広域モニタリング環境における ネットワーク異常検知

中村　信之

インターネットはすでに重要な社会インフラとして定着しており，インターネットを構成するネットワークが正常に機能するのが当然だと信じられている。しかし現在のインターネットは非常に脆く，ワームなど悪意のあるプログラムの活動によって大きな被害を受けてきた。本稿では，ネットワークに対するサービス妨害（以下DoS：Denial of Services）を引き起こす原因としてワームとDDoS（Distributed DoS）を例に挙げ，これらのプログラムの引き起こす異常なトラフィックを検知する手法について述べる。

インターネットの発展と脅威

インターネットを流れるトラフィックが少なかった頃は，ネットワーク管理者が全てのログをチェックすることにより異常の有無を確認することも可能であった。しかし，近年，インターネットの飛躍的な普及に伴い，ネットワークを流れるトラフィックが急激に増大したため，ネットワーク管理者は管理しているネットワークの状態を把握するのが困難になってきている。そこで，ネットワーク管理者が管理ネットワークの異常のみを把握するために，不正侵入検知システム（以下IDS：Intrusion Detection System）を利用することもあった。IDSは既に世の中で知られており異常パターンが登録されている“既知の異常”を検知できるが，未知ワームが発生させたトラフィックに気づかない可能性が高く，このような異常パターンの定義が未だされていない“未知の異常”に対しては有効なツールとは言えなかった。

一方で，IDSとは異なるアプローチで，異常かどうかではなく流れているトラフィックの状態を統計的に把握する定点観測が近年になって頻繁に行われるようになった。定点観測では，ネットワーク上の同じ場所で長期にわたってトラフィックを観測することで，管理するネットワークの状態を客観的に知ることができる。平常時のトラフィックを把握できるために，異常である状態に気づきやすいという特徴がある。定点観測で得られるデータのいくつかは公開されておりJPCERT/CC[1)] や@Police[2)] が有名である。また，公開されているデータと個別に取得したデータとを比較することによって周辺ネットワークとの関係を把握するような使い方も検討されている。

こうした異常検知技術の変化の背景には，ウイルス・ワームなどの攻撃手法の進化や目的の変化がある。2001年に登場したMS Blastはその被害の大きさから非常に有名なワームとして知られている。それまでのワームとMS Blastの一番大きな違いは，今までServer PCのみをターゲットにしていたワームが，ユーザの使っているClient PCをターゲットにしたところであり，ワームに感染したPCが特定のサーバーに対してDoS攻撃を仕掛けるようにプログラムされていたことにある。**図1**にDDoSの動作イメージ図を示す。この図は，ワームに感染したPCの台数が多いほど大規模なDDoS攻撃となることを示している。

その後，SQL SlammerやCode Redなどの新しいワームが出現し，そのたびに大きな被害を引き起こしてきた。ここで，ワームの引き起こす被害を整理すると，次の2つに分類できる。1つはワームが拡散する過程でのネットワークに対する過剰な負荷をかけることで引き起こされるDoSであり，もう1つはワームに感染した複数PCが踏み台として利用された結果引き起こされる被害である。

前者はMS Blastの感染（拡散）過程において，ICMP

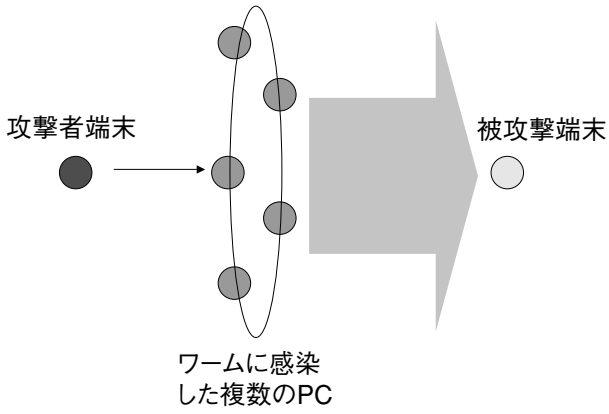

図1　DDoSの動作イメージ

メッセージが大量に発生し，ルータがダウンするなどの被害をもたらした。後者の場合，特定のサーバーに対して攻撃を仕掛けることによるDDoSや，スパムの中継など用途も被害の大きさも多種多様である。

