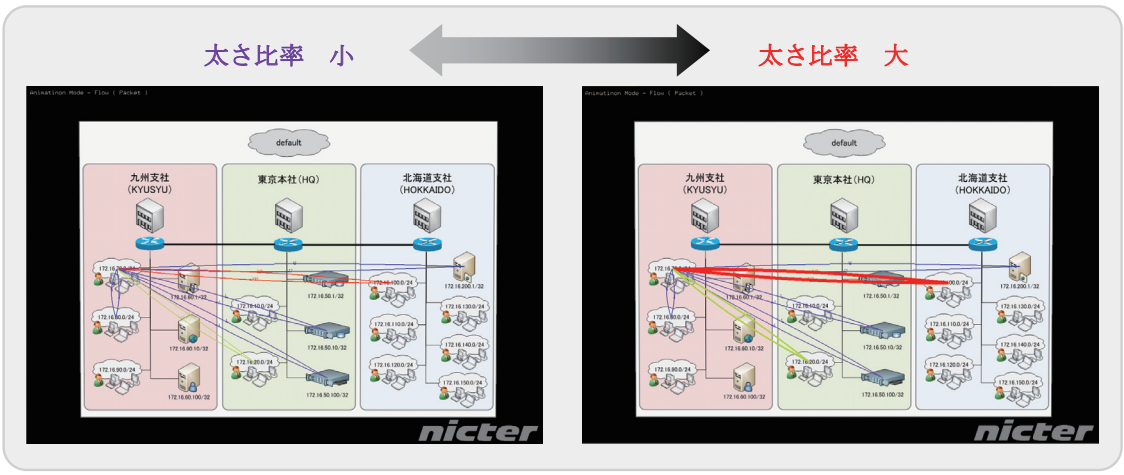

図 17　データ流量弧線の太さ

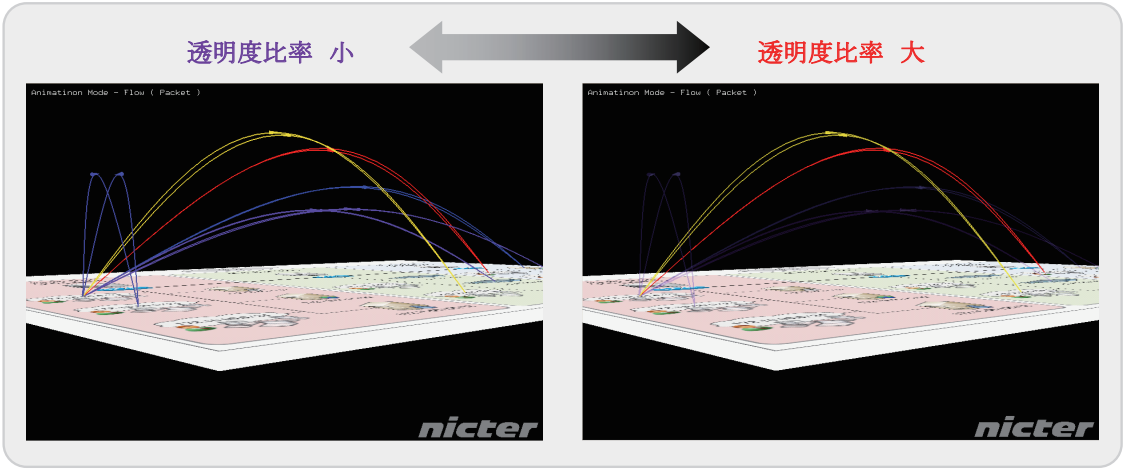

図 18　データ流量弧線の透明度

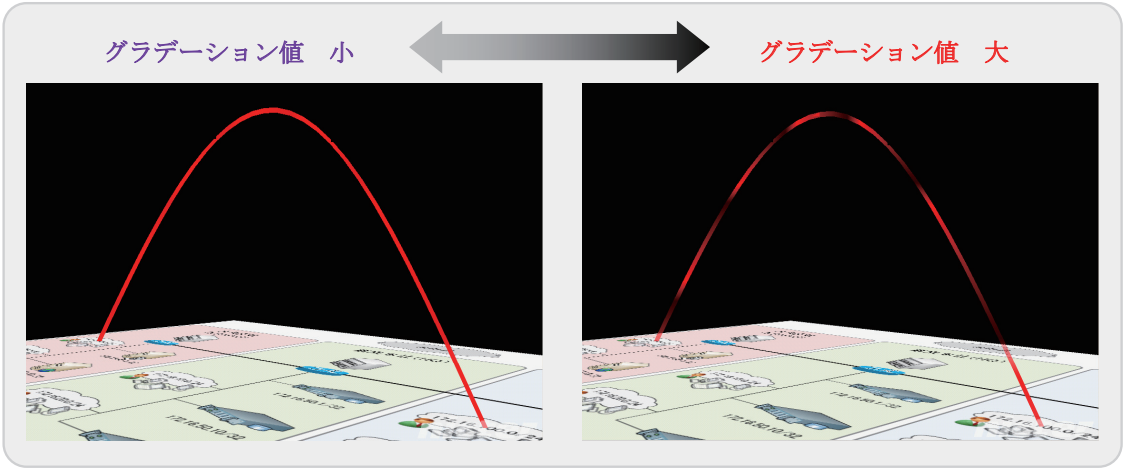

図 19　データ流量弧線のグラデーション

現する。トラフィックがカウントされていない弧線はグラデーション表示されない。

4.5.2 ネットワークセグメントのデータ送受信量

ネットワークセグメントを表す図形上に、該当IPアドレス範囲ネットワークのデータ送受信量（パケット数、データ量）を棒グラフで表現する。送信カウントは青の棒グラフ、受信カウントは赤の棒グラフで表現され、各棒グラフの頂点には、カウント数が表示される。表示されるカウント数は表2のとおりである。各棒グラフの高さは、最もカウント数が多い箇所が最も高く表現される。その他のグラフは最大カウント数の高さを基準に相対的に調整される。棒グラフの表示方法を図20に示す。

5 評価

5.1 性能評価

NIRVANAは実ネットワークトラフィックをキャプチャし可視化を行うシステムである。そのため、多量のトラフィックをリアルタイムで処理する必要がある。キャプチャしたトラフィックを全て可視化システムで処理可能かどうかを評価するため、当機構ネットワークにおける運用を通じて、NIRVANAの処理性能を評価した。

5.1.1 機構内ネットワーク運用時の本システム性能要件

当機構では、クラスB（16ビットネットマスク）のネットワークが運用されており、当機構のトラフィックを全て観測するためには、その構成から計13か所のトラフィックを観測する必要がある。各観測箇所の1秒間あたりのパケット数の瞬間最大値（pps）と1秒間あたりのデータ量の瞬間最大値（bps）を計測したところ、表3の結果となった。測定結果から、各システムの性能要件を以下のように定義し、表4に性能要件の数値をまとめた。

・センサシステムの性能要件

センサシステムの性能要件は、瞬間最大値が最も大きいポイント13の結果から、定常的に60,000pps、950Mbpsのトラフィック処理できることとする。

・ゲートシステムの性能要件

ゲートシステムの性能要件は、すべてのセンサシステムで観測したトラフィックを集約するため、全採取ポイントの瞬間最大流量の合計である170,184ppsのデータ流量を処理可能であることとする。この際、センサシステムとゲートシステム間の最大データ流量は、センサシステムとゲートシステム間のデータ長の平均が150byteであるこ

