

# 広域異常トラフィック検知・制御システム (WINDS) のアーキテクチャ

NTT情報流通プラットフォーム研究所では、インターネットサービスプロバイダのような大規模なIPネットワークにおける異常トラフィックの検知と制御を目的として、広域異常トラフィック検知・制御システム (WINDS) の研究開発を行っています。本稿ではシステムのねらいとアーキテクチャを紹介いたします。

にしだ はるひこ むらやま じゅんいち  
 西田 晴彦 / 村山 純一  
 いしばし けいすけ こばやし あつし  
 石橋 圭介 / 小林 淳史

NTT情報流通プラットフォーム研究所

## 広域異常トラフィック制御の必要性

DDoS (Distributed Denial of Service: 分散サービス拒否攻撃) という言葉をお聞きになったことがある方は多いと思います。これはネットワーク上で多数の攻撃者が対象に向かって攻撃を行い、対象のサービス提供を不能にするものです。従来の攻撃者が1拠点であるDoS (Denial of Service: サービス拒否攻撃) と比較すると攻撃者以外へのサービス提供を止めずに対処することが難しいという特徴があります (図1)。従来これらの攻撃への対処は、主な標的が企業等のサイトであったことから企業向けのアプライアンス製品等の導入が一般的な手法でした。しかしDDoSでは攻撃側1拠点からの攻撃トラフィックが少量であっても、全体としては数Gbit/sになるような攻撃が可能となるため、標的のサービスだけでなく、網全体への影響も問題になってきます。また、顧客サイトが攻撃されるケースにおいて、顧客側での対処では顧客への回線の輻輳には対応できないため、網側のオペレータの協力や作業が必要となります。

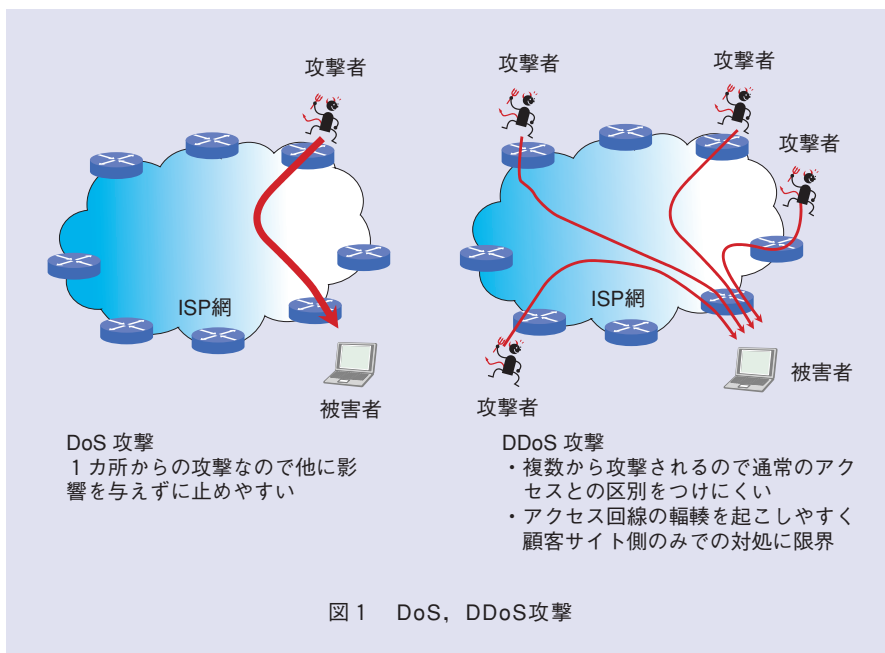


図1 DoS, DDoS攻撃

広域異常トラフィック検知・制御システム (WINDS) はISP (Internet Service Provider) のような大規模な網を対象に、DDoS等を含む網として対処が必要な異常を検知し、それに対して必要な制御を行います。網の規模としては数年先の大規模ISPレベルを想定して、交換トラフィックの総量が約10 Tbit/s程度、検知・制御対象のルータが1000台程度として、研究開発を行っています。

## 異常トラフィックへの対処の流れ

異常トラフィックの検知・制御は検知を監視と分析に分割し、これに制御を加えた3つのフェーズに分かれます (図2)。この3つは一般的な異常対処時のオペレーションの流れと同じですが、現状のISPより大きな網への適用性を確保するため各フェーズでさまざまな工夫がほどこされています。

