[研究論文]

サーバ側とクライアント側との マルチ手法による DDoS 攻撃対策に関する考察

岡崎美蘭

情報ネットワーク・コミュニケーション学科

A Study of DDoS Attacks Provision Method by Server and Clients

Mirang OKAZAKI

Abstract

A cyber-attack is any type of offensive maneuver (such as a DDoS attack) employed by individuals or organizations against infrastructures, computer networks, and/or personal computers and handheld devices. Assailants can attack targets using a variety of malicious actions, usually originating from anonymous sources, with the purpose of stealing from, altering, or destroying a specified target. Most Internet service providers have established countermeasures to DDoS attacks in their network backbones. These devices can control available bandwidth while implemented proxy responses, but they often cut off valid communications because it is impossible to clearly discern legitimate users from hidden attackers. In this paper, we consider about HTTP flood attacks provision method by server and clients. When a server determines attacks are in progress, it records the interval between the session establishment and update times and then diverts any further incoming attack messages to the virtual Web server(decoy server). If legitimate users are hijacked or tricked into attacking the server, the server displays an error page informing them of the nature of the attack and how to stop it.

Keywords: DoS, DDoS, HTTP-Get Flood

1. はじめに

ネットワーク技術の発展により,インターネット上での情報検索や電子商取引,コミュニケーションツールなどのWebサービスが急激に普及している．その為，24時間Webサービスが提供できる環境作りが求められている.つまりWebサービスが停止した際の社会への影響は多大なものになる．近年では特定組織に対しての抗議，主張，国際的な問題，個人的な憎悪が原因で，意図的に攻撃対象のシステムのサービス提供を不能にする妨害攻撃が問題視されている．中でもサービス妨害(Denial of Service: Dos)攻撃，分散サービス妨害(Distributed Denial of Service :DDoS)攻撃が深刻な問題となっている．DoS攻撃は単一のコンピュータからの攻撃を行うのに対して,DDoS攻撃は数千以上の大量の端末が攻撃対象となる特定のサーバに対して一斉に大量のパケットを送信し,通信経路や対象サーバをダウンさせる．従って，DoS攻撃が単一のホスト（通信相手）からの攻撃であればそのホストとの通信を拒否する手段を取ればよいが,膨大な規模のホストからなるDDoS攻撃は，個々に対応することが難しいとされている．またDDoS攻撃は少なくとも現状では標的にされれば完全に防ぐ方法はなく,インターネットの根幹に対する脅威となっている[1].

最近は攻撃者がWebサーバに大量のコネクションを張り，サーバのリソースを枯渇させるHTTP-GET-Flood攻撃が増えており,その対策などに関する研究が行われている[2][3].そこでは一般利用者の通信をできるだけ生かしつつ,対策を行っていることが攻撃者に気づかれにくくなるよう仮想マシンを複数台使用することで資源の分離を行い，攻撃者と通常利用者が使用できる資源を分けている.また，攻撃者が利用できる資源の操作を行うことで，攻撃が成功しつつあるかのように見せている.これらの対策では,攻撃者に攻撃が成功しつつあるかのように見せかけるだけで，実際に攻撃者の攻撃行為を止める対策ではない.従って,攻撃によりネットワークのリソースや帯域が圧迫されるなどの問題点が残る.

