DDoS Attackシミュレータ

DDoS Attack Simulator

永島　秀己[*1]　大野　浩之[*2]
NAGASHIMA Hideki　OHNO Hiroyuki

インターネットをビジネスの基盤としたEC(Electronic Commerce)が活発になる一方で，不正アクセスによる被害も深刻な問題になってきている。不正アクセスによるECサイトへの攻撃は記載情報の書き換え，不正な情報取得，取得した情報の漏洩，サイトのサービスを不能状態に陥れるものまで多岐に及んでいる。これらビジネスへの新たな脅威に対処するためには，その脅威を正確に把握し，十分な対策を検討する研究あるいはそれを行うシステムが求められる。

我々は不正アクセスのうち被害が甚大で，且つ根本的な対処方法が確立されていないDDoS Attack(分散型サービス不能攻撃)に注目し，DDoS Attackを模擬実験環境上で再現し，その影響や被害の解析を行うシミュレーション設備を開発，納入するとともに，今後のセキュリティビジネスでの活用を図っている。

While Internet-based EC (Electronic Commerce) has been thriving, the damage from unauthorized access has been generating serious problems. The attacks to EC site by unauthorized access causes various problems such as data falsification, fraudulent data acquisition, unauthorized data disclosure and denial service. For the countermeasures against such growing threat to businesses, the firm system that grasps the threat precisely and researches on sufficient countermeasures is required.

We focus on especially DDoS (distributed denial of service) Attacks, which causes the most serious damage among unauthorized accesses and for which fundamental solutions have not been established yet. We make the DDoS Attack reproduced in the simulation environment, and then we have developed the simulation equipment for analyzing the influences or damages by such reproduced DDoS Attacks, along with aiming for a practical use in the future security business.

1. はじめに

EC(Electric Commerce)はインターネットの普及に伴い，そのビジネスが活発になってきている。

EC業者にとっては，インターネットはそのサービスを世界中に対し24時間提供できるビジネスの生命線である一方，世界中から24時間不正アクセスなどによりビジネスを脅かす存在でもある。

中でもDDoS(Distributed Denial of Service；分散型サービス不能攻撃)はECサイトを広範囲に，また長期的にサービス不能状態に陥れ，大きな被害を与えている。

本システムは，Webサイトの形態を，「不正アクセス者(Attacker)」，「犠牲となるWebサイト(Victim)」，「正規のWeb利用者(user)」からなる模擬環境である。

この模擬環境上でDDoS Attackツールを動作させることにより不正アクセス状況を再現し，不正アクセス状況の詳細の把握，対処方法の検討を行う。

このシステムを用いて，不正アクセス者によりDDoSが行われた場合，犠牲となるWebサイトがどのように運用不能に陥るのか，また各種のデータを収集することにより詳細に分析し，その対応策の検討を行う事を目的とした。

2. DDoSについて

インターネット上でサービスを提供する者に対して，擬似のサービス要求などを大量に送り付ける事により，システムやサービスを過負荷状態にし，サービスが提供できない状態にする攻撃をDoS(Denial of Service)攻撃と呼ぶ。

このDoS攻撃を分散環境において多数のホストから同時に行うのがDDoS攻撃である。DDoS攻撃では，**図1**に示すように，攻撃者であるAttackerは，まずセキュリ

*1 IT事業部　NSビジネスセンター
*2 独立行政法人通信総合研究所非常時通信グループ

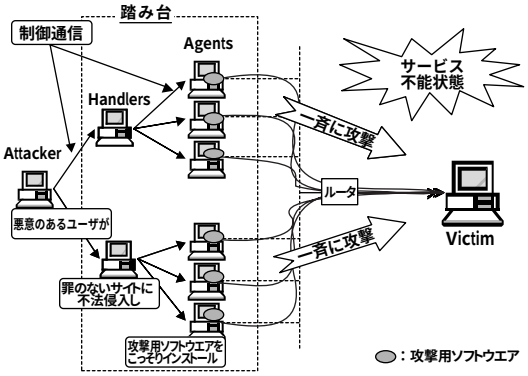

図１　DDoSの仕組み

ティの弱いサイトを見付け(踏み台)，これらに不正侵入して攻撃ソフトを潜ませておく。攻撃者からの合図で，それらのサイトは一斉にターゲットサイトに対して大量の要求を送り攻撃を実行するのである。[2][3]

