トラフィック監視・分析技術

インターネットのライフライン化に伴い，サービス継続の要求が高まる一方で，その攻撃手段が多様化しています．このような問題を解決する一手段として，フロー情報を活用して異常トラフィックを多角的に監視・分析する技術が注目されています．本稿では，このような技術の開発動向について紹介します．

村山 純一（むらやま じゅんいち）/小林 淳史（こばやし あつし）/倉上 弘（くらかみ ひろし）
桑原 健（くわはら たけし）/石橋 圭介（いしばし けいすけ）/三宅 延久（みやけ のぶひさ）
NTT情報流通プラットフォーム研究所

多様化するネットワーク攻撃手段

IP（Internet Protocol）ネットワークが普及し，ライフラインとしての役割が期待されています．このため，IPサービスの継続的な提供が重要な目標になっています．また，NTTグループのCSR（Corporate Social Responsibility：企業の社会的責任）憲章でも「安心・安全なコミュニケーション」が目標として掲げられています．

一方で，インターネット上での攻撃手段が多様化しており，これらの対策手段の確立が課題となっています．このような攻撃の例としては，大量の無効パケットを送りつけ，サーバをダウンさせるようなDDoS（Distributed Denial of Service：分散型サービス妨害）攻撃が有名です．

また，DNS（Domain Name System）サーバの内容を改ざんしてフィッシングサイト向けの偽IPアドレスを通知するキャッシュポイゾニング攻撃や，偽の経路情報を流すことで，サーバにアクセスできなくさせてしまう経路ハイジャック攻撃なども現れています．

NTT情報流通プラットフォーム研究所では，このように多様化する攻撃を防御するネットワークセキュリティ技術として，フロー情報を活用した多角的トラフィック監視・分析技術の研究開発を行っています．ここでは，これらの中から，DDoS攻撃対策，DNS攻撃対策，BGP（Border Gateway Protocol）経路ハイジャック対策およびフロー品質モニタリングにかかわる技術の開発動向を紹介します．

＊本研究開発は，総務省委託研究「次世代バックボーンに関する研究開発」の成果を含みます．

DDoS攻撃への対策技術

NTTグループのDDoS攻撃対策技術としては，トラフィック解析システムSAMURAI[1]があります．SAMURAIは，サンプリングされたフロー情報を基に，特定の攻撃パターンをシグネチャ機能で分析するとともに，異常なトラフィック増加をベースライン検知機能で分析します．これにより，特定サーバへの攻撃元を特定することができ，ルータのACL（Access Control List）やDDoS攻撃軽減対策アプライアンスCisco Guardなどにより攻撃トラフィックをフィルタリングすることが可能です．この技術はNTTコミュニケーションズで実際に活用されています．

ところで，DDoS攻撃では攻撃元が非常に多い場合があり，この場合送信元IPアドレスによるACLの設定が困難になる場合もあります．このときに用いられるのが異常トラフィック特定システムDELTAA[2]です．