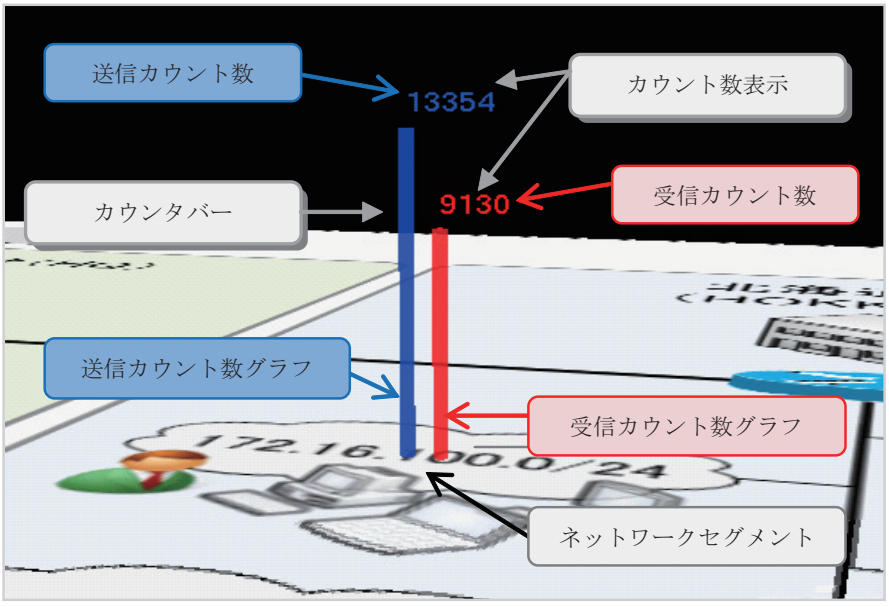

図20 ネットワークセグメントのデータ送受信量グラフ

とから、205Mbpsとなる。

・可視化システムの性能要件

可視化システムの性能要件は、ゲートシステムで集約した処理したデータを処理する必要があるため、ゲートシステムと同様、170,184ppsのデータ流量を処理可能であることとする。この際、ゲートシステムと可視化システム間の最大データ流量は、ゲートシステムと可視化システム間のデータ長の平均が120byteであることから、164Mbpsとなる。

5.1.2 評価環境

使用したOS、開発言語等の開発環境は以下のとおりである。

・センサシステム・ゲートシステム

- OS：FreeBSD 7.2[7]
- 使用言語：C/C++
- ライブラリ：libpcap-0.9系[8]（パケットキャプチャ）

・可視化システム

- OS：CentOS 5.4[9]
- 使用言語：C/C++
- ライブラリ：gtk-2.0[10]（GUI）、gtkglext-1.2系[11]、freeglut-2.4系[12]（グラフィック）

また、評価に使用したハードウェア環境を以下に示す。

・トラフィック生成装置

- Spirent TestCenter

・センサシステム・ゲートシステム

- Mode：DELL PowerEdge R210
- CPU：Intel Xeon X3450 2.66GHz
- Memory：2GB
- NIC：オンボードBroadcom NetXtreme Ⅱ BCM5716 1000Base-T

・可視化システム

- CPU：Intel Core2Quad Q9650 3.00GHz
- Memory：DDR2-667 8GB
- NIC：Intel 82573 10/100/1000Base-T
- Video Card：nVidia GeForce GTX285 1024MB

5.1.3 評価方法

センサシステムの評価は、トラフィック生成装置でパケットを生成し、可能な限りの高負荷でセンサシステムへ送信し実施した。試験時のパケット長は、64から1,500byteまでの各バイト長とIMIXパケットを使用した。IMIXとはインターネットミックス（Internet MIX）の略語であり、ネットワーク上で実行される典型的なトラフィックのタイプを表すトラフィックミックスを意味する。本評価では、64byteのパケットが約58.33％、570byteのパケットが約33.33％、そして、1,518byteのパケットが約8.33％で構成した。

ゲートシステムの評価は、トラフィック生成装置によりセンサシステム－ゲートシステム間のデー

表3 機構内各観測箇所の瞬間最大値

採取ポイント	pps	bps
ポイント1	26,378	427,534,624
ポイント2	99	1,604,592
ポイント3	4,642	75,237,536
ポイント4	79	1,280,432
ポイント5	4,117	1,280,432
ポイント6	50	810,400
ポイント7	3,407	55,220,656
ポイント8	312	5,056,896
ポイント9	42,712	692,276,096
ポイント10	139	2,252,912
ポイント11	24,945	404,308,560
ポイント12	4,705	76,258,640
ポイント13	58,599	949,772,592
合計	170,184	2,692,894,368

表4 各システムの性能要件

システム	パケット処理性能	データ処理性能
センサシステム	60,000pps	950Mbps
ゲートシステム	170,184pps	205Mbps
可視化システム	170,184pps	164Mbps

タを生成し、可能な限りの高負荷でゲートシステム送信することにより実施した。

可視化システムの評価は、トラフィック生成装置によりゲートシステム–可視化システム間のデータを生成し、可能な限りの高負荷で可視化システム送信することにより実施した。

5.1.4 評価結果と考察

試験結果を表5に示す。センサシステムは、いずれのパケット長の場合でも性能要件である60,000ppsを上回ったため要件を満たすことが確認された。しかし、今後これ以上トラフィック量が増える場合、Zero copy BPF[5]、ringmap[6]などのパケットキャプチャの高速化技術の導入や、センサを追加設置しセンサの負荷分散を考慮する必要がある。

