

インターネットトラフィック制御システム (i-TRACS) の開発

NTTでは、大規模なISP網における異常トラフィックの制御技術の研究開発に取り組んでいます。本稿では、トラフィック監視装置やネットワーク制御装置と連携して、DDoS攻撃などの異常トラフィックの検知から制御までを広域ネットワーク上で実現するインターネットトラフィック制御システムについて紹介します。

くわはら たけし やぎ たけし
桑原 健 / 八木 毅
 むらやま じゅんいち
村山 純一

NTT情報流通プラットフォーム研究所

インターネットにおける異常トラフィックの制御を目指して

インターネット上の異常トラフィックの中でもDDoS (Distributed Denial of Service) 攻撃は、近年多発しているサイバー攻撃の一種です。このような異常トラフィックを排除するためには、ネットワークのトラフィックを常時監視し、詳細に分析することで異常なトラフィックを識別し、これを廃棄するためにネットワーク装置に対して制御を行う必要がありました。トラフィックの監視や分析には高度なスキルが要求されるだけでなく、ネットワーク装置の設定をその都度変更することは、ISP (Internet Service Provider) のオペレータにとって非常に大きな負担となっていました。

NTT情報流通プラットフォーム研究所では、今後、ネットワークが大規模化し広帯域化が進んだ環境においても、異常トラフィックの対策をISPのネットワーク全体で実施可能なシステムとして、WINDS (Wide-area InterNet Defensive -System by traffic anomaly mitigation: 広域異常トラフィック検知・制御システム) の研究開発を行っています。異常トラフィックとして

は、DDoS攻撃以外にもさまざまな異常トラフィックを検知し、制御を可能とすることで安心・安全なネットワークの実現を目指しています。

インターネットトラフィック制御システム (i-TRACS) の概要

我々は、WINDSの中核的なシステムとして、i-TRACS (Internet Traffic Control System: インターネットトラフィック制御システム) のプロトタイプを開発しました (図1)。i-TRACSは、ISPのオペレータ向けのシステムであり、従来、運用上大きな負担となっていた異常トラフィックの初期監視から詳細分析、対処のためのネットワーク制御に至る一連のオペレーションが、簡単な操作によって行えるようになります。また、後述する監視装置や分析装置、ネットワーク制御装置などと連動し、これまで困難であった広域ネットワークにおける総合的な異常トラフィックの対策を可能とします。

■ i-TRACSと連携する装置群

i-TRACSは、WINDSを構成する1装置であり、以下の3つに大別される装置群と連携して制御するためのシステムとして位置付けられます (図2)。

(1) 監視装置

監視装置は、ルータなどのネットワーク装置からトラフィック情報を収集し、異常を検出した場合、アラート情報をi-TRACSに送信します。

監視装置としては、階層的に収集したトラフィック情報の交流分布を監視して異常を検出するNail-mx広域監視装置を開発しています。

(2) 分析装置

分析装置は、i-TRACSからの異常トラフィックの分析依頼を受けると、トラフィック情報を詳細に分析し、異常フローの特定を行いi-TRACSに通知します。ここで、フローとは、IPアドレスやポート番号、プロトコルが同一のIPパケットの集合であり、DDoS攻撃などを防止するルータの設定情報を生成するための元情報となります。