### ■監視

監視フェーズは網を構成するルータ等の装置からそこを通過するトラヒッ

\* 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』による成果です。

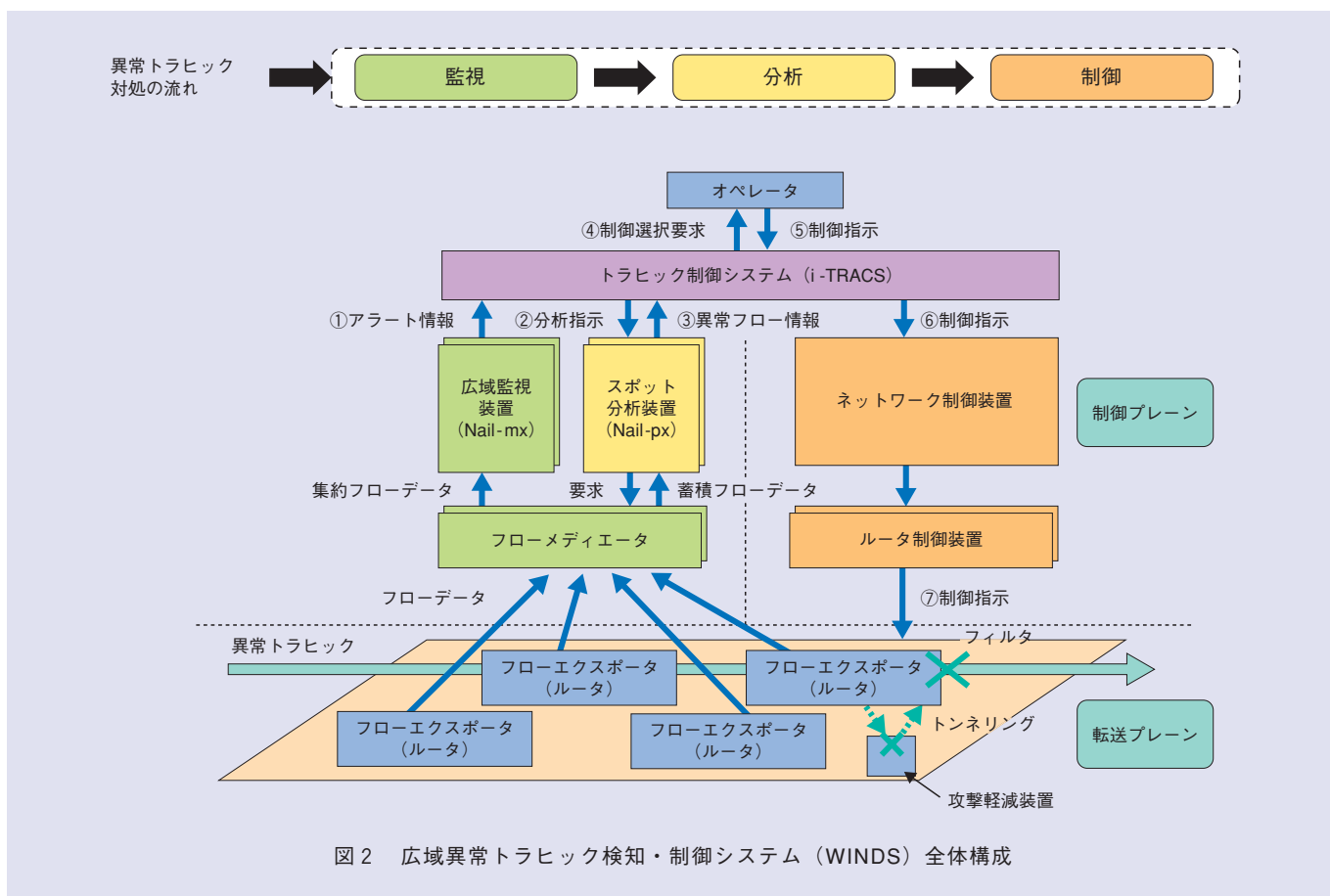


図2 広域異常トラフィック検知・制御システム (WINDS) 全体構成

クに関する情報を常時収集してリアルタイムで網全体のトラフィックについての解析を行い、疑わしい現象が発見されると分析フェーズへその情報を渡します。監視フェーズは網全体の情報を扱うため、スケーラビリティが特に求められる部分になります。

ルータ等の網構成装置からの情報としては主にフローデータを使用します。フローデータは機種・ベンダによってNetFlow, sFlow, cflowd等さまざまな名称が使われますが、いずれも通信を送受信元IPアドレス、プロトコル種別、プロトコルのポート番号などで仕分けし、その統計情報やルーティング情報等の付加情報を専用のパケット

表 監視用データの種類と特性

監視用データ	取得方法	データ量	データの詳細度
SNMP MIB	機器へのアクセス	小	カウンタのみ
フローデータ	機器から自動送出	中	送受信先・種別等
パケットキャプチャ	ポートミラー・タップ	大	全データのコピー

