DDoS 攻撃回避機構の試作

羽生 卓哉，森田 真由子，田村 直広，鳥居　悟，小谷野 修
富士通株式会社

１．　はじめに

サービス不能化（DDoS）攻撃に対してこれまで提案されている対策の多くは，攻撃に荷担しないためのものであった．DDoS 攻撃から自組織を防御する有効な対策は確立されていない．

我々は，DDoS 攻撃による実害発生を未然に防ぐことを目指した研究開発を行い，事前の攻撃予報に基づき，複数の組織が協力して攻撃回避を行うことを特長とする回避機構を設計した．本論文では，攻撃回避機構の仕組み，及び動作実験をした結果得られた知見について述べる．

２．　回避機構プロトタイプの処理フロー

我々が試作した DDoS 攻撃回避機構[1]のプロトタイプは，以下の 3 つのコンポーネントから構成される（図 1）．

回避策決定マネージャ(MDM)：DDoS 攻撃のターゲットとなりうる組織に配置され，以下のように遮断対象パケットを決定する．

(1)DDoS 攻撃予知機構[2]から，自組織への DDoS 攻撃の予報を受信する．(2)予報の内容に基づき，自組織に送付されるパケットのうち遮断すべきものを，プロトコル／送信元・先の IP アドレス／ポートを基準に決定する．(3)当該パケットを遮断するよう，自組織の接続 ISP(MEM)に対策依頼を送信する．

回避策実施マネージャ(MEM)：ターゲットの組織に接続する ISP に配置される．ネットワーク構成を知り得る ISP の役割として，以下のように回避策実施機器を決定する．

(1)MDM からの依頼を受信する．(2)遮断するパケットの送信元 IP アドレス等の情報から自 ISP で回避策を実施するのが適切と判断したら，予め登録された運用管理情報を元に ISP 内でその送信元に最も近接するルータを決定する．(3)送信元 IP アドレスごとに決定したルータで回避策を実施するよう，MEA に対策命令を送信する．

回避策実施エージェント(MEA)：MEM と同じ ISP に配置される．MEM から対策命令を受信し，それに従って並行的に各ルータと通信し，アクセスコントロールリスト(ACL)を設定し，DDoS 攻撃パケットを遮断する．遮断する送信元 IP アドレス（エージェント）1 つあたり ACL1 行となる．

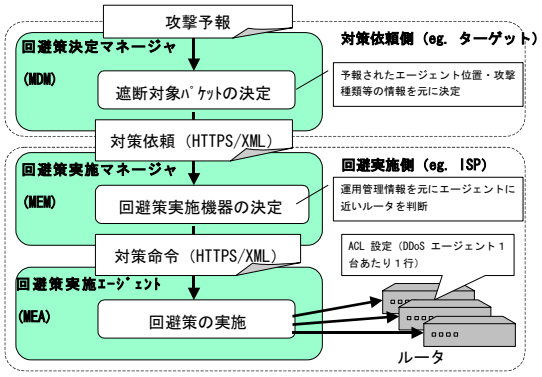

図 1　DDoS 攻撃回避機構の処理フロー

本機構は，自組織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設計されている．また，コンポーネント間の通信方式には，複数組織間で行われること，対策に関する詳細な情報をやりとりすること，暗号化・認証の必要性，実装の容易さを考慮し，HTTPS/XML を採用している．

本機構を用いると，ISP 内で DDoS エージェントに最も近いルータでパケットが遮断される．これにより従来より効果的に DDoS 攻撃を回避することが期待される．

３．　動作実験

ISP を模した実験環境において，実際に本機構が従来のものより優れていることを確認すること，性能測定を行うことを目的とし，本機構の動作実験を行った．

実験環境（図 2）は実際の ISP 環境を考慮し，多数の端点でユーザ組織と接続すること，ISP ネットワーク内では複数の経路が用意されていること，といった特徴を備えたものとした．ルーティングプロトコルには RIP を使用している．

ある ISP に接続している複数の組織の機器が踏み台となり，その ISP に接続する別の組織に一

Prototyping of the DDoS Prevention System,
Takuya Habu, Mayuko Morita, Naohiro Tamura, Satoru Torii, Osamu Koyano,
FUJITSU Limited