最初のＤＤｏＳによる被害は，'98年3月3日全米のNASA，海軍および大学の各施設のコンピュータが攻撃を受け，使用不能となった事件といわれている。

2000年２月７日～２月８日には，米国のＹａｈｏｏ，eBay，Buy.com，Amazon.comなど有名サイトがDDoS攻撃の標的となり，一説には，約３日間の被害総額10億３千万ドルともいわれる実際の被害を出している。その被害は増加する一方で，2001年５月はセキュリティの権威である米CERT(Computer Emergency Response Team)のWebサイトまでもDDoS攻撃を受け，サービスが中断される事態に陥った。

DDoSはその他の不正アクセスと比べ

・ECサイトの全サービスが停止に陥る。
・影響が広範囲/期間が長い。
・ネットワークインフラへも多大なインパクトを与える。
・決定的な対抗策がない。

という特長がある。

また，知らない間に攻撃用ソフトウエアをインストールされて踏み台となり，無意識のうちに加害者となってしまった場合も，セキュリティ管理の不備を問われ，社会的信用を失うという側面も持つ。

3. DDoS Attackシミュレータの要件

このようなDDoS攻撃を忠実に再現し，その影響の正確な計測を行い対処方法を検討する目的でDDoS Attackシミュレータの開発を行った。

DDoS Attackシミュレータの開発の要件として定義したものは次の通りである。

(1) DDoS Attackツールは多くの場合，**図１**にて示した通り，３階層(Attacker-Handler-Agent)或いは２階層(Attacker-Agent)からなるAttacker構成を形成する。