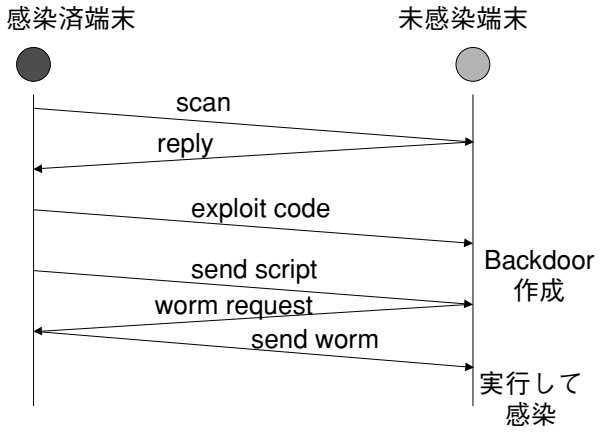

図2　ワームの感染シーケンス（例）

また未知ワームは，既存のパターンマッチングによる検知技術では検出できないため，既知ワームにくらべその検出はさらに難しい。**図2**にワームの感染シーケンスを示す。ワームの拡散過程では正常なServer-Client通信と変わるところがなく，通信を監視してその拡散を検知するのは難しい。一方，感染済み端末が踏み台に使われた場合，その動作は**図1**に示すDDoSの動作のようになる。攻撃元からの命令（トリガー）によって複数のワーム感染端末が特定のサーバーに対してDoSを行うことになる。この攻撃は即時性が高く，周辺ネットワークへの影響も非常に大きい。サービスが停止し利用できなくなっていることでDDoSが原因だったと判明することもあり，未然に防ぐのはかなり難しいとされている。

以上のことから，未知のワームの拡散を検知する方式や，ワームに感染したPCの引き起こすDDoSを早期に検知する方式が切に求められている。

技　術　動　向

ワームやDDoSなどの脅威から守るべき資産は，背景でも触れたように，サーバーや社内LANとバックボーンネットワークの2つに大きく分類でき，それら資産を守るためにそれぞれ異なる技術が適用される。

前者はたとえば企業・大学・自治体などがインターネット上に公開しているサーバーやインターネットと接続されている社内LANなどであり，インターネットのエッジに相当する部分である。具体的な装置としては，ホストコンピュータ，サーバー，ファイアウォールなどが挙げられる。 この分野は従来からハッキング・クラッキング・不正侵入という言葉で知られている課題を持ち，広義のハッカーとその対抗技術とのいたちごっこにより技術レベルが向上してきた側面がある。たとえば。ファイアウォールでは検知できない異常な通信を，パケットに含まれるデータを解析することで検知するIDSや，異常な通信を検知するだけでなく自動的に防衛もするようにIDSを拡張したIPS（Intrusion Detection and Prevention System）などがある。その他にも，攻撃者を騙すためのハニーポットや，社内LANに持ち込まれるPCの安全性を確保するための検疫システムなども登場してきている。

一方，後者はたとえばISP網やIX（Internet Exchange）のようなコアネットワークであり，インターネットのバックボーンに相当する部分である。具体的な装置としては，ルータやスイッチなどのネットワーク機器が挙げられる。この分野におけるワームやDDoSの脅威は最近になるまで話題になっておらず，MS Blastが猛威を振るった2001年頃から立ち上がってきた研究分野である。この分野には，技術的な課題以外に，ISP同士の連携を前提としないと有効なシステムにならないという社会的な課題もあり，そのために遅々として防衛技術の開発が進まなかった印象を受ける。現在ではtelecom-ISAC Japanが発足するなど状況は変わりつつあるが，未だ技術的に成熟したものは少ない。

現在のところ最も多く試行されているのが定点観測である。**図3**に定点観測の全体像を示す。定点観測ではインターネット上のさまざまな場所に置かれたファイアウォールやIDSのログおよびネットワーク機器のMIB（Management Information Base）情報などのデータをどのように可視化してネットワーク管理者が異常を判断しやすいように表示するかが課題である。また，ワームやDDoSが異常なトラフィックを発生させた際，どのよう