一方,昨今はファイアウォールやIDS等のセキュリティ製品での検知ができず,少ないパケット数でWebサーバのリソースを浪費させ，サービス不能にする高度的な「スロ

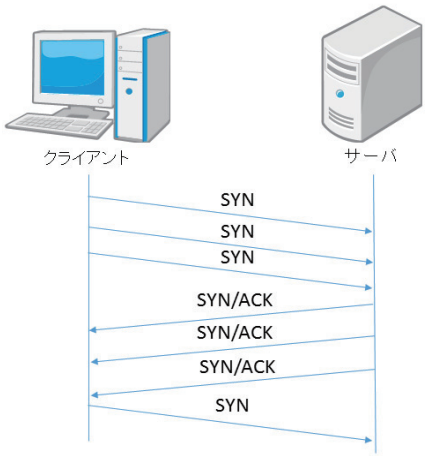

Fig.1 SYN Flood Attack

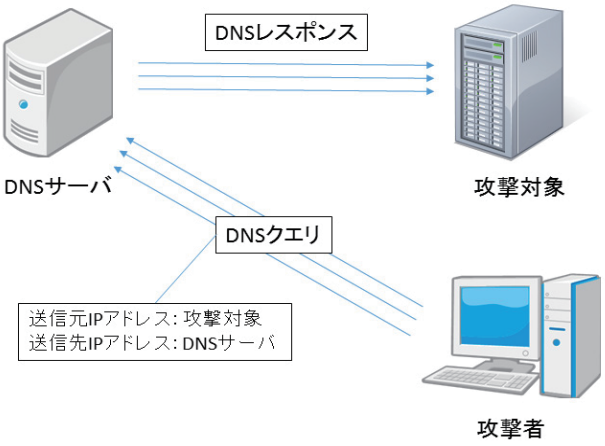

Fig.2 DNS Amp Attack

ークライアントアタック(Slow Client Attack)」攻撃が増加しつつある[5]. スロークライアントアタックには, Slowloris 攻撃, Slow POST DoS 攻撃, Slow Read DoS 攻撃がある. このようなスロークライアント攻撃の対策手法としては, Web サーバの Timeout 機能を利用して, プロセスとの接続が長くなるとコネクションを強制的に切断することができる. しかし, DDoS 攻撃の場合は複数の攻撃者が交互に攻撃することにより, 新しいコネクションを発行することができ, 完全に攻撃を防御できないと考えられる. 特に, Slow Read DoS 攻撃についてこのような Timeout の効果について実験を行った結果, Timeout の値を短く設定しても攻撃を防ぐことが難しく, 効率的に攻撃が実行できるという報告がある[6].

本研究では, 近年増え続けている HTTP 攻撃に焦点を当て, この攻撃に対してサーバ側で主動的にエラーページを攻撃者に見せることで, クライアント側にこの違法性があることを示して, 攻撃を止めさせる手法について検討する. そこで, 従来のサーバ側のみでの対策だけではなく, クライアント側も加えることによって, サーバ側とクライアント側とのマルチ手法による DDoS 攻撃対策手法を提案する. 更に, 提案手法の実装を行い, 実験を行うことで本提案手法の有効性を確認する.

以下, 2 章では DoS/DDoS 攻撃の概要と一般的な対策手法につて述べる. 3 章では, マルチ手法による HTTP 攻撃対策を提案し, 4 章で実験によりその有効性について考察する.

2. DoS/DDoS 攻撃対策

2.1 DoS/DDoS 攻撃とは

DoS(Denial of Service)攻撃とは, サーバや回線といったネットワーク上のリソースに対して攻撃を行い, 攻撃対象のシステムのサービス提供を不能な状態にする攻撃である. DDoS (Distributed Denial of Service)攻撃とは, 攻撃者が標的に対して直接攻撃を行うのではなく, セキュリティの弱い別の踏み台となるコンピュータに不正侵入し, 攻撃ソフトのインストールを行う. この踏み台は, 非常に多数のコンピュータで構成される. こうして分散された大量のコンピュータから一斉に特定のネットワーク機器へ大量の処理負荷を与えるためにパケットを送信し, サーバが大量のパケットを処理しきれずに通信路をあふれさせて機能を停止させる攻撃である. 単一のホスト (通信相手)からの攻撃であればそのホストとの通信を拒否すればよいが, 数千・数万のホストからでは個々に対応することが難しい. そのため, DDoS 攻撃は通常の DoS 攻撃よりも防御が困難であり, 攻撃による被害は DoS 攻撃よりも大きくなると考えられている. 攻撃を受けたサーバには踏み台となったコンピュータが攻撃主として認識される. DDoS 攻撃はほかの不正アクセスに比べて, サイトの全サービスが停止に陥る, 影響が広範囲で期間が長い, 決定的な対抗策がないという特徴がある. このような DoS/DDoS 攻撃は, 攻撃対象によって, 大きく以下の三つに分けることができる.

(1) 回線帯域への攻撃手法

ネットワークに大量のパケットを送りつけ, ネットワークのリソースを消費し, 接続をしづらくすることでサービスの提供を不能にする攻撃である. この攻撃は, ネットワークとシステムを接続する回線がパケットで埋め尽くされてしまうために, システムに余裕があっても通信ができない状態となる為, システム側での防御が困難なことが多い.

