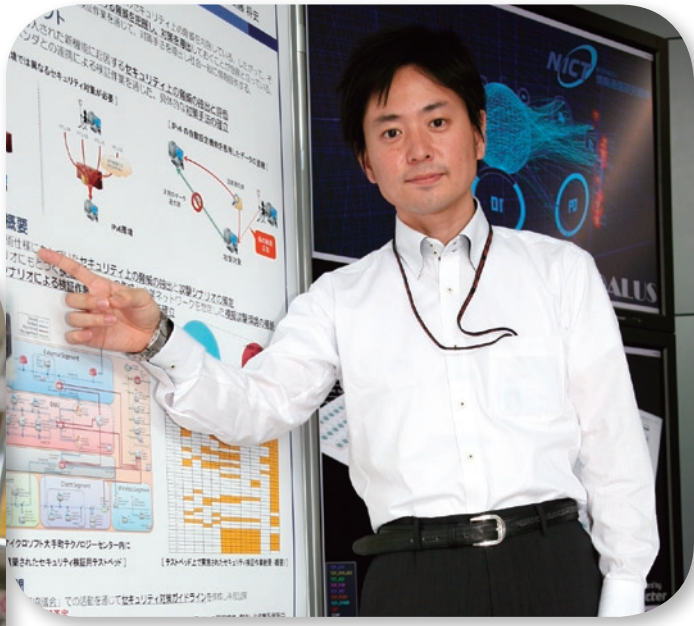
ネットワークリアルタイム可視化システムNIRVANA

ートラフィックの「今この瞬間」を描き出すネットワーク管理支援ツールー



「複雑化するネットワークを見える化し、ネットワーク管理を『苦しみのない世界』に。NIRVANA は nicter からスピンオフした強力なネットワーク管理支援ツールです。」

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

2003 年横浜国立大学大学院工学研究科博士課程後期修了後、独立行政法人通信総合研究所（現 NICT）に入所。2006 年より nicter の研究開発に従事。現在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 室長と、ネットワーク研究本部 ネットワークシステム総合研究室 研究マネージャーを兼務。博士（工学）。サッカーアルゼンチン代表と S.S. ラツィオがエネルギー源。

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

2005 年、NICT 入所。以来、nicter プロジェクトや IPv6 セキュリティなど、情報通信セキュリティ技術の研究開発に従事。nicter プロジェクトでは主に次世代型サイバー攻撃観測プラットフォームの研究に取り組む。博士（工学）。

はじめに

ネットワークが生活空間の隅々にまで張り巡らされ、地球上のどこかに蓄積された膨大なデータにハンドヘルドデバイスやタブレットコンピュータからアクセスし、海外にいる同僚とリアルタイムにビデオ会議をする…。私たち 21 世紀初頭の人類を取り巻く通信環境は、スタートレックの生みの親、ジーン・ロッデンベリー氏の豊かな空想をも上回るスピードで進化を続けているようです(もちろん亜空間通信はまだ実現していませんが)。しかしながら、その通信環境を支えるネットワークの管理は、エンタープライズ号の艦内のようにコンピュータ任せとはいかず、現代のネットワーク管理者達を悩ませ続けています。

そこで、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では、通信環境の進化とともに複雑化するネットワーク管理の負荷を軽減するために、ネットワークリアルタイム可視化システム NIRVANA*1 の開発を行っています。NIRVANA は、ネットワークを流れるトラフィックをリアルタイムに可視化することで、ネットワークの疎通確認や障害検知、輻輳の把握や設定ミスの検出などを迅速に行うことを可能にし、組織のネットワーク管理の効率を劇的に向上させる支援ツールです。そして、その可視化の仕組みは、同研究室で研究開発を進めているインシデント分析センター nicter で培ってきた技術群を応用したものです。

ダークネットからライブネットへ

インシデント分析センター nicter は、サイバー攻撃の発生を早急に把握するために、インターネット上に複数のセンサを設置し、未使用の IP アドレス(以下、ダークネット)の大規模観測を行っています。ダークネットにはマルウェアが次の感染対象を探すためのスキャンなど、不正なトラフィック(以下、ダークネットトラフィック)が大量に届きます。nicter では、ダークネットトラフィックを自動分析すると同時にリアルタイムに可視化し、迅速なセキュリティオペレーションを実現するための研究開発を行っています。

この nicter のダークネットトラフィック向けに開発した可視化技術を、ライブネットトラフィック(ユーザ端末やサーバ等が接続された実ネットワークを流れる通信)に応用し、強力なネットワーク管理支援ツールとしてスピンオフしたシステムが NIRVANA なのです。