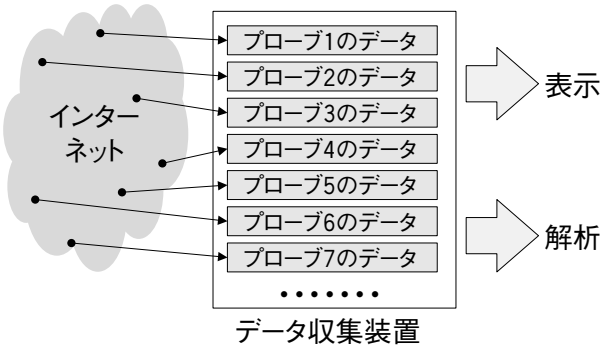

図3　定点観測

に自動検知するかといった検討もなされている。ここで，表示や解析をする際に最も問題になるのが，**図3**の真ん中に位置している複数プローブのデータの扱いである。従来は単体のプローブあるいは同じ環境下にある数台のプローブのみを考えればよかったが，全く別の環境に置かれた複数のプローブを考慮する必要がでてきた。

本稿で検討する広域モニタリングシステムとは定点観測の一形態で，観測対象がインターネット全体であることから，後者の技術と分類できる。次章以降では広域モニタリングを可能とするためのマルチプローブシステムに焦点を当てて検討する。

マルチプローブシステムを考慮したシングルプローブの機能

前章で述べたように，ワームやDDoSを検知するシステムには，1つのプローブで動作して検知するシングルプローブシステムと，複数が分散して動作し各々のデータを合わせて検知するマルチプローブシステムの2種類がある。

シングルプローブシステムでは設置場所のデータしか取得できず，取得したデータから広範囲なインターネットの状態を推定するのには無理がある。そこで，広域モニタリング環境では複数のプローブを用いてより正確に観測ネットワークの状態を取得し，異常を検知するための検討が必要になる。

マルチプローブシステムとは，基本的にはシングルプローブを複数設置したシステムである。しかし，シングルプローブでは設置場所に特化した情報しか取得できないため，そのままでマルチプローブシステムとして動作させることはできない。ここでは，マルチプローブシステムへの拡張における課題と検討の方向性に関して説明する。

マルチプローブシステムへ拡張する際の課題として以下の3点が挙げられる。

① ネットワークトポロジーの違い
② 下位ネットワークのサービスの違い
③ トラフィックの大きさの違い

これらの課題は，プローブの設置場所や設置台数の問題とも関連する課題であるが，①～③はプローブ設置後にも変化することが多いため解決は容易ではない。**図4**に想定するネットワークトポロジーを示す。インターネットでは，コアネットワークと呼ばれる側にISPがあり，大容量のトラフィックが流れている。一方，エッジ側では一般家庭からのADSLやFTTH接続などのような比較的容量の少ないトラフィックが流れている。

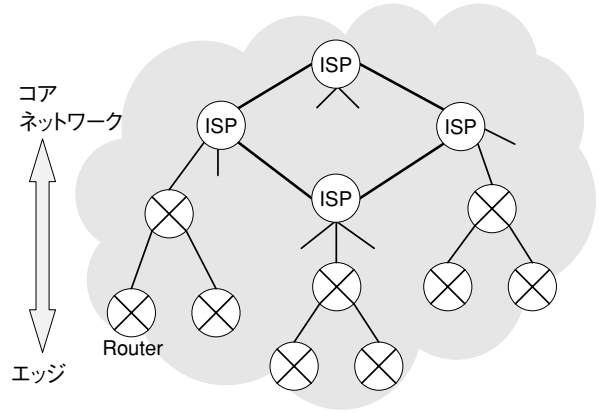

図4　ネットワークトポロジー

また，**表1**に設置場所の違いによるプローブの特徴を示す。異常発生時には急激に異常トラフィックが増加するためエッジでは影響が大きく検知も容易であるが，コアネットワークに近づくほど異常の影響が少なくなり検知しにくくなる。そのため，エッジに近いほどトラフィックの変化に伴う誤検知が多くなり，コアネットワークに近くなると誤検知は少なくなる。このようにプローブの設置場所や設置台数の違いによって生じる影響の差をできるだけ吸収し，複数のプローブにより効果的にワームやDDoSを検知する手法が求められる。

表1　設置場所の違いによるプローブの特徴

設置場所	異常発生時（初期）の影響の大きさ	異常の検知のしやすさ	異常を誤って検知してしまうことの多さ
コアネットワーク（ISP側）	少さい	検知しにくい	誤検知が少ない
⇕	⇕	⇕	⇕
エッジ（ユーザ側）	大きい	検知しやすい	誤検知が多い