(2) サーバのシステム資源を浪費する手法

攻撃対象に大量のリクエストの発行やコネクションの確立を行うことで, サーバの処理を超える要求を出しサーバに負荷をかけ, サービスの提供を不能にする攻撃である. この攻撃手法に対してはサーバ側で一定の対策が可能である. この種類の攻撃には, ネットワークレイヤ型攻撃, アプリケーションレイヤ型攻撃などが挙げられる.

(3) システムの脆弱性への攻撃

ルータやサーバの脆弱性を利用し, システムのサービス

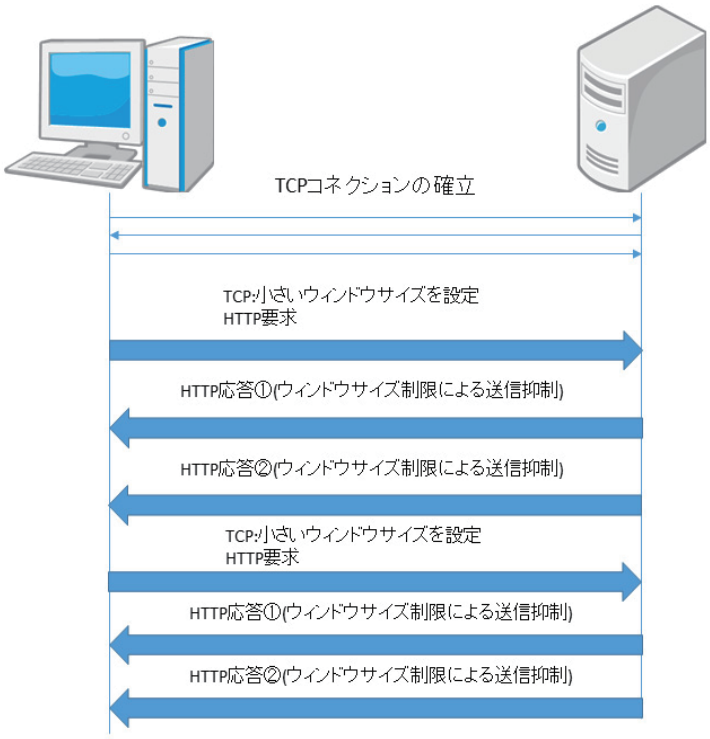

Fig.3　Slow Read DoS Attack

提供を不能にする攻撃である．この攻撃手法に対しては，アップデートやパッチを適用することで脆弱性を取り除くことで回避することができる．脆弱性を狙った攻撃には，Ping of Death 攻撃，Teardrop 攻撃，Land 攻撃などが挙げられる．

2.1.1 ネットワークレイヤ型（L4）攻撃

大量のパケットで，ネットワークの帯域を埋め尽くしたりすることにより，サーバ，ネットワーク機器の管理機能を過負荷にする攻撃である．攻撃対象と正常なセッションを確立しないため，送信元 IP アドレスの偽装が容易で攻撃者の特定が難しい．主な攻撃手法として，SYN Flood 攻撃，DNS Amp 攻撃などが挙げられる．

(1) SYN Flood 攻撃

インターネット上の TCP 接続において，本来ではクライアントがサーバに SYN パケットを送信し，受け取ったサーバがクライアントに対して SYN/ACK パケットを返信，最後にクライアントが ACK パケットの送信を行う 3way ハンドシェイクを行う． SYN Flood 攻撃とは，図 1 に示すように，攻撃者が意図的に大量の SYN パケットを送信し，ACK パケットの送信を行わずに放置することで，次第にサーバ側の「応答待ち」の接続数が限界を超え，新たに接続を受け付けられない状態となる．サーバ側は最後の ACK パケットが届くまでは「応答待ち」の状態で待機することになり、その接続のために用意されたメモリ領域などのリソースが利用できなくなる．

(2)DNS Amp 攻撃

DNA Amp 攻撃とは，図 2 に示すように，DNS サーバを増幅器として利用し，データサイズを増加させる手法である．この攻撃では，DNS レスポンスが DNS クエリよりもデータサイズが大きいことを利用する．発信元 IP アドレスに攻撃先となる IP アドレスを設定して小さなデータサイズの DNS クエリを DNS サーバに送信すると，DNS サーバは大きなデータサイズの DNS レスポンスを返送することになる．この場合，詐称された発信元のネットワークには大きなデータサイズの到着によりトラフィックが増大し，サービス不能状態に陥ってしまうことになる．