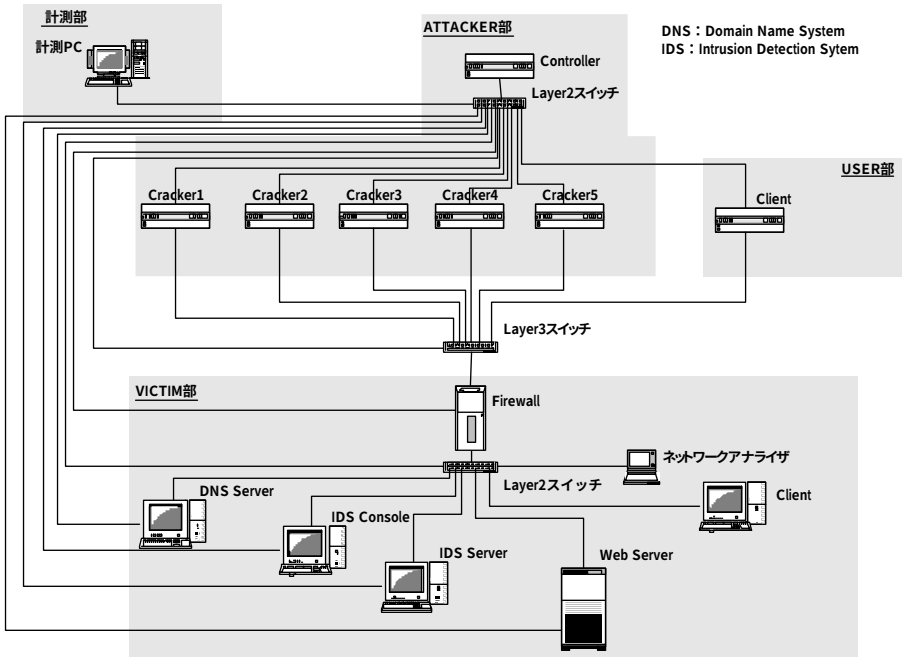

図２　DDoSAttackシミュレータの構成

またAttackerの数の多少が攻撃の成否に関わるツールも存在する。このようなDDoSの特徴を正確に模擬する為のその階層と規模を，任意に構成できる機能。

(2) 本システムで使用するＤＤｏＳツールは，インターネットなどを通じ入手することを基本とし，ツールを修正せず，ネイティブに実行可能な機能。

(3) DDoS攻撃によってサービス不能に陥る状況，過程を正確に把握するために，攻撃条件を正確に変更でき，Victimの影響を正確に把握する機能。

(4) 攻撃条件による実験成否(サービス不能の成否)がリアルタイムに把握でき，また比較検証するため実験毎のデータ保存が可能な機能。

(5) DDoS攻撃については，ベンダーから対抗手段がいくつか提供されているが，この有効性についても正確に評価可能な機能。

4. DDoS Attackシミュレータの構成

DDoS Attackシミュレータの要件を満たすように開発したDDoS Attackシミュレータの構成を，**図２**に示す。

DDoS Attackシミュレータは次の４つの部分から構成されている。

・攻撃を行うＡＴＴＡＣＫＥＲ部
・ＡＴＴＡＣＫＥＲ部からの攻撃を受けるVICTIM部
・サービス不能状況を外部から計測するUser部
・各機器，ネットワークのデータ(ＰＩＮＧ，ＨＴＴＰ，ＤＮＳ，ネットワーク負荷等)を測定する計測部

ＡＴＴＡＣＫＥＲ部は5台のCrackerPCで構成され，一斉或いは個別のDDoSツールで攻撃を行うことが可能である。

ＡＴＴＡＣＫＥＲ部とVICTIM部はインターネットを模したLayer3スイッチにより接続される。

計測対象となる，PC，サーバ，ネットワーク機器はそれぞれデータ収集時にDDoS攻撃のトラフィックの影響を受けないよう計測専用のネットワークインタフェースを備えている。各計測対象のトラフィック量，ネットワークリソース消費量，CPU負荷率などのデータは，そのネットワークインタフェースを経由して計測用PCへ収集される。

データ収集はSNMP(Simple Network Management Protocol)を基本としたが，DDoS攻撃の状況を把握する上で標準で対応できない部分については専用のAgentを開発し，データ収集を行った。

収集したデータは計測対象毎にリアルタイムでトレンドグラフ表示し，実験成否の判断が即座に行えるようにした。

また同時に全てのDDoS攻撃パケットをキャプチャし，ＭＡＣアドレス-IPアドレス対応表示を行い，IPスプーフィング(IPアドレス改竄)状況を観測可能とした。収集したデータは実験終了後CSV形式のファイルとして保存し，攻撃状態の把握，対応手段の検討のため表計算ソフトウエアなどによる解析を可能とた。