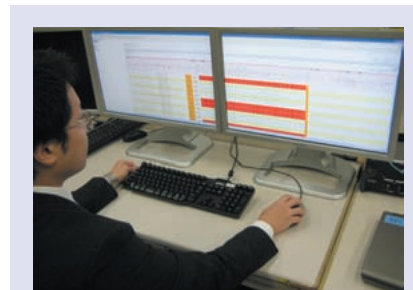


図1 i-TRACSのプロトタイプ

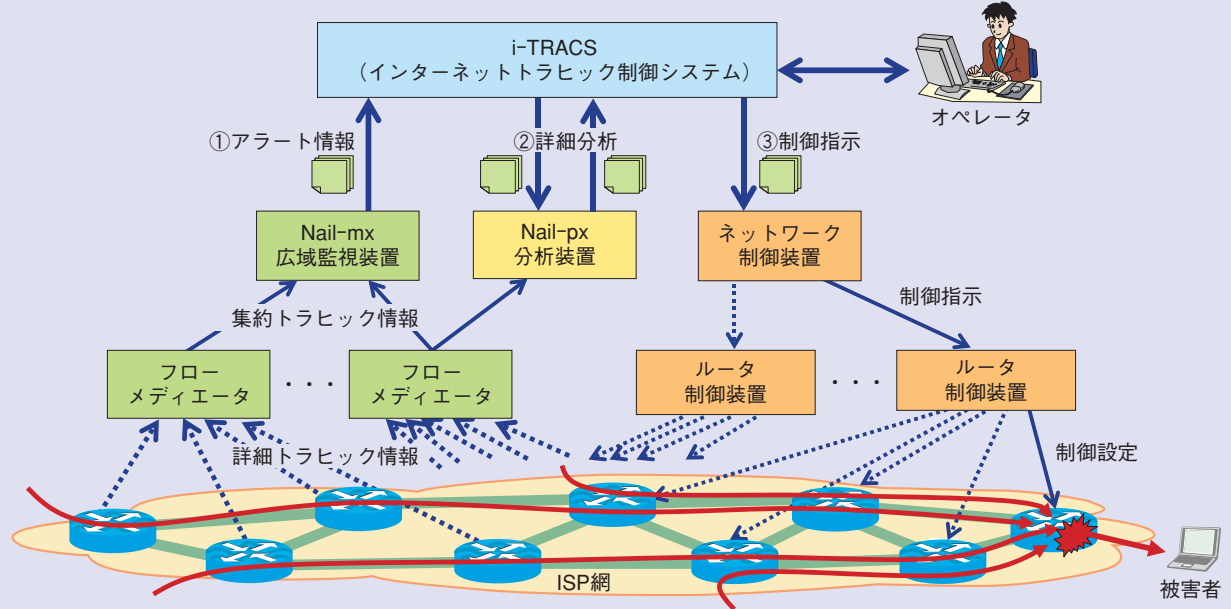


図2 i-TRACSのシステム構成と動作概要

分析装置としては、蓄積されたフロー情報から定常時と異常時を比較して異常フローを抽出するNail-px分析装置を開発しています。

(3) ネットワーク制御装置

ネットワーク制御装置は、i-TRACSからの異常フローの制御指示を受けて、ネットワーク内で異常フローを防止するための設定を行うポイント（制御対象となるルータやそのインタフェース）を自動的に特定し、設定を行います。配下に収容するルータ制御装置と階層構造を取ることで、多数のルータに対して短時間で制御を行うことが可能

です。

■ i-TRACSの動作概要

i-TRACSは、前述の3つの装置群と接続し、以下のように動作することで異常トラヒックの検知から制御までの一連の処理を行います。

(1) アラート情報の受信

異常トラヒックが発生すると、広域監視装置からアラート情報がi-TRACSに送信されます。大規模ネットワークを監視する際には、短時間で大量のアラートが発生する場合があります。オペレータが個別のアラート情報を確認することが困難な状態になるケースがありま

す。そこでi-TRACSでは、受信したアラート情報の中から集約可能なものをまとめたうえでオペレータに提示することで、この問題を解決しています。受信したアラート情報には受信時刻と識別番号が付与され、時系列で管理することができます。

(2) 詳細分析と異常フローの管理

オペレータは、i-TRACSが受信したアラート情報に対して詳細な分析を要求することができます。i-TRACSは、オペレータが指定したアラート情報を基に、分析装置に対して分析要求を送信します。この分析要求には、ア

ルート情報から抽出した時間情報や監視対象となっていたルータ情報が含まれており、i-TRACSはこれらの情報を監視装置から分析装置に効率的に受け渡す役割を担っています。

分析装置では、トラフィック情報を詳細に分析し、異常フローを特定し、結果をi-TRACSに返します。i-TRACSは、この分析結果の中から一定しきい値以上の値を持つフロー情報のみを異常フローとしてデータベースに蓄積し、オペレータ用の画面に表示します。このようにすることでオペレータが確認しなければならない情報量を削減する効果があります。

(3) ネットワーク制御の指示

オペレータは分析結果として得られた異常フロー情報の内容を確認し、制御を行うか否かを判断します。オペレータが制御すべき異常フローを選択すると、i-TRACSは実施可能な制御

方法をオペレータに提示し、候補の中から制御方法が決定される仕組みを採用しています。このように重要な判断を伴う処理はオペレータを介在させることで安全なネットワーク制御が可能となります。

制御方法が決定されると、i-TRACSはネットワーク制御装置に対して、防止すべき異常フローと制御方法を通知します。ネットワーク制御装置は、これを基に制御ポイントを特定し、ルータ制御装置を介して異常フローを防止する設定をルータに行います。

