社団法人 情報処理学会　研究報告
IPSJ SIG Technical Report

2004－ＤＰＳ－117　(24)
2004－CSEC－　24　(24)
2004／3／5

DDoS 攻撃回避システムの開発

田村 直広、森田 真由子、羽生 卓哉、鳥居 悟、小谷野 修

富士通株式会社

ＤＤｏＳ攻撃の被害から、攻撃対象となったサイトのサーバだけでなく、インターネットのネットワーク基盤を守るためには、攻撃が開始される前に、ネットワーク上に分散している各ＤＤｏＳ攻撃エージェントの直近のネットワーク装置で対策を実施することが有効である。本稿では、ＤＤｏＳ攻撃予測システムからＩＳＰ接続組織へ通知されるＤＤｏＳ攻撃予報に基づいて、ＤＤｏＳ攻撃への対策を実施することにより、ＤＤｏＳ攻撃を回避するシステムを提案する。また、本システムを実装し、擬似インターネット環境で、その性能を評価した結果について報告する。

Development of DDoS attack prevention system

Naohiro Tamura,　Mayuko Morita, Takuya Habu,
Satoru Torii,　Osamu Koyano
Fujitsu Limited

It is effective to take measures at the network devices as close to DDoS agents as possible before attack starts, in order to protect not only target servers but also infrastructure of the Internet. In this paper, we propose a system which blocks DDoS attacks at the closest network devices to DDoS agents following forecasts issued by DDoS forecast system. And we present the results of applying our prototype to a pusedo Internet in our laboratory. The paper concludes by discussing the potential and limitation of this approach.

1. はじめに

DDoS（Distributed Denial of Service：分散型サービス不能化）攻撃とは、インターネット上で攻撃者がソフトウエアの脆弱性を利用し乗っ取った複数のホスト（DDoS 攻撃エージェント）から、一斉に大量のパケットを一つのターゲットに向けて送信し、ターゲットの提供しているサービスを不能化したり、通信経路上のネットワーク基盤を不能化する攻撃である[1]。典型的なＤＤｏＳ攻撃は、インターネット上で入手可能な TFN2K[2]等の攻撃ツールを使用し、数百台規模のホストから攻撃が成されると考えられている。最近の例では、2003 年 5 月に SCO 社の Web サイトが、138 台のホストから DDoS 攻撃されたと報告されている[3]。

このような状況において、インターネット上に分散した多数の DDoS 攻撃エージェントからターゲットを防御し、且つネットワーク基盤を正常に維持するための、自動防御システムが求められている。

我々は今までに、インターネット上に分散する各 DDoS 攻撃エージェントの直近に位置するネットワーク接続装置で DDoS 攻撃に対処する回避システムを提案し、単独 ISP 環境におけるシステムの性能と有効性について評価報告した[4][5]。

本稿では、インターネットを想定した複数 ISP 環境で動作させるために設計を見直した DDoS 攻撃回避システムについて説明し、擬似インターネット環境で、システムの性能と有効性について評価した結果を報告する。

以下、まず、2 章にて従来の DDoS 防御技術と課題を整理する。次に、3 章にて我々の提案する DDoS 攻撃回避システムの狙いと特徴を示し、4 章にて DDoS 攻撃回避システムの構成と機能について説明する。5 章にて擬似インターネット環境における性能基礎実験方法を示し、6 章にて実験結果を評価する。最後に、7 章にてまとめを述べる。

2. 従来の防御技術と課題

従来の防御技術としては、ターゲットで攻撃パケットをブロックする技術が最も一般的に利用されている[6]。最近の研究としては、ターゲットの属する ISP が隣接 ISP との境界でターゲットへのパケットをブロックする技術が一部実用化段階にある[7][8][9]。これらの技術･研究は、ISP 利用者あるいは ISP が自らのシステムを DDoS 攻撃から単独で防御する考え方である。

しかしながら、インターネットのさらなる発展にともない、DDoS 攻撃の規模は拡大すると予想され、単独組織による防御だけでは防御不能となる可能性が高くなる。大規模(多数の攻撃エージェント)、高トラフック負荷の DDoS 攻撃から、インターネットインフラ、インターネットコミュニティを広範囲に守る防御システムが求められている。

3. DDoS 攻撃回避システム

我々の DDoS 攻撃回避システムは、インターネットの構成員である ISP、ISP 利用者が協調することにより、大規模･高負荷の DDoS 攻撃にも耐えられる防御効果の高い回避システムである。