フォーマットで出力するものです。従来のSNMP MIBによるインタフェースのカウント値の取得と比較すると、通信の集中している通信対象やサービス種別などのトラフィックの分析に有用な情報がより多く得られるため、近年多くのISPやデータセンタ等のサービスプロバイダが取得・分析を行うようになってきています(表)。

トラフィック監視手法としては他に

wireshark, tcpdump等を利用したパケットキャプチャによる解析もあります。これは流れているパケットそのものを解析するためもっとも情報量が多く、詳細な解析が可能です。しかし多大な計算資源と回線容量を必要とするため、ここで行おうとしているような大規模網全体のリアルタイム監視には向いていません。

フローデータによるトラフィック監視

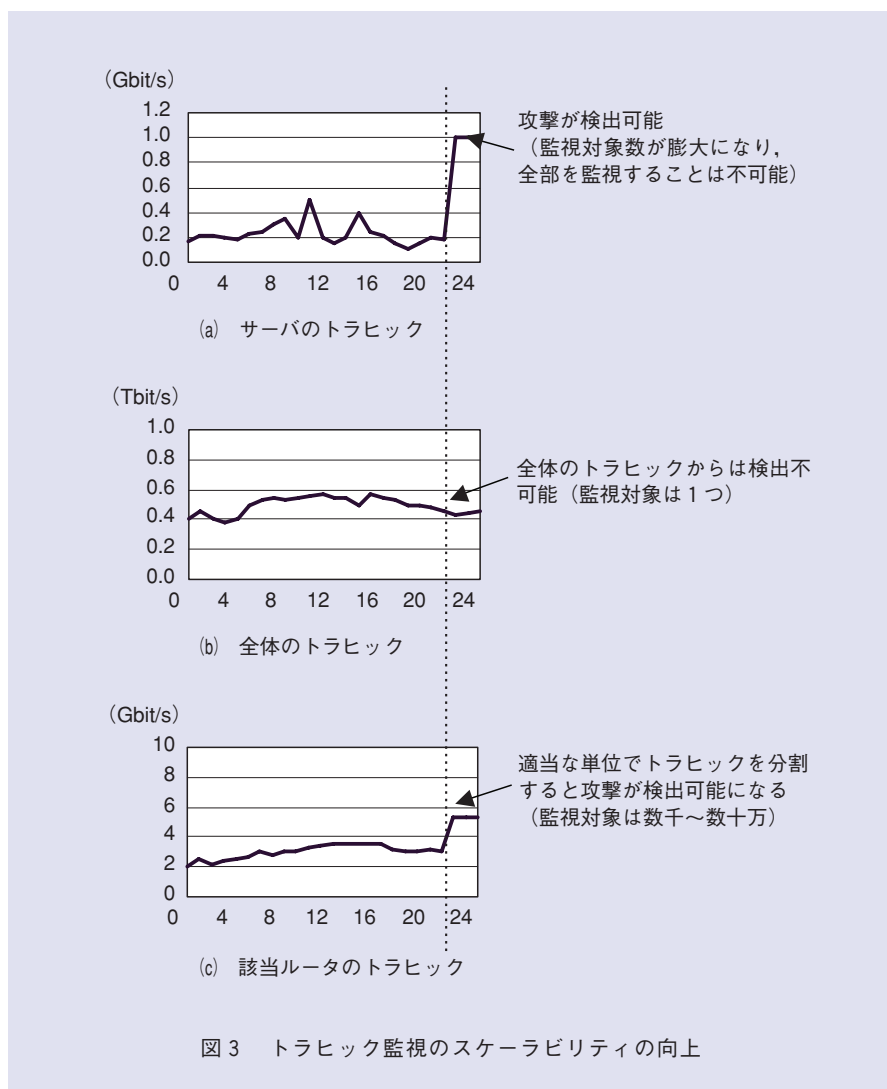
をISPやデータセンタ等で行う場合、ルータへの負荷の低減や扱うデータ量の低減を目的として、フロー生成前に対象パケットのサンプリングを行う場合がほとんどです。本システムは現状のプロバイダと比較するとその数十倍のデータを扱うことになるため、例えば地域拠点ごとなどの単位でフローデータを収集し、それを集約することでさらにスケーラビリティを上げる工夫を導入しています。

こうして収集されたフローデータは広域監視装置で監視されます。フロー全体は非常に大きな数となるため、送受信元の組合せ単位で監視することは困難です。このため従来の監視手法では

- ・ 流量の多いフロー・送信先・送信元のみ注目
- ・ 特定の（サーバ等守るべき対象の）アドレスのみを監視

などの工夫で監視すべき対象を絞り込んでいます。しかしこの2つの手法は監視対象を一部に限ってしまうため、網全体の監視を行いたい場合には使用できません。そこで広域監視装置では通信の送受信元ではなく、通過する通信装置単位や地域拠点単位で集約したマトリクスに個々のフローをマッピングすることで網全体を監視する工夫を導入しています（図3）。また、この手法を導入しても数十万個程度の個別のトラフィック変動を常時監視することになるため、高速に、かつ、しきい値を個々に設定せずに監視できるアルゴリズムを開発しました。