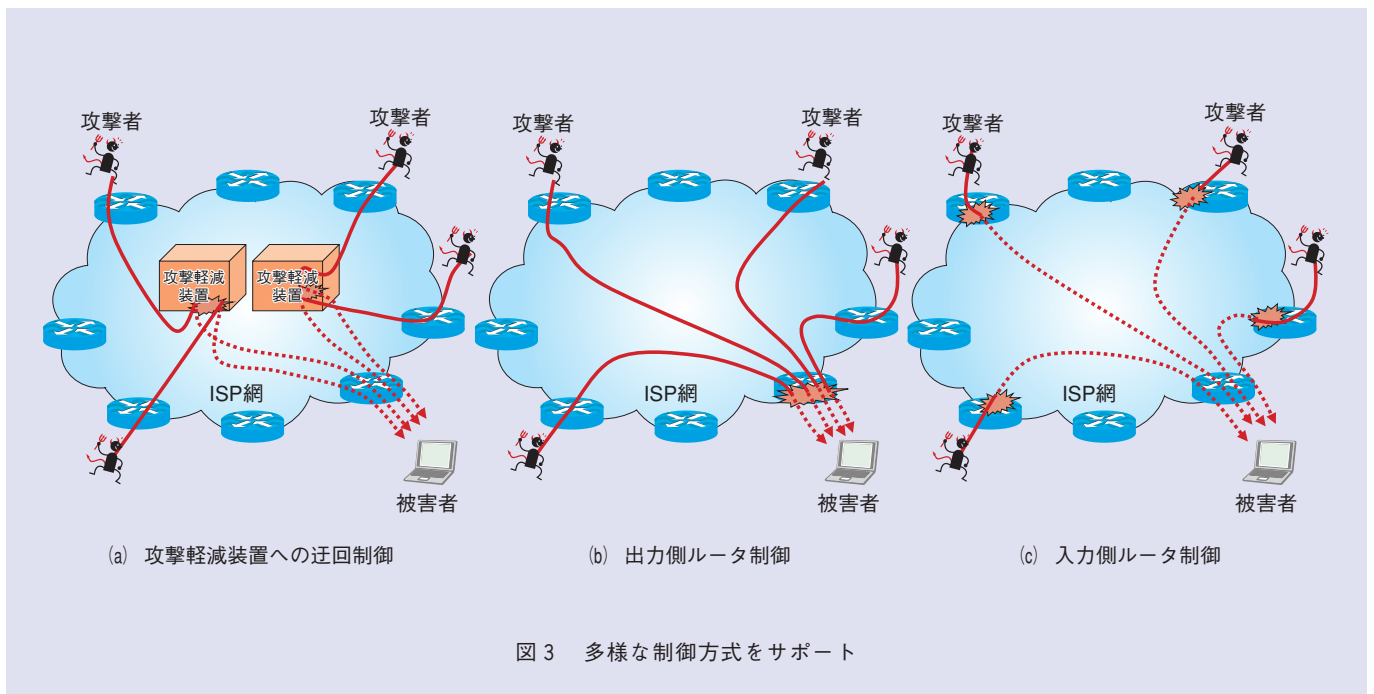
i-TRACSの特徴

■多様な監視方式・ネットワーク制御方式をサポート

i-TRACSは、監視装置やネットワーク制御装置と連携して広域なネットワーク全体を多様な方式で監視および制御することができます。

監視方法としては、トラフィックの交流分布を監視する広域監視のほかに、特定のサーバ向けのトラフィック量をしきい値判定で監視する方法や特定のアプリケーションの packets 内容を監視してアプリケーションレベルの異常を検知する方法もサポートしています。

ネットワーク制御についても同様に複数の方式をサポートしています(図3)。i-TRACSでは、攻撃軽減装置⁽¹⁾と呼ばれるDDoS攻撃対策用のアプリケーションへのトラフィック迂回制御や負荷分散制御を行うことが可能です。トラフィックを迂回させるため、ネットワークの利用効率は低下しますが、攻撃軽減装置の機能により、異常トラフィックを詳細に特定して廃棄することが可能です。また、ネットワーク全体で攻撃軽減装置を共用することができ、経済的にDDoS攻撃の対処を行うことができます。