複数の組織が協調して攻撃回避を行う上で考慮すべき事項として以下の2点がある。

- 攻撃回避の発動者･タイミング
- 攻撃回避実施者･回避場所

上記考慮事項に関して、我々の攻撃回避システムでは以下のとおりとした。

- ターゲットの組織が ISP に対して攻撃対策依頼を行うことで、回避システムを始動させる。
- 複数の ISP が協調、分担することで、攻撃エージェントの直近で対策する。

この考え方に基づき構築した DDoS 攻撃回避システムの全体処理フローを図 1に示す。

攻撃回避システムへの入力は、1)DDoS 攻撃のパケットの特徴、2) DDoS 攻撃の発生する時間、3) DDoS 攻撃の発生する確率、4)DDoS 攻撃の発信元、5) DDoS 攻撃の宛先、といった情報であり、DDoS 攻撃予測システムから予報として DDoS 攻撃のターゲットに通知される[10][11][12]。

その後、1) ターゲットが対策依頼判断、2) ターゲットが自分の属する ISP へ対策依頼、3) ターゲットの属する ISP が DDoS 攻撃エージェントの属する ISP へ依頼転送、4) DDoS 攻撃エージェントの属する ISP が対策実施、という4段階で実行される。

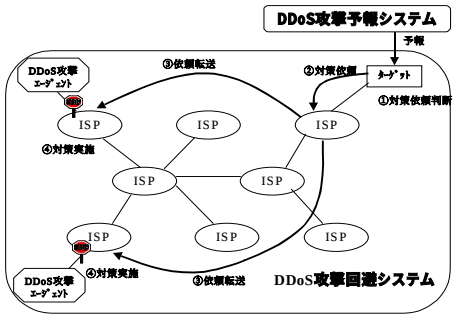

図 1 DDoS 攻撃回避システム処理フロー

ターゲットは、予報に含まれる DDoS 攻撃の発生する時間、DDoS 攻撃の発生する確率、DDoS 攻撃の宛先を元に対策依頼を行うかどうか自組織の判断基準に照らし合わせ判断する。

その結果、対策依頼が必要であると判断したら、ターゲットは遮断等の対策の対象とするパケットを決定し、ISP に対策を依頼する。

ターゲットの属する ISP は、ターゲットから予報に含まれていた DDoS 攻撃の発信元アドレスをキーに、DDoS 攻撃エージェントの属する ISP を判別し、依頼を転送する。

DDoS 攻撃エージェントの属する ISP は、更に DDoS 攻撃の発信元アドレスをキーに DDoS 攻撃エージェントの直近のネットワーク接続装置を判別し、そこで依頼内容に従ってターゲット宛てのパケットを遮断する。

この処理フローにより、大規模･高負荷の DDoS 攻撃にも耐えられる防御効果の高い DDoS 攻撃回避システムが実現できる。

4. 攻撃回避システムの機能構成

ここでは、前章で示した攻撃回避システムの性能目標と、システムを実現するための機能構成について述べる。

4.1. 性能目標

我々は、攻撃予測システムから攻撃回避システムが予報を受信して30秒以内に対策設定が完了する（1,000 台の DDoS 攻撃エージェントがインターネット環境に分散配置されている攻撃規模）という性能目標をたて攻撃回避システムを設計した。

2001 年 8 月に発表された論文[13]によるとインターネット上で観察された DDoS 攻撃のパケット総流量の最大は約 600Kpps と報告されている。また、我々が TFN2K[2] の 1 PC（CPU Pentium Ⅲ 1GHz）当たりのパケット送出量を計測したところ約 6Kpps であったことから、600Kpps の攻撃規模は

TFN2K で換算すると 100 台 に相当する。ここで更に、2001 年 8 月からの時間の経過を考慮し、目標の DDoS 攻撃エージェント数をその 10 倍の 1,000 台とした。

また、攻撃者は DDoS 攻撃ツールを使用して DDoS 攻撃開始までに複数の司令コマンドで DDoS 攻撃エージェントを操作する必要があることから、少なくとも数分必要であると推測した。そして DDoS 攻撃予測システムでの処理時間も考慮し 1,000 台の DDoS 攻撃エージェントへの対策完了まで 30 秒とした。

4.2. 機能構成と配置

3章で示した処理フローを実現するために、DDoS 回避システムの機能を3つの役割（対策依頼, 処理判断, 対策実施）に分け、それぞれを1つのコンポーネントとし、図 2に示すように配置する。

