DDoS 攻撃回避を目指した組織間連携方式

森田 真由子　羽生 卓哉　田村 直広　鳥居 悟　小谷野 修
富士通株式会社

１．　はじめに

DDoS攻撃に対する従来の対策では、攻撃の受信を契機とした事後の検出であるための対応の遅れ、単独組織のインターネット接続口で対策を行うためのリソースの限界といった課題が存在している。

これらの課題に対し我々は、事前に導出された予報に基づき、DDoS攻撃のターゲットとなった組織がISPなどの他組織に対策を依頼することによって、より踏み台に近い場所で対策を実施する攻撃回避機構を提案している。[1][2]

本稿では、複数組織に跨る回避の実現に向けた課題と、我々が採用した連携方式について述べる。

２．複数組織間に跨る DDOS 回避機構のねらい

典型的な DDoS 攻撃は、各踏み台からターゲットに大量のパケットを送付することで、大きな被害を及ぼす。これをターゲット付近で遮断しても、有効でない場合がほとんどである。

そこで我々は、各所の踏み台からのパケットがターゲットに集中して莫大な流量のトラフィックになる前に、より踏み台に近い複数の場所で、分散して対策を実施することにより、DDoS 攻撃を回避することをねらいとする。

３．　複数組織に跨る DDoS 回避機構の課題

（１）組織間の信頼関係構築

自サイトの安全性に関わる対策を見知らぬ者に依存するわけにはいかない。また、見知らぬ者からの自サイトのネットワーク運用に関わる依頼を安易に実施するわけにはいかない。

そこで、複数組織が協調して回避策を決定・実施するため、組織間の信頼関係を予め構築しておくことが必要になる。

（２）組織間による要望のすり合わせ

DDoS 攻撃のターゲットなった対策依頼元は、不正なトラフィックは全て遮断し、正規のトラフィックは全て通過させる回避策を最善と考える。一方、対策依頼先である ISP は、サービス提供者として、通信性能が全く低下しない回避策を最善と考える。

そこで、対策依頼元による要望と対策依頼先による要望のギャップのすり合わせが必要になる。

なお、要望のすり合わせに時間がかかると、対策が遅れるため、すり合わせには迅速さも求められる。

（３）被害を最小化する対策実施場所の特定

対策を依頼された ISP の都合により、踏み台の直近で対策を実施できない場合がある。

そこで、実施の可否とその有効性を考慮した、適切な対策実施場所を特定することが必要になる。

（４）状況判断に基づく最適な回避策の決定

複数組織に跨る場合、対策依頼元・対策依頼先それぞれにおいて入手できる情報には制限がある。

また、あらかじめ検知事象と対応付けて定義されていた防御策を機械的に実施すると、不十分な回避、あるいは、正常リクエストの遮断などの弊害の可能性がある。

そこで、回避策の実施時点におけるサービス状況や計算機環境と、実施すべき回避手段とを対応付けることによって、状況に応じた回避策を決定することが必要になる。

４．　実現方式

課題解決のため、我々は以下の方式を採用した。

なお、本機構の実装評価については[3]で述べる。

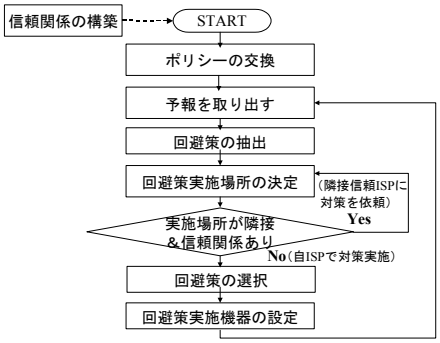

図 1　処理フロー

A Collaborative DDoS Prevention System,
Mayuko Morita, Takuya Habu, Naohiro Tamura, Satoru Torii, Osamu Koyano, FUJITSU Limited