まず，①のネットワークトポロジーの違いは，たとえば，ISPのコアルータ，企業内LANとインターネットを結ぶルータ，FTTHやADSLで接続しているブロードバンドルータを比べた場合の接続されているネットワーク機器の台数やトラフィックの流れ方の違いである。この違いを最も簡単に表すことのできる要素としてIPアドレスがある。エッジでは，送信元あるいは送信先アドレスのい

ずれかは常に同じアドレス空間であるが，インターネットのコアネットワークに近づくにつれて，送信元と送信先アドレスに特徴が見られなくなる。なぜならば，エッジでは内部ネットワークから外部ネットワークへの通信と外部ネットワークから利用者ネットワークへの通信以外は通過せず，コアネットワークでは不特定の場所からのパケットを不特定の場所に中継しているためである。

以上より，トラフィックに含まれる要素のうち，ネットワーク規模・トポロジー情報に依存する要素はそのままではマルチプローブで利用できないことがわかる。

しかし，IPアドレスは，偽装されている可能性はあるが，送信元や送信先の国が特定できるなど，非常に有益な情報である。異常検知後の原因の解析には重要な役割を果たす可能性があるため，国ごとに分けてカウントするなど，うまくデータ収集する仕組みが必要である。

次に，②の下位ネットワークのサービスの違いとは，たとえば，下位ネットワークにWebサーバーやDNSを提供するサーバーがある場合と何もサービスを持たない場合の違いである。具体的には，下位ネットワークにWebサーバーを持つプローブではhttp（80/tcp）に対する通信があり，下位ネットワークにWebサーバーを持たないプローブではhttp（80/tcp）に対する通信が少ないか，あるいはファイアウォールなどでフィルタされているために全く無い。同様に，DNSを提供するサーバーがある場合はDNS（53/udp）の通信があり，場合によってはDNS（53/tcp）の通信も発生するが，DNSを提供するサーバーを持たない場合は，DNS（53/udp）やDNS（53/tcp）の通信が少ないかあるいは全くない無い。

このように，下位ネットワークのサービスの有無や提供されるサービスの違いによって，トラフィック中に含まれるTCPやUDPなどのトランスポート層プロトコルや，Port番号などの要素が違ったものになる。トランスポート層プロトコルとポート番号はネットワーク上で利用されているアプリケーションを判断する上で有効な指標となる。さらに，ワームの感染プロセスは脆弱性の見つかった特定のアプリケーションに依存し，またDDoSの攻撃プロセスも特定のアプリケーションを利用するものであるため，ポート番号という要素を用いてプローブ間のデータを比較する手法が有効であると考えられる。しかし一方で，新しいアプリケーションやプロトコルは今後とも開発され，数が増加していくことが予想される。たとえばIPv6やMobile IPは比較的新しいプロトコルであるし，無線環境での利用に適したTCPも盛んに研究されている。アプリケーションに関しては従来のServer-Client型のアプリケーションだけでも非常に多く，最近ではPeer to Peer型のアプリケーションも多数開発されている。このように，OSIの上位階層を扱うほどトラフィックデータが複雑なものとなり処理にかかる負荷も大きくなるため，できるだけ下位層の情報を利用して異常を検知できることが望ましい。広域モニタリング環境でのリアルタイムなワーム検知を考える際には，検知のフェーズでは下位層のデータを用い，解析のフェーズで上位層のデータを用いるのが良いと考えられる。

最後に，③のトラフィックボリュームの違いを説明する。これは，たとえば数kbit/sで流れているトラフィックと数Gbit/sで流れているトラフィックとの違いである。

たとえば，同じワームが感染活動を始め，時間とともに通信の内容が変化することを比較する場合，数kbit/sで流れているトラフィックは急激に大きなトラフィックに変化するが，数Gbit/sで流れているトラフィックにおいては変化が認識できるまでに相当な時間がかかる可能性がある。

この課題に対しては，パケットのさまざまなサンプリング手法を適用することで解決できると考えられる。IETF（Internet Engineering Task Force）のpsamp（Packet Sampling）ワーキンググループ[3]において，標準的なサンプリング手法を定義しており，取得したいデータによってサンプリング手法を選択することになる。また，パケットの数値的なサンプリング手法だけではなく，サンプリングには意味情報のサンプリング手法も存在する。たとえば，IDSやファイアウォール，MIBなどの発するアラートやイベントなどであり，これらはトラフィック中の特定のパケットやフローのみを抽出するためのサンプリング手法である。 複数あるサンプリング方式のうち，どのサンプリング手法を選択するのが良いかを評価していくことが必要である。