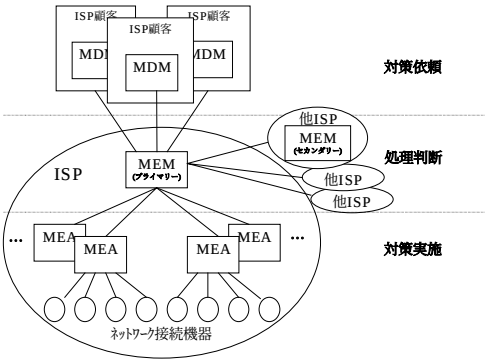

図 2 攻撃回避システムコンポーネント配置構成

第 1 のコンポーネントは ISP 顧客に付き 1 つ配置される MDM（Measure Decision Manager：回避策決定マネージャ）で、受信した予報に基づいた対策依頼判断と対策依頼の役割を持つ。

第 2 のコンポーネントは、ISP に付き 1 つ配置される MEM（Measure Execution Manager：回避策実施マネージャ）で、対策実施場所決定等の処理判断の中心的な役割を持つ。便宜上、対策依頼を転送する MEM をプライマリーMEM、対策依頼を転送された MEM をセカンダリーMEM と呼ぶ。

第 3 のコンポーネントは、ISP 内に複数存在し、各ネットワーク機器の管理単位に1つ配置される MEA（Measure Execution Agent：回避策実施エージェント）で、対策実施の役割を持つ。

図 3に各コンポーネントの機能構成を示す。

各コンポーネントを構成する機能単位は、処理性能を考慮し、コンポーネント間通信も含めて、できる限り独立した処理として並列に実装できるように機能設計した。

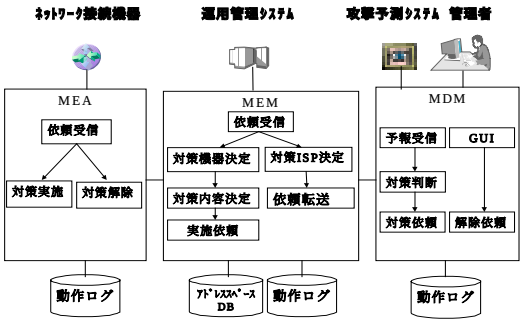

図 3 攻撃回避システム機能構成

4.2.1 MDM

予報受信機能は、DDoS 攻撃予測システムから予報を受信し、次に、対策判断機能は、予報に含まれる DDoS 攻撃の宛先、DDoS 攻撃の発生する確率と時間を元に対策依頼を行うか判断する。

4.2.2 MEM

依頼受信機能は、MDM 及びプライマリ MEM から依頼を受信し、それを分別する。

MDM からの対策依頼の場合、対策 ISP 決定機能は、アドレススペース DB を検索し、DDoS 攻撃エージェントのいる ISP を決定し、依頼転送機能がそのセカンダリーMEMへ依頼を転送する。この時、複数のセカンダリーMEM への依頼転送は並列処理される。

一方、プライマリ MEM からの対策依頼の場合、対策機器決定機能は、運用管理システム（例えば [14]）を参照し、対策実施機器を決定する。次に、対策内容決定機能が、対策実施機器のサポートしている機能（パケットフィルタリング、流量制御、経路制御等）より対策実施内容を決定する。そして、実施依頼機能が、対策実施機器を管理する MEA へ対策実施を依頼する。この時、複数の MEA への対策実施依頼は並列処理される。

4.2.3 MEA

依頼受信機能は、対策実施依頼と対策解除依頼を受け、それを分別する。そして、対策実施機能がネットワーク接続機器へ DDoS 対策を設定し、対策解除機能がネットワーク接続機器から DDoS 対策を解除する。この時、複数のネットワーク接続機器への設定は並列処理される。

5. 基本性能評価実験

ここでは、回避システムを複数 ISP 環境で性能評価するための、評価項目、擬似インターネット環

境、実験概要について述べる。

5.1. 評価項目

4.1章に示した設計時性能目標を基準に複数ISP 環境における有効性を評価するために、以下2つの観点で性能評価する。

1) 単独ISP における性能評価

ISP の都合により、ISP 内に配置できる MEA 数と、1つの MEA に管理させるネットワーク接続機器数は、変わってくると考えられる。まずここで、MEA の配置数と MEA が管理するルータ数が DDoS 攻撃回避システムの性能にどのように影響するか評価し、最も性能のよい MEA 配置形態と最も性能の悪い MEA 配置形態を求める。