一方、ゲートシステムの処理性能は、191,597ppsであり要件を満たしていることが確認できた。

可視化システムでは、パケット単位の可視化の場合、パケットオブジェクトの描画時間とパケットの処理性能が反比例関係にあることがわかる。これは、パケットオブジェクトの描画時間が長いほど、可視化画面上で同時に表示される3Dオブジェクトの数が増加するためである。NIRVANAでボトルネックとなる部分は可視化システムのビデオ性能である。そのため、可視化システムにはパケットオブジェクトを一定の割合で間引くサンプリング機能を実装し、受信パケット数がパケット処理性能を上回った場合にも、パケット数の比率は保ったまま表示することが可能となっている。一方、データ流量の可視化の場合、パケット処理性能を大幅に向上できることが分かった。

5.2 実運用による効果の評価

現在、NIRVANAは、当機構の情報システムチーム（現 情報システム室）にて運用され、機構内ネットワークの運用をサポートするために使用されている。現状のトラフィック把握やネットワーク機器入れ替えの際の動作確認、設定ミスによる不正トラフィックの発見に役立てられており、実際に管理者がPCの設定ミスによる不正トラフィックを発見し、PC使用者に対策を指示するといった事例など、NIRVANAが運用支援ツールとして有用であることが確認できた。

ただし、NIRVANAはトラフィック情報をリアルタイムに可視化することに特化したツールであり、情報はあくまで一過性のものである。そのため、前述のような不正トラフィック発生時に、管理者が簡易に過去情報にアクセスすることはできない。トラフィックの可遡性を実現するためには、nicterで実現しているようにトラフィック情報を蓄積するシステムと連携し、過去情報を再現する仕組みが必要となる。

表5 各システムの性能評価結果

システム	評価条件	パケット処理性能
センサシステム	64 byte	179,191pps
	570 byte	187,864pps
	1,518 byte	82,240pps
	IMIX	187,645pps
ゲートシステム	–	191,597pps
可視化システム	データ流量の可視化	180,000pps
	パケット単位の可視化 描画時間1秒	12,000pps
	パケット単位の可視化 描画時間3秒	4,000pps

6　まとめ

nicter 世界地図攻撃可視化システムをベースとした、実ネットワークトラフィック可視化システム NIRVANA について、その要件を整理し、実装した各種機能について概説するとともに、その評価を行った。

今後は、nicter プロジェクトの社会還元の一環として、NIRVANA の技術移転を積極的に進める予定である。NIRVANA をさらに実用的なシステムとするためには、実運用の中で様々なニーズや課題を洗い出し、機能改善を継続的に行う必要がある。

参考文献

1 Koji Nakao, Daisuke Inoue, Masashi Eto, and Katsunari Yoshioka,“Practical Correlation Analysis between Scan and Malware Profiles against Zero-Day Attacks based on Darknet Monitoring,” IEICE Trans. Information and Systems, Vol. E92-D, No. 5, pp. 787–798, 2009.

2 Daisuke Inoue, Masashi Eto, Katsunari Yoshioka, Shunsuke Baba, Kazuya Suzuki, Junji Nakazato, Kazuhiro Ohtaka, and Koji Nakao,“nicter: An Incident Analysis System toward Binding Network Monitoring with Malware Analysis,” WOMBAT Workshop on Information Security Threats Data Collection and Sharing（WISTDCS 2008）, pp. 58–66, Apr. 2008.

3 中尾康二，松本文子，井上大介，馬場俊輔，鈴木和也，衛藤将史，吉岡克成，力武健次，堀良彰，“インシデント分析センタ nicter の可視化技術”

4 鈴木和也，馬場俊輔，和田英彦，中尾康二，高倉弘喜，岡部寿男，“迅速な障害対応を支援するトラヒック可視化システムの構築と評価,” 信学論（B），Vol. J92-B No.10, Oct. 2009.

5 http://www.seccuris.com/documents/whitepapers/20070517-devsummit-zerocopybpf.pdf

6 http://code.google.com/p/ringmap/

7 http://freebsd.org

8 http://www.tcpdump.org

9 http://centos.org

10 http://www.gtk.org

11 http://gtkglext.sourceforge.net/

12 http://freeglut.sourceforge.net/

（平成 23 年 6 月 15 日 採録）

鈴木宏栄（すずき こうえい）
ネットワークセキュリティ研究所
サイバーセキュリティ研究室技術員
システムエンジニアリング、ネットワークエンジニアリング

衛藤将史（えとう まさし）
ネットワークセキュリティ研究所
サイバーセキュリティ研究室主任研究員　博士（工学）
ネットワークセキュリティ、マルウェア解析、ネットワーク運用

井上大介（いのうえ だいすけ）
ネットワークセキュリティ研究所
サイバーセキュリティ研究室室長
博士（工学）
ネットワークセキュリティ、情報セキュリティ