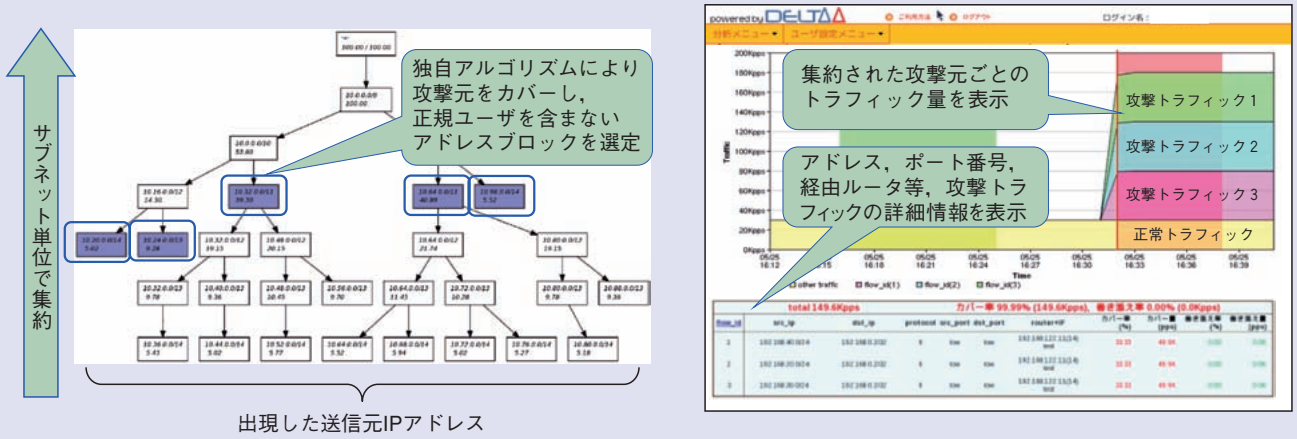
DELTAAはトラフィックを急増させたホストを攻撃元と認識して，これをサブネット単位に集約していきます．この際に，正規ユーザが含まれないように，緻密な計算を行います（**図1**(a)）．超多数の攻撃元が少数のサブネットとして特定されるため，攻撃トラフィックは，ルータのACLにより簡単にフィルタリングすることができます．

DELTAAは，このほかに，集約された攻撃元ごとの攻撃トラフィック量や攻撃開始時刻などを可視化する機能も搭載しています（図1 (b)）．これにより，オペレータがDDoS攻撃を容易に把握することが可能となります．

現在，DELTAAはSAMURAIと連携したかたちでの実用化を目指しています（**図2**）．

DNS攻撃への対策技術

DNS攻撃としては，フィッシングサイト等の偽IPアドレスを通知させるDNSキャッシュポイゾニング攻撃が知られています．DNS攻撃を検出するために用いられるのが，DNS攻撃監視・



(a) DELTAAによる攻撃元IPアドレスの集約

(b) DELTAAによる攻撃トラフィックの可視化

図1　DELTAAによる異常トラフィック特定

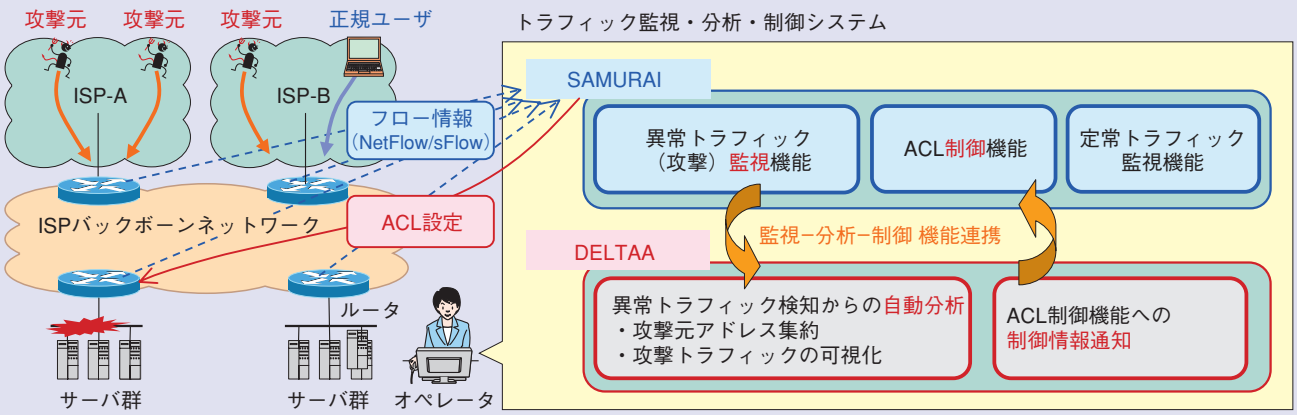


図2　DELTAAとSAMURAIの連携

分析ツールKOROKUです．KOROKUでは，DNSサーバ宛のトラフィックから全数サンプリングされたフロー情報[3]を監視・分析します．

DNSキャッシュポイゾニング攻撃の場合，偽装された名前解決応答パケットのみが多数DNSサーバ宛に到着することから，全数サンプリングされたフロー情報を監視・分析することで，これらの攻撃を検出することが可能となります（**図3**）．