2) 複数 ISP における性能評価

DDoS 攻撃の規模(DDoS 攻撃エージェント数)が大きくなるに従って DDoS 攻撃回避システムの性能が劣化すると考えられる。そこで、最も性能のよかった MEA 配置形態と最も悪かった MEA 配置形態で、DDoS 攻撃エージェント数が対策実施性能にどのような影響を及ぼすか評価する。

5.2. 擬似インターネット環境

擬似インターネット環境を構築するにあたり、ISP へヒアリング調査した結果、国内大手 ISP は境界ルータ(他 ISP との境界及び顧客との境界)を 1,000 台程度持つことが判明した。

そこで、我々は主要大手 ISP が100社でインターネットの大部分がカバーされると考え、擬似インターネット環境を境界ルータ 1,000 台持つ主要 ISP が 100 社で構成されたネットワークと定義した。

実験環境は、実際に ISP で使用されている機器と近い性能のルータ8台、Layer2 スイッチ10台を用い Fast Etherent でネットワークを構築し、各コンポーネントと、MEM シミュレータ、MEA シミュレータ、ルータシミュレータを計21台の PC 上で動作させ攻撃回避システムを構築した。

各シミュレータは、処理依頼を受けると、各コンポーネントの必要する処理時間分の遅延(実測により求めた)を再現し、応答する仕組みである。

図 4は、境界ルータ 1,000 台持つ1ISP を、MEA50台(実機1台と MEA シミュレータ49)が、それぞれルータ20台(実機 1 台とルータシミュレータ19)づつを管理する形態で実現し、その ISP が 100 ある環境を MEM 実機2台と MEM シミュレータ98の計 100 で実現している様子を示している。また、1ISP あたり 500 台の DDoS 攻撃エージェント(Attacker)が仕込まれて、100ISP 全体で 50,000 台の DDoS 攻撃エージェントが均等に分散している様子を示している。

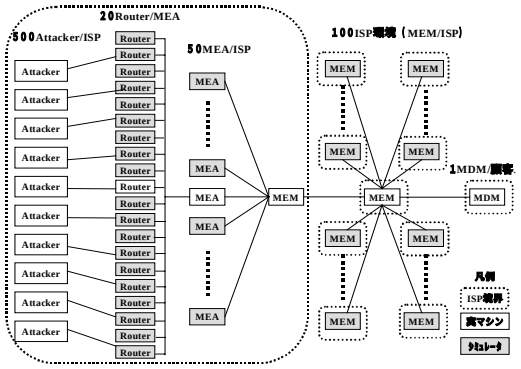

図 4 擬似インターネット環境

5.3. 実験概要

評価項目の実験概要を以下に示す。

全ての実験は、定常トラフィックがなく、各 MEM が ISP のアドレススペース情報をアドレススペース DB に格納し、各マシンクロックが同期した状態の、擬似インターネット環境で行った。

性能計測は、MDM が予報を受信して、MEA が DDoS 攻撃エージェントのいる直近ルータ全てに 1 行の ACL (Access Control List) を設定するまでの所要時間と、MDM、MEM、MEA の処理時間を、各コンポーネントの動作ログから、ミリ秒単位で求めた。

1) 単独ISP における性能評価

2ISP で、一方にプライマリーMEM、他方にセカンダリーMEM を配置する。そして、プライマリーMEM のいる ISP のターゲットに MDM を、セカンダリーMEM のいる ISP に境界ルータ 1,000 台と、DDoS 攻撃エージェント 1,000 台(1ルータに1台)を配置する。

この状態で、セカンダリーMEM のいる ISP の MEA と境界ルータの組み合わせを6通り(10 対 100、20 対 50、25 対 40、40 対 25、50 対 20、100 対 10)に変化させ性能計測した。

2) 複数 ISP における性能評価

100ISP で、1つにプライマリーMEM、他99にセカンダリーMEM を配置する。プライマリーMEM のいる ISP のターゲットに MDM を、全ての ISP に境界ルータを 1,000 台を配置する。

この状態で、単独 ISP における評価で求めた最も性能のよかった MEA 配置形態と最も悪かった配置形態の2通りについて、100ISP 全体に、均等に配置した DDoS 攻撃エージェント数を8通り(10、100、1,000、5,000、10,000、15,000、50,000、100,000 台)に変化させ、性能計測した。