NIRVANA のシステム構成

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視覚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ります(図 1)。これは、nicter のダークネット観測システムから継承したシステム構成です。

センサシステムには、観測対象ネットワークからポートミラーリングやネットワークタップによって複製・分岐されたライブネットトラフィックを入力します。また、sFlow*2 によってサンプリングされた情報を入力することもでき、組織のネットワーク環境に応じた柔軟な観測方法を選択可能です。センサシステムは観測対象ネットワークに複数設置できるため、例えば、組織のネットワークが日本各地に分散しているような場合にも対応できます。

ゲートシステムは、センサシステムにおいてパケットサマリデータ*3 に変換されたライブネットトラ

*1 nicter real-network visual analyzer
*2 高速・大容量化したネットワーク管理の効率化を可能にする、ネットワークスイッチ等における情報収集技術のインターネット標準(RFC 3176)。
*3 パケットをネットワーク層とトランスポート層のヘッダ情報と、アプリケーション層のハッシュ値に圧縮したデータ。ライブネットトラフィックに比べ、大幅なデータ量の削減が可能。

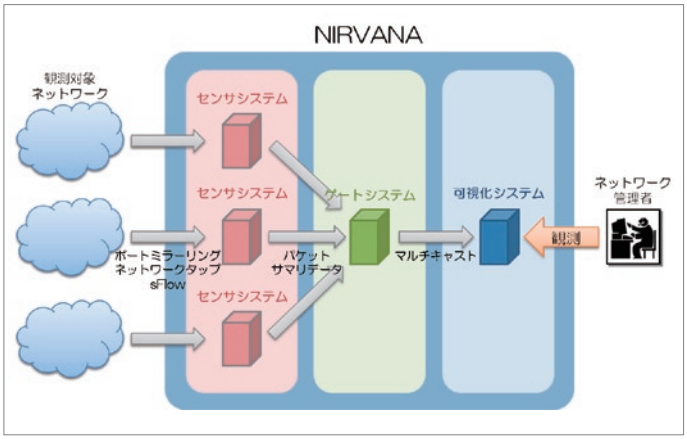


図1　NIRVANAのシステム構成

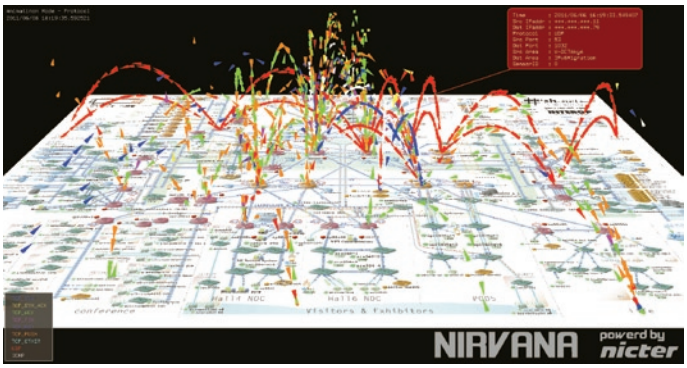


図2　NIRVANAによるライブネットトラフィックの可視化（パケットモード）*4

NIRVANAによるライブネットの可視化

NIRVANAの可視化システムは、リアルタイム性、インタラクティブ性、カスタマイズ性を重視して設計・開発されています。リアルタイムに可視化されたライブネットトラフィックは、ネットワーク管理者の操作によってインタラクティブに拡大縮小や視点切替え、一時停止、詳細情報の表示などが行えます。また、3Dオブジェクトの形状や色、軌道の高度、スピードなど多岐に渡るパラメータをカスタマイズ可能です。さらに、フィルタリング機能も充実しており、送信元 / 宛先IPアドレスやプロトコル、ポート番号、センサシステムのIDなどによってトラフィックのフィルタリングが可能です。

NIRVANAにはパケットモードとフローモードという2つのモードがあります。パケットモードは、ライブネットトラフィックをパケット単位で可視化するモードであり、ネットワークの疎通確認や、経路の障害検知などに威力を発揮します。図2は、Interop Tokyo*6 2011の展示会場ネットワーク「ShowNet*7」にNIRVANAを導入し、パケットモードでトラフィックを可視化したものです。各パケット(ロケット)の色はパケットの種別*8を表し、パケットの軌道の高さはポート番号の大きさに比例(対数軸)しています。また、図右上の赤色のウインドウには、選択されたパケットの詳細情報が表示されています。パケットはルータをホップするように流れていきますが、これにはOSPF*9によって