現在，KOROKUは，プロトタイプでの実機検証やデモンストレーションを行っています．

BGP経路ハイジャックへの対策技術

インターネット上の一部の経路を密かに不正な経路に変更してしまう攻撃としてBGP経路ハイジャック攻撃が知られています．

このような攻撃を検出するために用いられるのが，BGP経路トラフィック分析システムSASUKEです．SASUKEでは，BGPルータと直接BGPピアリングすることで，BGP経路情報を収集し，各ルータから収集されてくるサンプリングされたフロー情報との相関性を監視・分析することで，トラフィックに影響を与えるような経路ハイジャック，経路変動を検知します．

インターネット上のBGP経路の数は膨大なため，これらの正当性を１つひとつ検証することは現実的ではありません．そこで，SASUKEでは，BGP経路変動を検知すると，これにかかわるトラフィック流量の多少を分析します．トラフィック流量が多い場合には，アラートを挙げ，経路変動の原因究明をオペレータに促します（**図４**）．

現在，SASUKEはプロトタイプでの実地検証やデモンストレーションを行っており，将来的なDELTAA/SAMURAIと連携した実用化を模索しています．

フロー品質モニタリング技術

IPTVやVoIPなどのリアルタイムアプリケーションの普及によって，ネットワークとユーザ間での故障切り分けの難易度が高まっています．このため転送品質の監視が重要な課題となっています．

このようなネットワーク側での品質監視を行うツールとして，IPTV（マルチキャスト）品質監視ツールQcastがあります．Qcastでは，IPTVの転送品質を監視する場合，該当するマルチキャストツリーから特定の頻度で全数サンプリングされたフロー情報を監視・分析します．