提案するネットワーク異常検知方式の概要

ここまで，プローブを複数設置してマルチプローブシステムとして動作させる際に考慮しなければならない点を述べてきたが，最後に現在取り組んでいるネットワーク異常検知エンジンの概要を説明する。この検知エンジンは前章で挙げた課題を解決するための以下のような特徴を持つ。

各プローブを流れるトラフィックの特徴を定義し，定義されたトラフィックをもとに異常トラフィックを検知する。これにより，各プローブで異常検知した結果をプローブ間で単純に比較できるようになり，異常が発生したのか，異常が広範囲に広がりつつあるのか，あるいは異常が広範囲に広がった状態であるのかを検知すること

ができる。

まず，前章③に挙げた“ トラフィックの大きさの違い”に着目してトラフィックの特徴の定義をする。プローブ同士を比較するためにトラフィックの大きさとトラフィックに含まれる要素の関連を考え，その比率によってトラフィックを特徴づける。一例を**図5**に示す。図では，ネットワーク層，トランスポート層，TCPフラグ，TCP Portなどを例に挙げているが，比を取って意味を成すものであれば他の要素にも適応できる。たとえば確実ではないがTCP Portによるトラフィックの特徴づけは前章の課題②に対して有効である。他にも，送信元の国別に比を取ることで海外からの攻撃状況を特徴付けられ，セグメントごとにアクセス数の比をとることでインターネットのエッジに近いプローブなのかコアに近いプローブなのかが特徴付けられるなど，前章の課題①に対しても有効な解決策となる。

以上のようなトラフィックの特徴づけにより，プローブ間でデータ比較が可能となり，有意なデータ差を得ることができる。たとえばTCP Portの比率が似ている，つまり利用アプリケーションが似ているトラフィックでは，その他の要素の比率も似通ったものになる可能性が高いため，利用アプリケーションが似ている別のプローブで取得した他の要素と比較することで意味のあるデータが得られる。

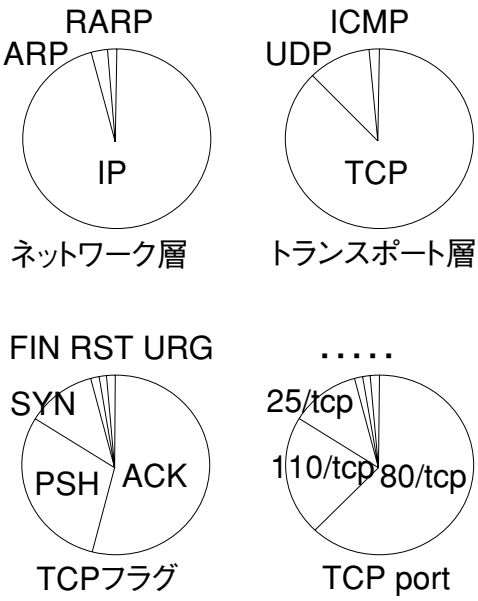

図5　トラフィックの特徴要素（例）

また，ネットワーク上の同じ場所でトラフィックを観測する限りにおいて，トラフィック量が変わってもこの比率は大きく変動することは無いと考えられる。よって各比率が大きく変動することでワームやDDoSの発生させる異常トラフィックが検知できる可能性がある。この点に着目した異常検知手法の特徴を次に述べる。ここで提案する異常検知では，**図6**に示すように，教師データを用いて評価データを評価する方式を用いる。ここで，教師データとは過去一定期間の同じプローブで取得したデータのうち評価データを評価するのに適したデータ群であり，評価データとは同プローブで取得したデータのうち最も新しいデータである。また，データは前述した各要素の比率である。この教師データと評価データに対して適切な評価式[4] を用いることで，プローブが評価したデータの“異常度”が計算される。“異常度”は “評価データは過去データとどの程度の違いがあるか”を示し，全く同じである場合は0，違いが大きい場合はその分大きな値になる。

ここまで説明してきたとおり，プローブ間で単純比較可能な比率を用いて異常度を計算し，現在のプローブの状態を特徴付けることにより，シングルプローブシステムをマルチプローブシステムに拡張するための前章で挙げた課題を解決した。