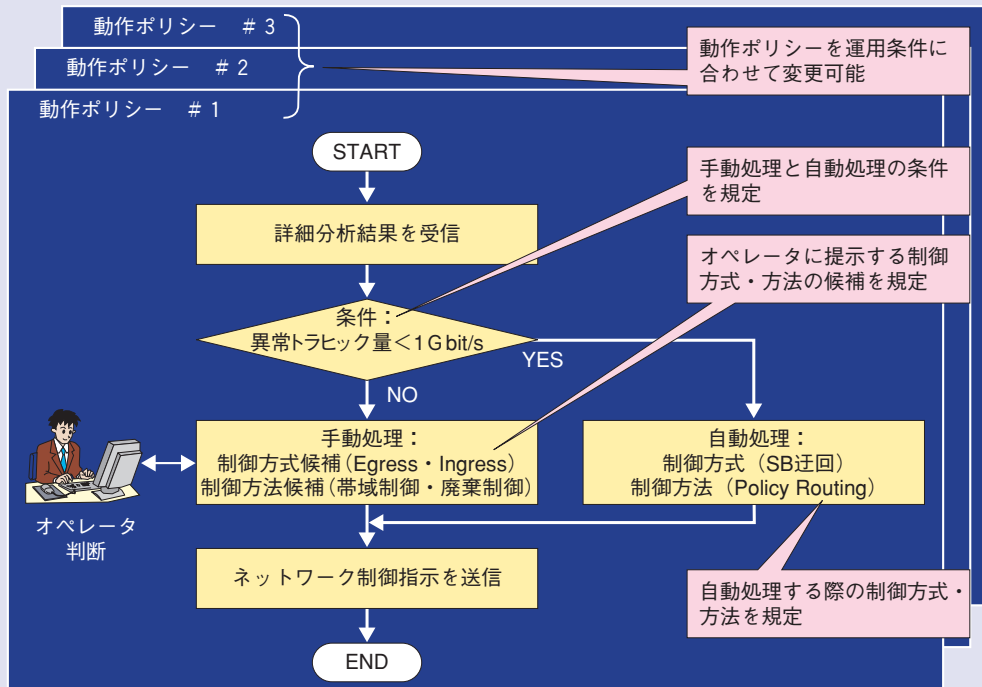


図4 動作ポリシーの例

一方、ネットワーク内の適切なポイントでフィルタ制御や流量制限を行うことで、異常トラフィックを抑制することも可能です。具体的には、出力側のエッジルータに対する制御や、入力側のエッジルータを特定し対処を行う制御方式を選択することができます。DDoS攻撃の場合、出力側の制御方式は制御ポイントが集中するためにルータの設定は容易ですが、出力側で制御するため異常トラフィックがネットワークを通過することとなり、ネットワーク全体のリソースを消費します。対して入力側で制御する方式は、ネットワークの入口で制御を行うためにネットワークへの影響を最小に抑えることができますが、DDoS攻撃の場合、攻撃元が分散しているため、多数のルータに対し

て設定を行う必要があります。

このようにさまざまな監視方式・ネットワーク制御方式をサポートすることで、多様化する攻撃種別や異常トラフィックに応じて、適切な対処を行うことが可能となります。

■対話型ユーザ・インタフェースとカスタマイズ性

異常トラフィックを短時間で適切に対処するためには、オペレータが大量でかつ多様なアラート情報の中から必要な情報を抽出し、詳細に分析を行い、その結果から対処すべきか否かを迅速に判断し、的確な対処方法を決定して実施する必要があります。したがって、オペレータに対して最適な情報を提示し、一連の操作が簡易に行えることが重要となります。

i-TRACSを操作するオペレータは、GUI (Graphical User Interface) を利用して、アラート情報を確認したり、ネットワーク制御の指示を出すことができます。その際、あらかじめシステム内に規定された動作ポリシーによって、自動制御の実行条件や、オペレータの判断を仰ぐ制御方法の設定画面の表示内容を規定することができます (図4)。これにより、システムの動作仕様を運用環境に応じてカスタマイズすることが可能となるとともに、オペレータに高度なスキルを要求することなく、一連の処理が可能となるため、運用負荷が軽減されることが期待されます。