IPTVのようなリアルタイムトラフィックでは，パケットが定期的に流れ続けるため，全数サンプリングされたフ

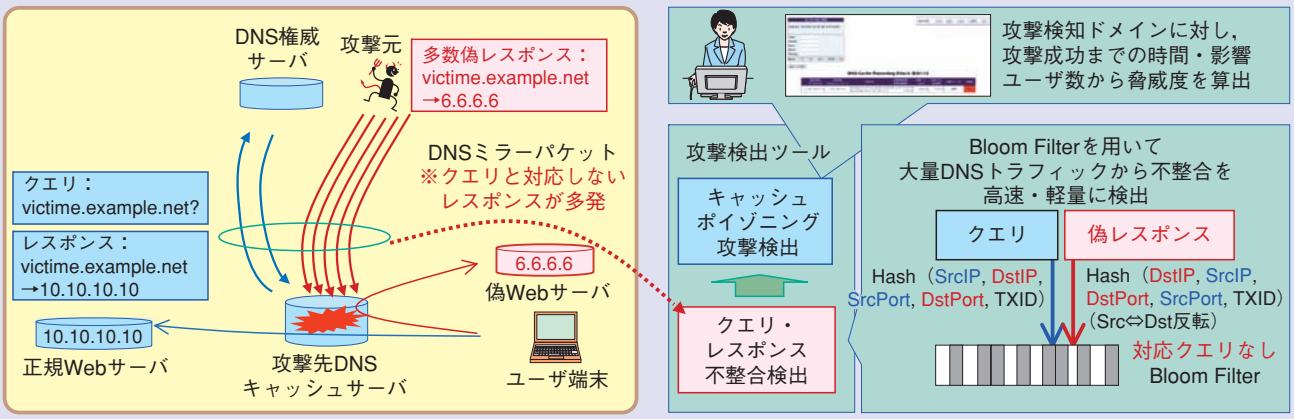


図３　DNS攻撃検出ツール（KOROKU）

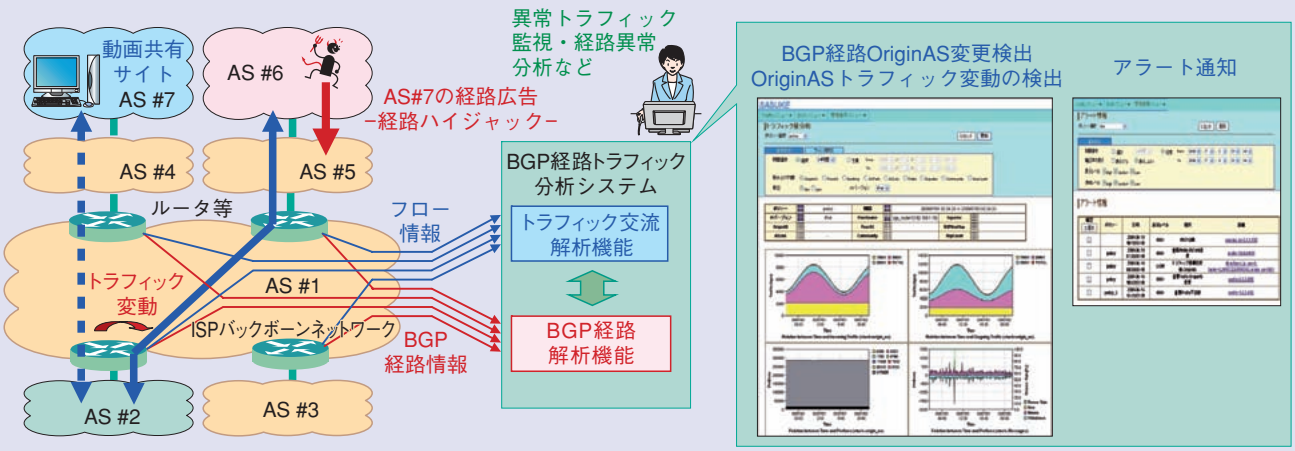


図４　BGP経路トラフィック分析システム（SASUKE）

ロー情報も定期的に生成されることになります．したがって，このフロー情報の到着間隔を監視・分析することで，パケットが適切な品質で転送されているかどうかを確認することができます（**図5**）．

また，同様の手法でVoIPの転送品質を監視・分析するツールとしてVoIP品質監視ツールvoipScoopがあります．voipScoopでは，あらかじめSIP（Session Initiation Protocol）シグナリング情報を監視のうえ，該当するRTP（Real-time Transport Protocol）メディア情報を特定し，この転送品質を監視するといった，シグナル－メディア連携監視も実現しています（**図6**）．