6　結果と評価

ここでは、コンポーネント配置形態と攻撃エージェント数が性能に及ぼす影響と、複数 ISP 環境における有効性の評価について述べる。

6.1.　単独 ISP における性能評価

1) コンポーネント配置形態が対策設定所要時間に及ぼす影響を図 5に示す。

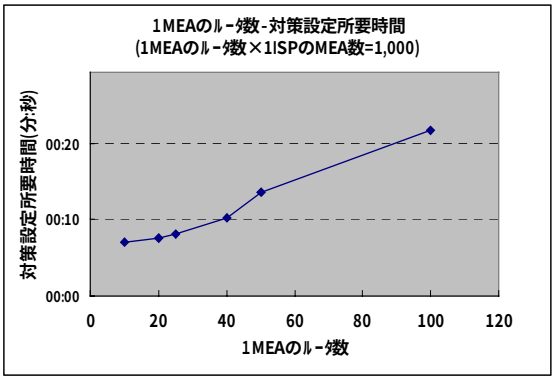

図 5 コンポーネント配置形態別性能

この結果より、対策設定所要時間は1つの MEA が管理するルータ数の増加によってほぼ線形に増加していくことがわかる。

MEA 数が 10 で1つの MEA が 100 のルータを管理している時、性能は最も悪く、MEM 数が 100 で1つの MEA が 10 のルータを管理している時、性能は最もよい。

2) コンポーネント配置形態毎の各コンポーネント処理時間内訳を図 6に示す。

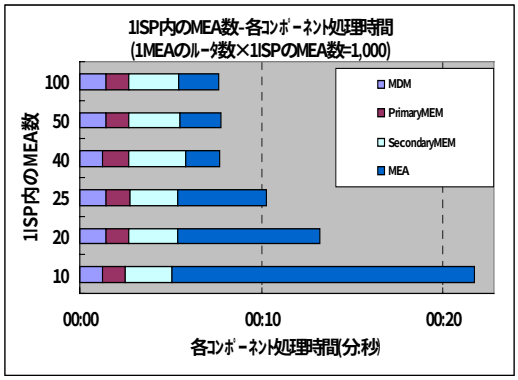

図 6 配置形態別処理時間内訳

この結果より、セカンダリーMEM の処理時間は MEM に接続する MEA 数にかかわらずほぼ一定で、MEM の処理時間は MEA 数にほとんど影響を受けないことがわかる。一方、MEA の処理時間は、MEA が管理するルータ数が多くなるほど長くなり、ルータ数 100 (MEM 数 10) の時、MEA の処理時間は全体の 77%を占めるに至っている。つまり、MEA の管理するルータ数が DDoS 攻撃回避システム全体の性能大きな影響を与えている。

MEM は接続する MEA 数が増えても性能が劣化せず、MEA は接続するルータ数が増えると性能が劣化している原因として、MEM と MEA の1対多通信はスレッドとして実装されており、MEA とルータの1対多通信は MEA がルータの数だけプロセスを起動する実装になっていることがありうる。従って、MEM とルータ間の通信をスレッドとして実装すれば、DDoS 攻撃回避システム全体の処理性能は、MEA が多数のルータを管理しても著しく劣化しないように改善することが可能と考えられる。

6.2.　複数 ISP における性能評価

1) 対策設定する DDoS 攻撃エージェントの数が性能に及ぼす影響を図 7に示す。

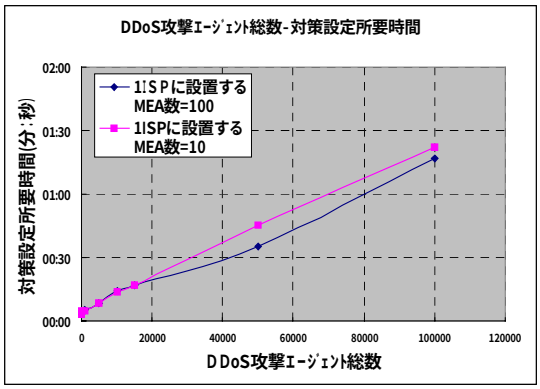

図 7 DDoS 攻撃エージェント数別性能

この結果より、DDoS 攻撃エージェント数が増えるに従って、対策設定所要時間も線形に増加することがわかる。その要因として DDoS 攻撃エージェント数が増えるに従って予報に含まれる攻撃元に関するデータ量が増え処理時間が増加していくためと推測される。

また、DDoS 攻撃エージェント数が 100,000 (1 ISP あたり 1,000) では、6.1章の評価条件と同じになるため、MEA 数10と100の配置形態間の性能差は、MEA の管理するルータ数の差によると考えられる。一方、DDoS 攻撃エージェント数が 15,000 (1ISP あたり 150) 以下で、MEA の配置形態間で、性能に差が出ないのは、MEA が対策設定のために処理するルータ数が非常に少なくなるためと考えられる。例えば、DDoS 攻撃エージェント数が 10,000 (1ISP あたり 100) の時、MEA 数 10 では1つの MEA が管理する 100 台のルータの内 10 台