■柔軟性、拡張性の高いシステム

i-TRACSは、多様な監視装置や

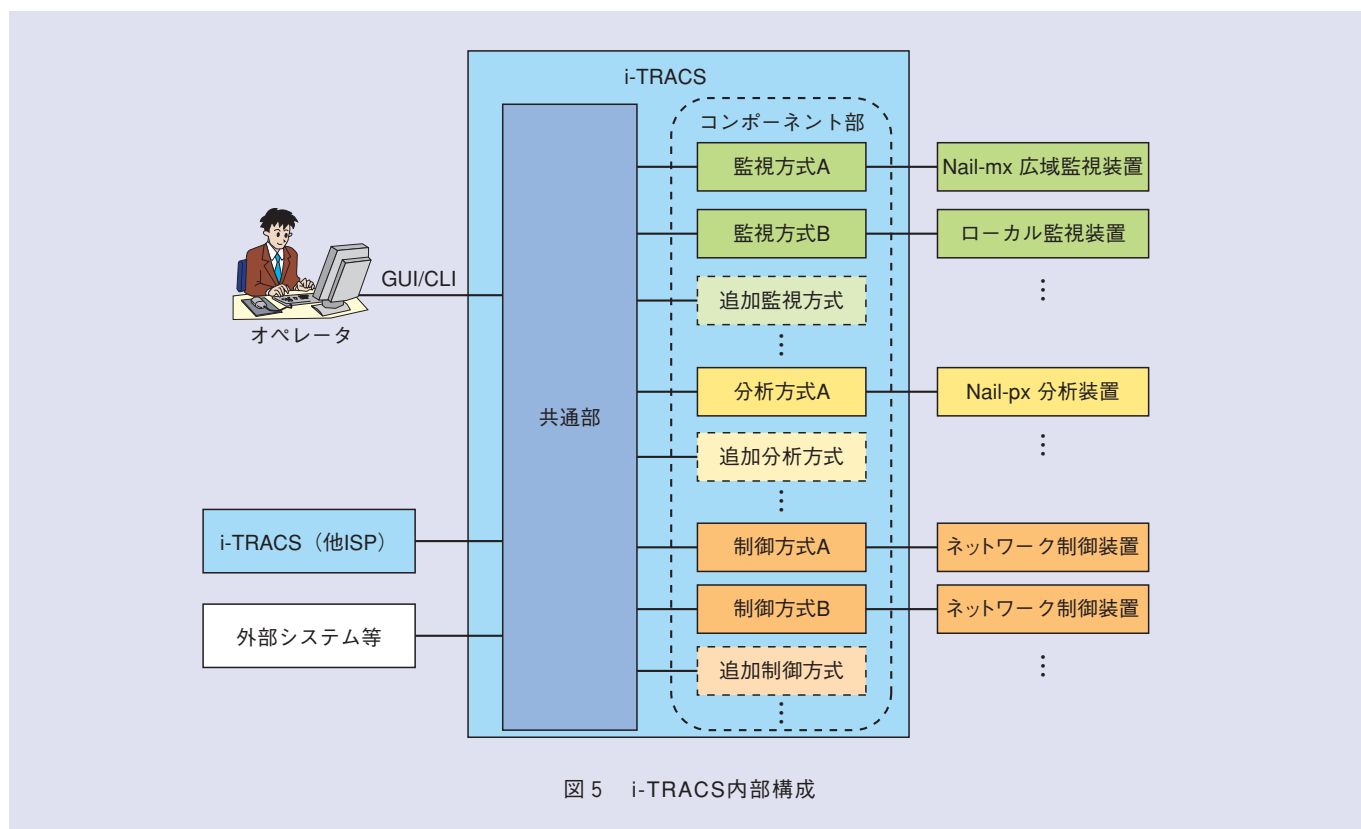


図5 i-TRACS内部構成

ネットワーク制御装置と連携することを前提とした内部アーキテクチャを採用しています(図5)。監視、分析、ネットワーク制御の対向装置ごとの機能を持つコンポーネント部と、アラート情報やネットワーク制御の状態を管理し、オペレータ向けのGUIなどの機能を持つ共通部によって構成することで、各コンポーネント部の独立性を保っています。また、外部装置とのインタフェースには汎用性・拡張性の高いXML-RPC (Extensible Markup Language-Remote Procedure Call)⁽²⁾を採用することにより、システムとしての拡張性を確保しています。

このような構造を取ることで、今後新たに発生する攻撃やさまざまな異常トラフィックに対しても、対応する外部

装置とコンポーネント部を追加することで機能を拡張することができます。

今後の取り組み

今後は開発したi-TRACSのプロトタイプを用いて、さまざまな監視装置、分析装置、ネットワーク制御装置との接続性や多様な制御方式を検証していきます。また、ISP網を模擬したテストベッドを構築し、運用性などの評価を通じて、さらなる機能追加や改善を図っていく予定です。

■参考文献

- (1) 八木・大倉・田邊・村山・外山：“DDoS攻撃軽減装置共用化のためのネットワーク制御方式の評価,” 信学技報, Vol.106, No.420, pp.103-108, 2006.12.
- (2) <http://www.xmlrpc.com/spec/>



(左から) 八木 毅/桑原 健/
村山 純一

NTT情報流通プラットフォーム研究所では、今後も次世代のインターネットセキュリティ技術の研究開発を通じて、安心・安全なネットワークと豊かなコミュニケーション社会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 0422-59-3333
FAX 0422-59-5637
E-mail kuwahara.takeshi@lab.ntt.co.jp