現在，QcastやvoipScoopはプロトタイプでの実機検証やデモンストレーションを行い，将来的な実用化を目指しています．

多角的な監視・分析技術

これまで述べたように，多様化するネットワーク攻撃に備えるためには，フロー情報をさまざまなかたちで活用することが重要です．このような基盤技

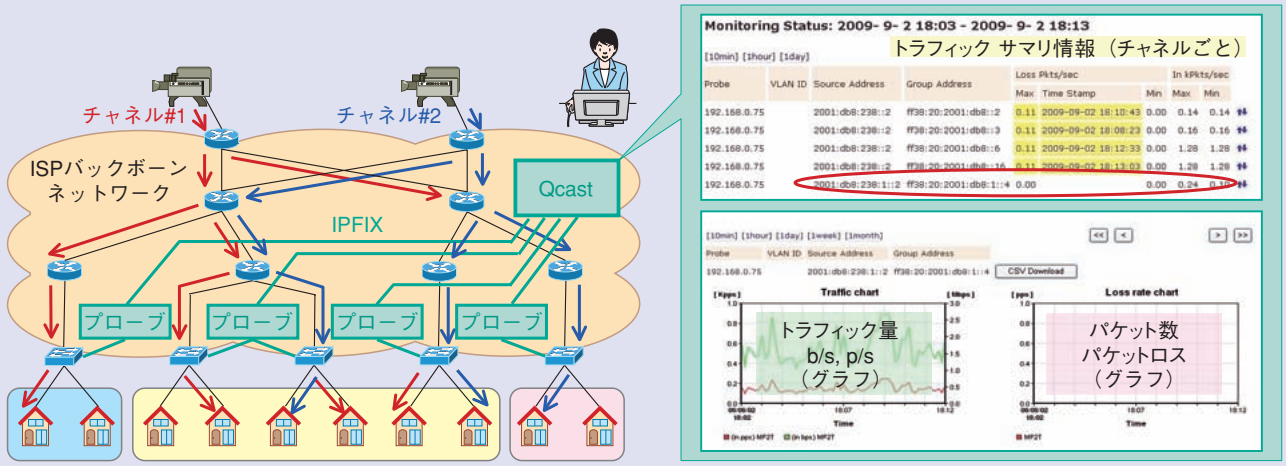


図5　IPTV（マルチキャスト）品質監視ツール（Qcast）

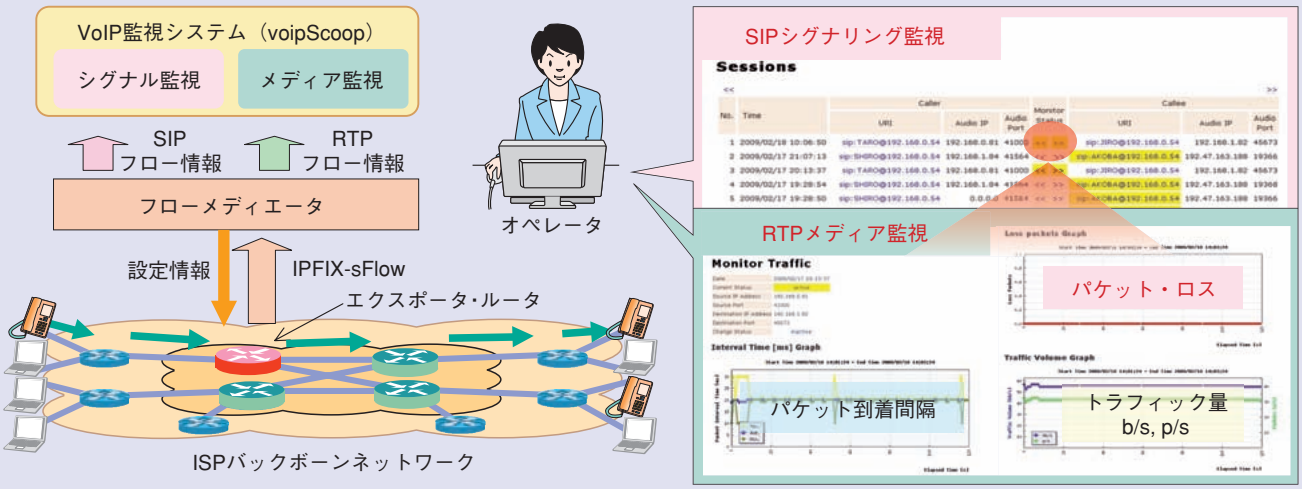
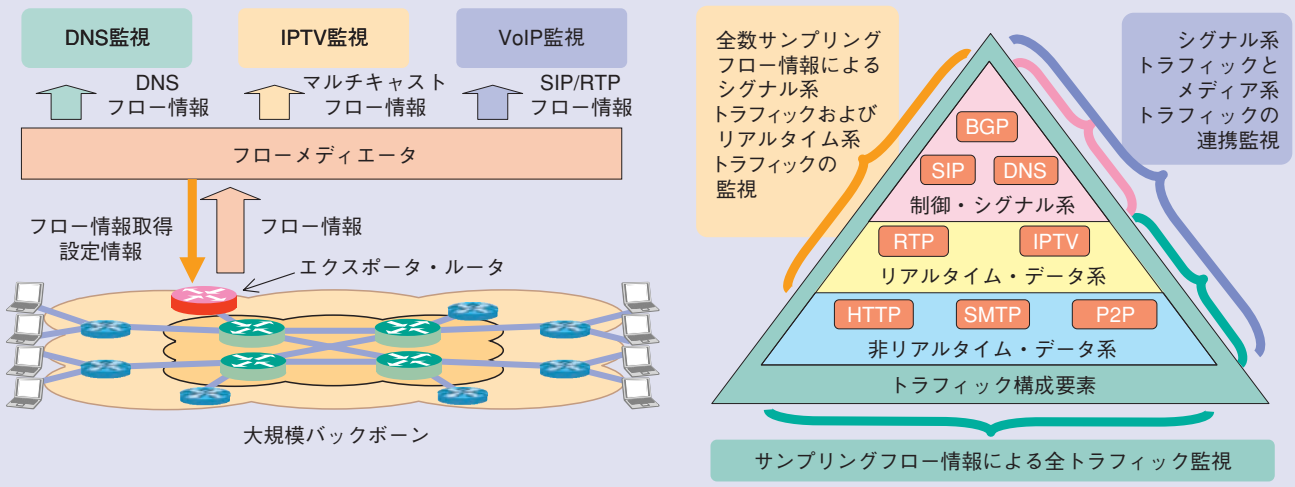