フィックを集約し、可視化システムに向けてマルチキャストします。組織のネットワーク規模に応じて、ゲートシステムを複数設置することも可能です。

可視化システムは、ゲートシステムからマルチキャストされたパケットサマリデータを受信し、リアルタイムに3Dアニメーション表示します。可視化に必要な情報はマルチキャストされていますので、ネットワーク管理者が複数いるような場合でも、可視化システムのハードウェアを追加してマルチキャストを受信すれば、多地点でのモニタリングが可能になります。可視化システムは単体動作させることも可能であり、ローカルに保存したPCAPファイル*5を再生して可視化することができます。

*4 Copyright (c) Interop Tokyo 2011 NOC Team Member and NANO OPT Media, Inc. All rights reserved.
*5 ネットワーク上を流れるパケット情報を保存するためのファイル形式。多くのネットワーク管理ツール(tcpdump、Wireshark 等)で利用されています。
*6 例年、数百の出展社が最新のネットワーク機器やソリューションを展示し、同時に多数の講演やコンファレンス等が開催される、ネットワーク分野における世界最大規模のイベント。
*7 国内外のネットワークベンダが世界最先端のネットワーク機器を結集して構築する、Interopの心臓部とも言える展示会場全体のネットワーク。

定期的に取得したルーティングテーブルを利用しており、パケットの送信元 / 宛先 IP アドレスの組からその経路を決定しています。そのため、観測中に経路の変更が起こった場合でも動的に追従可能です。

一方、フローモードはトラフィックの流量を直感的に把握するためのモードです。フローモードではネットワーク機器間のトラフィック量を表現するためにリボン状の曲線を用い、その高さや太さ、色によって相対的な流量を表しています。図 3 は「ShowNet」をフローモードで可視化したものです。図中央の基幹ルータ間のホップが赤いリボンで表現されており、この機器間を流れるトラフィック量がネットワーク中で最大であることが把握できます。また、各機器の上に表示されている青と赤のバーは、それぞれ送・受信パケット数(設定によってはデータ量)を表しています。フローモードを用いることで、ネットワークのボトルネックを迅速に把握することが可能になり、前述のパケットモードとの併用で、ネットワーク管理の負荷を劇的に軽減できます。

NIRVANA の中で描かれるネットワーク図は、汎用の作画ツール Microsoft Visio*11 によって作成できます。NIRVANA はネットワーク図中の各オブジェクト(ネットワーク機器)に設定された IP アドレスを読み込んで、図中の座標に IP アドレスを自動設定することができます。そのため、ネットワークの構成変更が頻繁に起こるような組織でも、容易に NIRVANA のネットワーク図をアップデートすることができます。また、ネットワーク管理者のアイデア次第で、様々なネットワーク図を用いることができます。

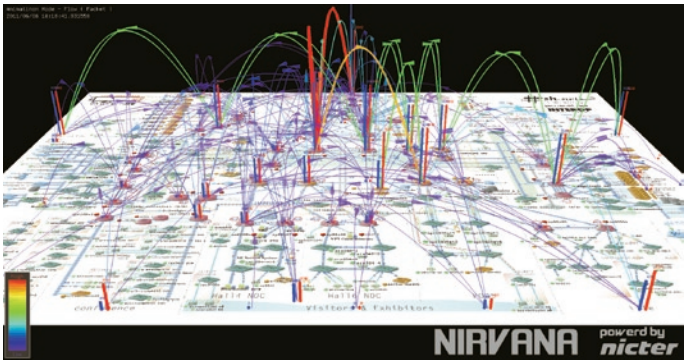


図3　NIRVANAによるライブネットトラフィックの可視化 (フローモード) *10

まとめ

仮想化技術の発達やクラウドコンピューティングの普及などにより、ますます複雑化するネットワーク管理が「苦しみのない世界」となることを目指し、インシデント分析センター nicter の研究成果からスピンオフした NIRVANA の社会展開と、さらなる高度化を進めていきます。

*8　図 2 の例では、青 : TCP SYN、黄 : TCP SYN-ACK、緑 : TCP ACK、桃色 : TCP FIN、紫 : TCP RST、橙 : TCP PUSH、水色 : TCP OTHER、赤 : UDP、白 : ICMP。
*9　Open Shortest Path First。ダイクストラ法によって最短経路のルーティングテーブルを作成するルーティングプロトコル。
*10　Copyright (c) Interop Tokyo 2011 NOC Team Member and NANO OPT Media, Inc. All rights reserved.
*11　Microsoft 及び Visio は、米国 Microsoft Corporation の米国及びその他の国における登録商標又は商標です。