に、MEA 数 100 は 10 台の内1台に対策設定するのみであるためである。

2) DDoS 攻撃エージェント数 (両配置形態で全ての MEA が稼動開始する 10,000 以上) 毎の各コンポーネント処理時間内訳を図 8に示す。

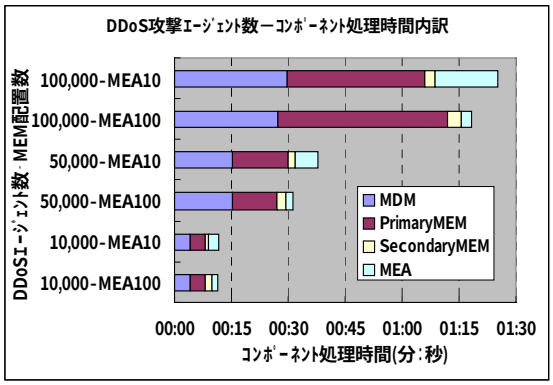

図 8 DDoS 攻撃エージェント数別処理時間内訳

この結果より、MDM と MEM の各処理時間は、配置形態が MEA 数10と 100 でほぼ同じで、DDoS 攻撃エージェント数が増加するにつれてコンポーネント内処理時間が線形に増加していることがわかる。このことから、MDM と MEM の処理時間は DDoS 攻撃エージェントに関するデータ量の増加によって増えることが確認できる。

一方、MEA の処理時間は、MEA 数10と 100 を比較すると、MEA 数 100 の方が 10 に比べて短く、MEA の処理時間は実際に処理するルータ数が増えるに従ってが増えることが確認できる。

6.3. 有効性評価

2つの評価観点を通して、擬似インターネット環境において、最も性能のよい配置形態である MEA 数 100 の時、30 秒で約 44,000 攻撃元、最も性能の悪い配置形態である MEA 数10の時、30 秒で約 30,000 攻撃元を処理できることがわかった。

つまり、本攻撃回避システムは、ISP の都合により最も性能の悪い配置形態を採らざるをいない場合であっても、少なくとも設計性能目標の30倍規模の DDoS 攻撃を回避できることを示している。

ゆえに、本 DDoS 攻撃回避システムは典型的な DDoS 攻撃ツールによる攻撃規模を回避するために求められる性能を有し、基本性能に関してインターネット規模の複数 ISP 環境で有効に機能することが確認できたといえる。

7. まとめ

本稿では、「DDoS 攻撃予測システム」の予報に基づき、複数の ISP が連携し DDoS 攻撃元にできる限り近いネットワーク接続装置で対策を実施する「DDoS 攻撃回避システム」を提案し、その試作・評価結果について報告した。今後は、多数の対策設定や対策解除の依頼が連続した高負荷状態等の性能検証と有効性評価を行い、完成度を高めていく予定である。

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」の一環として行われているものである。

参考文献

[1] CERT Coordination Center, "Trends in Denial of Service Attack Technology," October 2001, http://www.cert.org/archive/pdf/DoS_trends.pdf

[2] http://packetstormsecurity.com/distributed/TFN2k_Analysis-1.3.txt

[3] http://zdnet.com.com/2100-1105_2-999584.html

[4] 森田 他, *"DDoS 攻撃回避を目指した組織間連携方式"*, 情報処理学会 第 65 回全国大会, Mar. 2003

[5] 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

[6] Adrian Brindley, "Denial of Service attacks and the emergence of Intrusion Prevention Systems", November 2002, http://www.sans.org/rr/firewall/prevention.php

[7] http://www.arbornetworks.com/

[8] http://www.netzentry.com/

[9] http://www.ntt.co.jp/news/news03/0302/030218.html

[10] 三友 他, *"DDoS 攻撃予測システム"*, 情報処理学会 CSS2003, Oct. 2003

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

[12] 久保田 他, *"不正アクセスシナリオの導出に向けた検知ログ解析"*, 情報処理学会 第 64 回全国大会, Mar. 2002

[13] David Moore, Geoffrey Voelker, and Stefan Savage, "Inferring Internet Denial-of-Service Activity", Proceedings of the 10th USENIX Security Symposium, Aug. 2001

[14] http://systemwalker.fujitsu.com/jp/