図6　VoIP品質監視ツール（voipScoop）



(a) 多様なフロー情報の監視目的に応じた分配　(b) 多様な攻撃への網羅的な対処アプローチ

図7　フローメディエーション基盤技術（ScoopFlow）

術として，フローメディエーション基盤技術ScoopFlowの研究・開発を行っています．

この技術の中核となるのはフローメディエータです．このツールは，ルータからさまざまなフロー情報を収集し，これを適切なコレクタ（監視・分析装置）へ分配します．また，必要に応じて，要求されたフロー情報を収集できるようルータの制御を行います（**図7**(a)）．

最終的には，①サンプリングフロー情報による全トラフィックの監視，②全数サンプリングフロー情報によるシグナル系トラフィックおよびリアルタイム系トラフィックの監視，③シグナル系トラフィックとメディア系トラフィックの連携監視，といった3つの視点によって，多様な攻撃に網羅的に対処していきます（図7(b)）．

このフローメディエーション技術は，幅広い普及が重要であることから，プロトタイピングだけでなく，IETF・IPFIX WGにおいて標準化活動にも取り組んでいます[4]．

今後の取り組み

今後も攻撃手段の多様化が予想されますが，前述の対策手段を適切に選択・活用することで，効率的に攻撃防御の網羅性を高めていきます．今後は各技術の実用化に向けて，フィールドトライアルやデモンストレーションを積極的に行っていく予定です．

■参考文献

(1) 水口・神谷・吉田・桑原・ホウバッ・牛久・宮川・市川：“トラフィック解析システムSAMURAIとサービス展開，”NTT技術ジャーナル，Vol.20，No.7，pp.16-19，2008.
(2) 川原・森・原田・上山・近藤・石橋：“異常トラヒック測定分析手法，”NTT技術ジャーナル，Vol.20，No.3，pp.21-25，2008.
(3) 山本・小林・近藤・廣川・石橋：“大規模ネットワーク向け異常トラヒック監視システムの開発，”NTT技術ジャーナル，Vol.20，No.3，pp.16-20，2008.
(4) A. Kobayashi and H.Nishida：“IPFIX Mediation: Framework，”IETF Internet-Draft，Oct. 2009.

（後列左から）桑原　健/ 小林　淳史/ 石橋　圭介
（前列左から）倉上　弘/ 三宅　延久/ 村山　純一

NTT情報流通プラットフォーム研究所では，今後も安心・安全なコミュニケーションの実現を目指していきます．

◆問い合わせ先
NTT情報流通プラットフォーム研究所
セキュアコミュニケーション基盤プロジェクト
TEL　0422-59-3949
FAX　0422-59-5660
E-mail　murayama.junichi@lab.ntt.co.jp