本システムでは、トラブル対処時など部分的にもっと詳細な情報が必要と



なる場合に向けて、例えば特定のサーバ向けのトラフィックのみサンプリングなしでフローデータを取得する機能を持つルータの試作をしています。この機能を選択的sFlowと呼び、現在検証実験を行っています。

■分析

分析フェーズは監視フェーズからの疑わしいトラフィックの情報を契機に実際に何が起きているのかを分析します。

監視フェーズでの異常候補検出は、

例えば1つのDDoS攻撃に対して複数の異常候補が検出される場合があります。分析フェーズはまずいくつかの異常候補が、例えば1つのターゲットに向かう攻撃のようなグループに集約できるかどうかを検討します。その後、各グループに対して元のフローデータを参照して詳細な分析を行い、トラフィックの変動原因、送受信元の特異性、何らかの攻撃によるものなのか、単にアクセスが増えただけで対処の必要のないものなのか、などの判断を行います。

す。一等シンプルな分析手法は異常候補のグループの中でトラヒックの多いフローを調査するものですが、本システムでは異常が検出される前のトラヒックとの差分を比較し、より精度を高める手法を取り入れています。

分析フェーズでなんらかの攻撃、あるいは対処が必要な通信があると認定された場合にはその送受信元とプロトコル、ポート番号などの情報が特定されます。これらの情報が次の制御フェーズで利用されます。

## ■制御

制御フェーズは分析フェーズまでで確定された異常への対処を決定し、実行します。

監視・分析から見つけた異常への対処までの処理を完全に自動化することは技術的には可能ですが、実際のオペレーションでは異常パケットであってもフィルタリングがオペレータの関知しないところで全自動で実行されれば問題となることが想定されるので、現在の実装ではいくつかのオペレーションの候補を表示し、それをオペレータが選択したうえで実行する、という形態にしています。

オペレーションの候補としては、分析フェーズで攻撃と判断されたトラヒックをすべて遮断するフィルタリング、ネットワークまたは攻撃対象の動作に差し支えない程度への流量制限、また網内に分散設置された攻撃軽減装置（よりインテリジェントに攻撃パケットを分別廃棄するアプライアンス）への迂回、の3種類を用意しています。

オペレータにより決定された対処策は、ネットワーク制御装置、またその

下部に配置されたルータ制御装置によって実際にフィルタ・流量制限・迂回処理のルータが特定され、設定変更が行われます。

## 従来技術との差異

DDoSへの対策では、企業向けのアプライアンス製品が存在します。これらは主に既知の攻撃のパターンやシーケンスに関する知識を持ち、通過したトラヒックにこのパターン・シーケンスに合致するかで異常を検知します。この手法は既知の攻撃に対しては非常に検出精度の高い方式です。反面本稿のような大規模網への適用を考えた場合、パケットキャプチャによる分析と同様に攻撃パケットが流れる可能性があるすべての通信路にアプライアンスを挿入しなければならないこと、計算資源を多く消費し、現状の網で要求される10 Gbit/s以上のスループットで監視できる装置の開発が困難なことからスケーラビリティに問題があります。

## 標準化への取り組み

フローデータを利用したネットワークの監視は比較的新しい技術で、先に述べたNetFlow, sFlow, cflowdのようにベンダ個別の技術が個々に標準化されていました。現在IETF（インターネットエンジニアリングタスクフォース）のIPFIX（IP Flow Information eXport）とPSAMP（Packet Sampling）の2つのワーキンググループでフローデータの内容や送り方に関する標準化が進められています。NTT情報流通プラットフォーム研究所からもこの標準化に参加しており、主

に大規模網でのフロー取得・解析に必要な機能の提案を行っています。

## 今後の取り組み

スケーラビリティの現在の到達点はトラヒック総量約1 Tbit/s、監視・制御対象のルータが100台程度です。これは従来技術に比べると大きな数字ですが、最終到達目標まで継続的に検討を続けます。また対応可能な攻撃種別の検証・拡大や、フローデータ以外の情報を利用した検出精度の向上、監視結果をプロビジョニングやトラヒックエンジニアリング等の他分野への適用可能性についても検討を進めていく予定です。



（後列左から）村山 純一/ 小林 淳史  
（前列左から）石橋 圭介/ 西田 晴彦

網全体のセキュリティの向上とオペレーションの現場で使える技術開発を目指しています。

### ◆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 0422-59-4963  
FAX 0422-59-5637  
E-mail nishida.haruhiko@lab.ntt.co.jp