斉に DDoS 攻撃を行おうとしている中，ターゲットの組織へ攻撃が予報された状況を想定する．

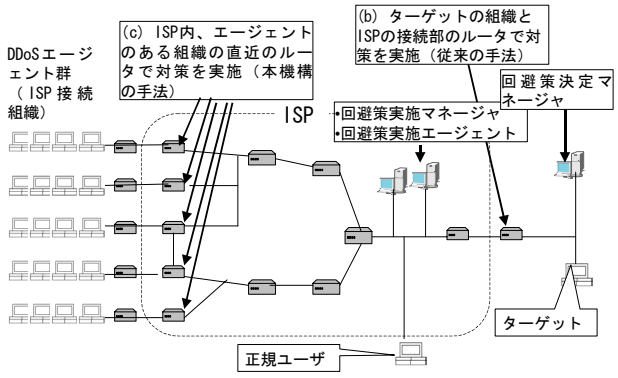

図 2　DDoS 回避機構実験図

３．１ 従来手法との有効性の比較

本機構における攻撃回避の手法が従来の手法より有効であることを実験を通して確認する．

図 2 の環境で(a)対策せず(b)従来の手法(c)本機構の手法，を実施し，DDoS 攻撃による被害の程度を見る．ただし従来の手法とは，ターゲットの組織と ISP の接続部のルータでパケット遮断の設定を行うことである．その上で DDoS エージェントの台数を変えて UDP Flood 攻撃を行い，正規ユーザを想定したマシンのブラウザからターゲットサイトの Web サーバに 10 回ずつアクセスを試み，接続成否及び応答時間を測定した．

３．２ 処理時間の測定

(1) 本機構は事前の攻撃予報に基づいて対策を行うことを前提とするが，回避策実施が攻撃発生前に完了するよう早期の予報出力が求められる．一方，攻撃発生の直前に予報を発行する方が予知の精度は高いと考えられる．そこで回避機構の処理時間を測定し，期待される予報出力時期を導出する．

(2) 回避機構の全体処理時間を短縮することは，より遅い時期に出された予報を活用することに繋がり大いに有効である．そこでコンポーネント別の処理時間を測定し，性能ボトルネックを見極め，今後の改良に役立てる．

(1)(2)のねらいから，回避策実施ルータの数及び設定する ACL の行数を変化させ，攻撃予報の受信から一連の対策実施が完了するまでの本機構の処理時間をコンポーネント別に測定した．

４．　実験結果及び考察

４．１ 従来手法との有効性の比較

表 1 の網掛け部の通り，従来の手法(a)(b)ではエージェントが 5 台以上の場合に遅延や接続失敗が発生する場合があった．一方，方法(c)では，常に平常時と同じ応答時間を確保することができ，本機構の有効性が基本的に確認できた．

なお(a)(b)では，エージェントが 15 台以上の場合に，ISP 内のルータが RIP 情報の交換に失敗し経路情報を失う現象がみられた．

表1 手法／エージェント数別・正規ユーザWebアクセス結果(回)

手法	(a)対策せず					(b)従来の手法					(c)本機構の手法				
エージェント数	1	5	10	15	20	1	5	10	15	20	1	5	10	15	20
問題なし	10	5	6	4	3	10	7	8	7	2	10	10	10	10	10
遅延1秒以上	0	0	3	0	2	0	0	1	0	0	0	0	0	0	0
遅延10秒以上	0	5	1	6	1	0	3	1	0	0	0	0	0	0	0
ｻｰﾊﾞ接続失敗	0	0	0	0	4	0	0	0	3	8	0	0	0	0	0

４．２ 処理時間の測定

(1) 平均処理時間の測定結果は表 2 の通り．

表 2 DDoS 回避機構の平均処理時間（秒）

ルータ数	1	2	3	4	5
ACL1行/1ルータ	4.6	7.7	11.2	14.3	17.9
2行	6.0	10.5	15.0	20.0	24.8
3行	7.4	13.1	19.3	25.4	31.8
4行	8.8	15.9	23.5	31.2	38.8

これより，ルータ R 台に各 A 行の ACL を設定する場合，処理時間 T は以下の式で近似できる．R×A は DDoS エージェントの総数と一致する．

$T(sec) = 1.4RA + 1.9R + 1.15$

本機構では攻撃発生の T 秒以上前に予報を受信することが期待される．

(2) コンポーネント別の処理時間は次の通り．

表 3 コンポーネント別処理時間(R=5,A=4)（秒）

コンポ名	全体	MDM	MEM	MEA
処理時間	38.8	<0.1	0.6	38.2

これより，性能のボトルネックは MEA にあることがわかる．1 つの MEM に対し MEA を複数，分散的に配置すれば全体処理時間が短縮され，性能改善に有効であると考えられる．

５．　まとめ

DDoS 攻撃回避機構を試作，動作確認した結果，従来に比べた有効性が確認された．また処理時間の近似式を導き，性能ボトルネックが MEA にあることを示した．今後，MEA の分散配置による性能改善など，本機構の改良を行う予定である．

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] 羽生 他，*“DDoS 攻撃回避機構の実現に向けて”*，情報処理学会 第 64 回全国大会，Mar. 2002

[2] 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