（1） 組織間での信頼関係の構築

オフライン契約によって、信頼関係を構築する。

（2）組織間による要望のすり合わせ

事前のポリシー交換、及び対策依頼側から対策実施側へ、構造化した情報を一度に受け渡すプロトコルを採用する。これによって、要望のすり合わせが迅速に行える。

事前に交換すべきポリシーを以下に示す。

- 連携相手の組織がセキュリティ上信頼できるか判断するためのセキュリティポリシー
- 回避策決定・実施に関するポリシー

（3）被害を最小化する対策実施場所の特定

対策を依頼された ISP が、攻撃元により近い隣接 ISP に順次対策を依頼する。この時、回避策実施に関するポリシーや機器の環境により、踏み台に最も近い場所で対策を実施できない場合でも、踏み台にできるだけ近い対策実施場所を特定できる。

回避策実施場所の決定法、回避策実施機器の設定法を以下に示す。

a)回避策実施場所の決定

対策を依頼された ISP は、予報に含まれる攻撃元情報から、回避策実施場所を決定する。

実施場所が隣接 ISP でかつ信頼関係がある場合、隣接 ISP に対策を依頼する。さもなければ、自 ISP の境界機器で対策を実施する。

b)回避策実施機器の設定

自組織で対策を実施すると判断した場合、運用管理システムと連携することによって、回避策実施機器を決定し、対策を設定する。

（4）状況判断に基づく最適な回避策の決定

回避策の抽出・回避策の選択からなる回避策決定方式は、対策依頼元・対策依頼先の役割分担を最適化する。このことによって、対策依頼元・対策依頼先それぞれにおいて入手できる情報を最大限に利用し、状況に応じた最善の回避策を決定することが可能になる。

最適な役割分担を実現する対策依頼手順と対策依頼形式は、以下のようになる。

a） 対策依頼手順

ISP 接続組織は、予報の内容に基づき回避策の抽出を行い、当該パケットを遮断するよう対策依頼を送付する。次に、ISP は、依頼された対策の中から実施可能でかつ最善であるような回避策の選択を行う。

この仕組みは、ISP に届く通信のうち何を遮断するかは自組織の責任において決定する、との考え方に基づいている。

b)対策依頼形式

攻撃元サイト・対策対象などの詳細な情報が複数含まれることを考慮し、XML 形式を採用する。

５． システム概要

以下にシステムの概要を示す。

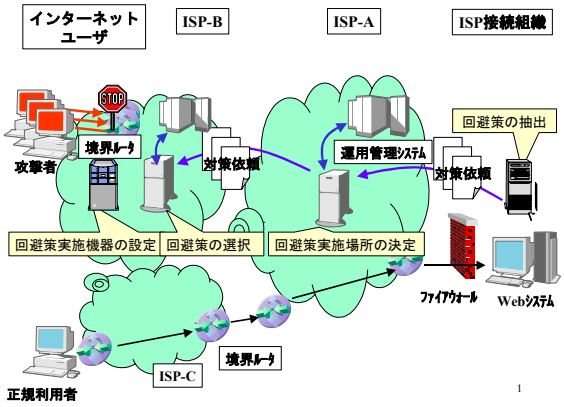

図 2 システム概要

６． まとめ

本稿では、複数組織に跨る攻撃回避機構の４つの課題とその実現方式について述べた。

今後は、複数 ISP を考慮した環境における実証実験と、本技術の有効性評価を行い、アルゴリズム及びプロトコルの改善を行っていく予定である。

謝辞

本研究は、通信・放送機構の委託研究テーマ「サービス不能化(DDoS)攻撃に対する防御技術に関する研究開発」の一環として行なわれているものである。

参考文献

[1] 三友 他, *“攻撃モデルを用いた DDoS 攻撃の予兆検知方式”*, 情報処理学会 第 65 回全国大会, Mar. 2003

[2] 鳥居 他, *“不正アクセス予知回避機構の提案”*, 情報処理学会 第 62 回全国大会, Mar. 2001

[3] 羽生 他, *“DDoS 攻撃回避機構の試作”*, 情報処理学会 第 65 回全国大会, Mar. 2003