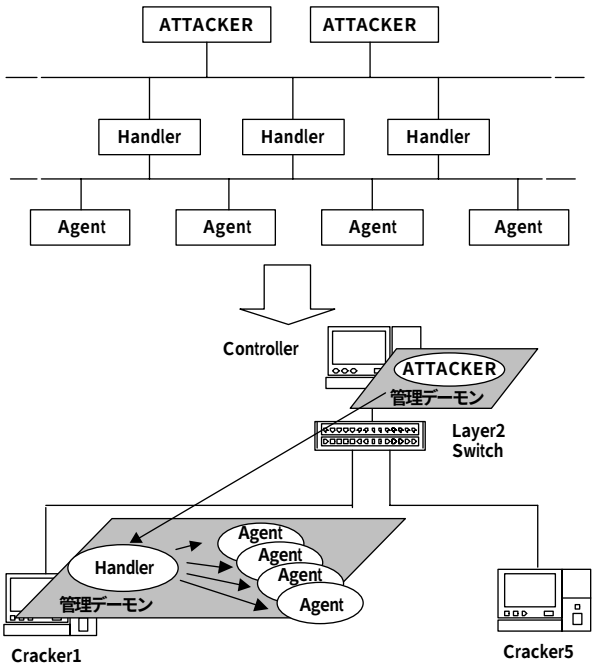

図３　シミュレーション環境上でのDDoS構成

DDoSツールは，ツール毎にソフトウエアの完成度に開きがある。DDoS Attackシミュレータでは，ソフトウエアとして未熟なDDoSツールも起動／停止など確実に管理することを目的に管理デーモンを開発し，このデーモン上でDDoSツールを実行させた。この管理デーモンはJavaで開発し，DDoSツールに合わせOS非依存で実行できる。

また，この管理デーモンにより**図３**に示すように，１台のPC上でDDoSツールを複数動作させることが可能であり，実台数以上の構成でのDDoS Attackシミュレーションを可能とした。

5. DDoS Attackシミュレータの改良

このように構成したシステムでDDoS Attackのシミュレーション実験を行い，一定の成果を得ることができたが，次のような問題点も明らかとなった。

(1) シミュレータは，AttackerPC上に複数のAgentをシミュレートすることにより，限られたAttackerPC上でもスケーラブルにDDoS環境の構築が可能な事を一つの特長とした。反面，**図１**で示したAttacker-Handler間制御信号を捕らえ解析することができない。

(2) Attacker-Handlerが１台のPC上に存在する為，Attacker-Handler間に擬似のDDoS停止信号を送るタイプのDDoSカウンターツールの動作検証ができない。

図４　不正アクセス模擬実験システム

（3）AttackerからVictimへの流入パケット量はAgent数に拠り，微妙な流入パケット量を調整することが難しい。そのため，機器のサービス不能に陥る閾値を正確に把握することができない。

これらの点を改善し，“ 不正アクセス模擬実験システム ”として開発し，総務省通信総合研究所(現独立行政法人通信総合研究所)へ納品した製品が**図４**で示すシステムである。[(5)]

このシステムでは，管理デーモンによるAgentのシミュレートを行わず，100台のAttackerPCでAttacker部を構成している。１台のAttackerPCでは１つのAgentのみを動かすこととし，より実環境に近い状況を作り出している。

また，Attacker部とVictim部の間に帯域制御装置を配置し，通信量を任意に設定することが可能な機構も備えている。

6. おわりに

当社では，今回実験装置開発で得たノウハウをベースにDDoSや他の不正アクセスの解析，対策についての研究を進め，より一層堅牢なシステムの構築に寄与していきたい。

また，独立行政法人通信総合研究所では，“ 不正アクセス模擬実験装置 ”を使用し，不正アクセス行為やサイバーテロへの対策の研究を進め，将来共同研究や受託研究も計画している。

本システムの開発に当り，独立行政法人通信総合研究所非常時研究グループ各位，大野浩之グループ長より貴重なご指導，ご助言を頂き，深く感謝の意を表します。

参考文献

(1) 大野浩之，武智洋，永島秀己，“ インターネットの脅威に対抗しうる脆弱性データベースと検証システムの構築 ”，(社)情報処理学会DSM研究会主催DSMシンポジウム'2001，2001

(2) "DDoS: Is There Really a Threat?," USENIX Security Symposium, August 16, 2000
http://staff.washington.edu/dittrich/talks/sec2000/

(3) Distributed Denial of Service（DDoS）Attacks/tools
http://staff.washington.edu/dittrich/misc/ddos/

(4) Sven Dietrich, Neil Long, David Dittrich, "Analyzing Distributed Denial of Service Tools: The Shaft Case", In Proceedings of USENIX LISA 2000, December 2000

(5) 独立行政法人通信総合研究所プレスリリース
http://www2.crl.go.jp/pub/whatsnew/press/010523/010523.html