DDoS攻撃回避機構の実現に向けて

2H－01

羽生 卓哉，佐々木 和孝，小谷 誠剛，小谷野 修
富士通株式会社

1．はじめに

サービス不能化（DDoS）攻撃に代表されるインターネット上の不正アクセス攻撃の手法は高度化している．攻撃の受信を契機として自組織のインターネット接続口で対策を行う従来の手法では，攻撃を防ぐことが極めて困難な状況となっている．特にDDoS攻撃に対しては，これまで提案されている対策はいずれもDDoS攻撃に荷担しないためのものであり，自組織を防御する有効な対策は存在していない．

我々は，このような攻撃による実害発生を未然に防ぐことを目指し，研究開発を行っている．今回我々が提案する機構は，複数の組織が協力して事前の攻撃検知および攻撃回避を行うことを特徴とするものである．本論文では，この攻撃回避機構に限定し，そのメカニズムの基本となるモデルに関して述べる．

2．DDoS攻撃

近年の傾向としては，DDoS攻撃手順の自動化が進み，またワーム等を用いた侵入・感染手法がDDoS攻撃として認識されている[2]．今回我々が研究対象としているDDoS攻撃の代表的な手順は以下の通りである．

(1) 多数のコンピュータに侵入して踏み台とし，攻撃用ソフトウェアをインストールする(deployment)．

(2) 踏み台に攻撃指令を出す(use)．

(3) 各踏み台から攻撃対象に大量のパケットを送付する(impact)．

3．従来の防御技術の課題

このようなDDoS攻撃による実害発生を未然に防ぐための技術を確立する上での課題は，以下の二つに集約できる．

課題(1) 事後の検出であるための対応の遅れ：従来は，ターゲットとなる自組織内のみを監視し，DDoS攻撃を受信したimpactの段階で攻撃を検出していた．このため，それを契機に対策を実施しようとしても手遅れとなる可能性が高い[1]．広範囲な監視により，被害に遭う前にその攻撃の予兆の検知が必要である．

課題(2) 単独組織の持つリソースの限界：従来は，ルータでの遮断等，自組織内のみで対策を行っていた．単独組織の持つ計算機資源（帯域，システムの処理能力，記憶容量等）は有限であり，このため，その限界を上回る規模のDDoS攻撃には耐えることができない．複数の組織に跨る対策機構が必要である．

4．攻撃予知機構

課題(1)を解決するためには，deploymentやuseの段階で攻撃を予知する必要がある．そのため，一連のDDoS攻撃の手順を表す攻撃モデルに基づき，攻撃の予兆となる事前の事象を抽出することによりDDoS攻撃を予報することが有効と考えられる．

また，一般にDDoS攻撃の踏み台はターゲットと異なる複数の組織のネットワークに位置するため，他の組織まで含めた広範な監視を行うことが必須となる．

詳細については，ここでは割愛する．

5．攻撃回避機構

5．1 ねらい

課題(2)を解決するためには，他の組織と連携し，より多くのリソースをもって攻撃を防ぐ体制を作る必要がある．各所の踏み台からのパケットがターゲットに集中する前に，より手前の複数の場所で対策を行うことが有効と考えられる．

例えばISPに接続されている企業へのDDoS攻撃を防ぐには，自組織のインターネット接続口で遮断するよりも，より帯域の広いISPの基幹ネットワーク上で

Consideration for Implementation of DDoS Prevention System,
Takuya Habu, Kazutaka Sasaki, Seugou Kotani, Osamu Koyano,
FUJITSU Limited

攻撃を遮断するのが効果的である[4].

5．2 要件

このような複数の組織に跨る攻撃回避策を実施するには,従来と同様の回避手段を決定する機能に加え,さらに,その回避策を実施する場所を決定する機能が必要となる.

すなわち,攻撃回避を行うにあたり,以下を決定する必要がある.

”Who”：どの機器で対策を行うか.

”What”：何を対策として行うか.

5．3 制約条件

攻撃回避を他の組織に依頼する場合には,従来の自組織内での回避と比べて,以下の制約条件がある.

制約(1) 対策依頼元が依頼先組織のネットワーク構成情報を把握できず,どの機器で対策実施すべきかを判断できない.

制約(2) 依頼先のセキュリティポリシに反する対策実施の依頼は断られる可能性がある.

5．4 対策決定

これを踏まえ,攻撃回避のための対策決定において依頼元・依頼先が決めるべきことを明らかにする.

まず,制約(1)により,依頼元では具体的な機器を決定できない.ただし,”Where”すなわちどの組織に依頼するかは依頼元で決定することが可能である.

”What”は,基本的には予報等を元に依頼元で決めるのが妥当である.しかし,制約(2)により決定した回避策が却下される可能性がある.

5．5 ポリシの調整

このため,制約(2)の考慮,すなわち,依頼元で決定した対策が依頼先のポリシと合わない場合の調整法が必要となる.

依頼元で決定した対策と依頼先のポリシとの整合性をとるための調整に関しては,回避手段と実施場所が相互に依存する関係であるため,対策を決定・依頼する前に行うのが望ましいと考える.

5．6 基本モデル

これまでの議論を整理することで,以下のようなモデルに集約できる.

まず,あらかじめ,組織間の相互の信頼関係を認識するためのセキュリティポリシの交換を行っておく.依頼元では,攻撃予報を受け,それと想定される被害および関連する組織との相互信頼関係を参照し,回避する手段”What”と回避を依頼する組織”Where”を決定する.依頼先では,自組織の内部情報を元に回避を実施する機器”Who”を決定し,回避を実施する(図1).

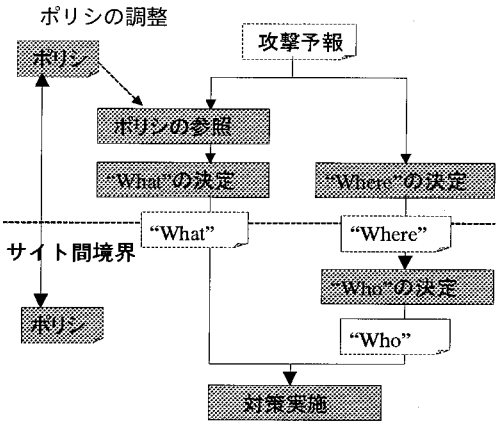

図 1 攻撃回避の基本モデル

6． まとめ

DDoS攻撃の現状と課題を明らかにし,それを解決するための攻撃回避機構の基本モデルについて議論した.

今後は,予知の前提となる攻撃モデルの確立,具体的な回避策の決定法,その他本機構の実現に必要な検討を続け,システムの試作を行う予定である.

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」の一環として行なわれているものである.

参考文献

[1] 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

[2] K.J.Houle, G.M.Weaver, *“Trends in Denial of Service Attack Technology,”* CERT/CC, Oct. 2001 <http://www.cert.org/archive/pdf/DoS_trends.pdf>

[3] 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

[4] JPCERT/CC, *“サービス運用妨害攻撃に対する防衛”*, JPCERT-ED-2001-0005, Dec. 2001 <http://www.jpcert.or.jp/ed/2001/ed010005.txt>