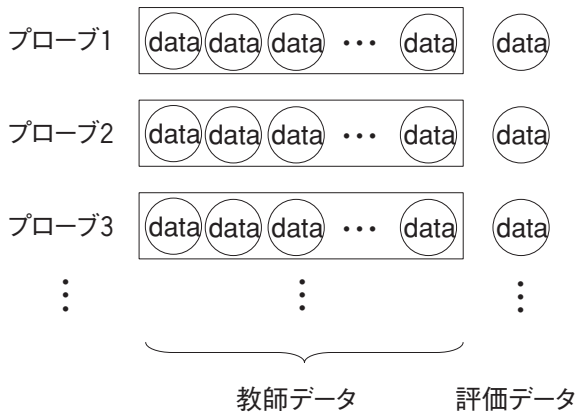

図6　提案する異常検知方式

最後に，マルチプローブシステムにおける異常検知の概要を示す。**図7**は，マルチプローブを用いた異常検知の説明図である。ネットワーク内には複数のプローブが設置され，前述した異常度を計算し続けている。この異常度が一定の閾値を超えたときを異常状態と定義すると，図の左で示すようにネットワーク全体に異常が発生した場合と図の右で示すようにネットワークの一部で異常が発生しているなどの異常な状態検知が可能となる。また，異常度の値を段階的に区別することによって，異常が広がりつつある状況を検知できる。

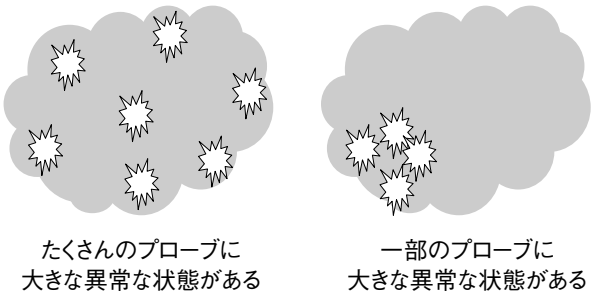

図7　マルチプローブでの異常検知

次に，異常と判断した原因を切り分け，その原因を解析する。各プローブは**図5**で示した各要素に関しても異常度を計算しているため，異常と判定した要素とその度合いがわかる。したがって，異常と判定した要素の組み合わせとその度合いが似ているものは，異常と判定した原因が同じと判定できる。さらに異常度の大きな1つ以上の要素を解析することで，原因となるワームやDDoSのプロトコルや特徴を把握することができ，検知した異常に対する対策を立てることもできる。

本稿では主にワームをどのように検知にするかに主眼を置いて説明したため，DDoSの検知に必要な“早期検知”に関してはほとんど触れていない。“早期検知”に関する取り組みは今後の課題である。

ま と め

本稿では，ネットワークの脅威としてワームとDDoSを挙げ，それらの脅威が発生させるトラフィックの異常を早期に検知する定点観測システムについて述べた。さらに，シングルプローブをマルチプローブに拡張する際に考慮すべき点を整理し，提案する手法の概要を述べた。

世の中は“いつでも”“どこでも”“だれでも”を合言葉としたユビキタスネットワーク社会へと向かっており，多くの便利さが提供されている。その一方で，ネットワークは有線と無線の混在が当然になるなど多様化・複雑化が進み，ネットワークの抱えるリスクは急激に上昇している。沖電気はe社会の実現に向けて，安全・安心なインターネットを実現するためのネットワーク異常検知の研究を続けていく予定である。

謝　辞

本研究は，情報通信研究機構（NiCT）の委託研究テーマ「広域モニタリングシステムに関する基盤技術の研究開発」の一環として行われているものである。ここに深謝する。 ◆◆

■参考文献

1）JPCERT/CC：インターネット定点観測システム，
http://www.jpcert.or.jp/isdas/
2）警察庁：インターネット定点観測，
http://www.cyberpolice.go.jp/detect/observation.html
3）IETF：Packet Sampling Working Group，
http://www.ietf.org/html.charters/psamp-charter.html
4）中村 他：トラフィックの内部状態変化を利用したネットワーク異常検知，電子情報通信学会，信学技報，NS2005-5

●筆者紹介

中村信之：Nobuyuki Nakamura. 研究開発本部 ユビキタスシステムラボラトリ