このような攻撃の多くは，セキュリティ能力の高いファイアウォールや IPS/IDS などの検知システムによって防御が可能である．

2.1.2 アプリケーションレイヤ型（L7）攻撃

近年では攻撃の手法が，ネットワークレイヤ型攻撃からアプリケーションレイヤ型攻撃に移行してきている．主な攻撃手法として，攻撃者が大量のコネクションを Web サーバに張り，攻撃対象となる特定のサーバのリソースを枯渇させ，サーバをダウンさせる HTTP-GET Flood 攻撃がある．最近では，大量のパケットやデータを送らないで，ゆっくりリクエスト/レスポンスデータを送受信する「スロークライアントアタック（Slow Client Attack）」と呼ぶ攻撃が多い．スロークライアントアタックには，スローHTTP ヘッダ（Slow HTTP Headers）攻撃，スローHTTP ポスト（Slow HTTP POST）攻撃，Slow Read 攻撃などが挙げられる．これらは，通常のセッションを確立するため正規の通信と攻撃を区別することが難しい．

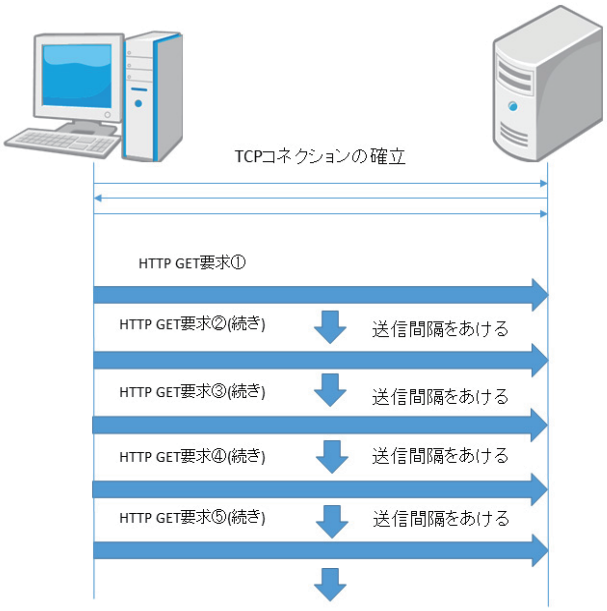

Fig.4 Slowloris Attack

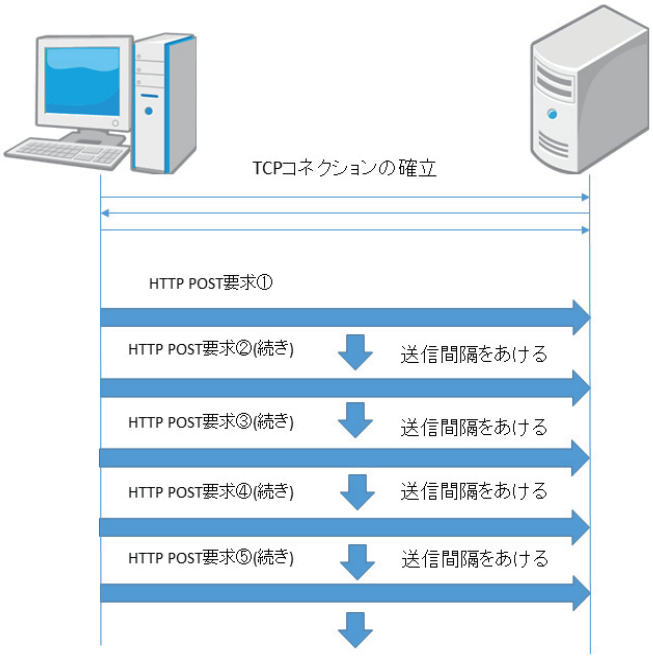

Fig.5 Slow POST Attack

(1)HTTP-GET Flood 攻撃

HTTP-GET Flood 攻撃とは，Web サーバとの間に TCP コネクションを確立させた後に，HTTP-GET 要求を送信し，Web サーバにコンテンツを応答させる処理を大量に実行する手法である．このようなコンテンツの応答は，Web サーバの負荷を上げるだけではなく，接続するネットワークに大量のパケット転送を発生させるためトラフィックが増大し，Web サイトがサービス不能状態にはまってしまうことになる．

(2) Slow Read DoS 攻撃

Slow Read Dos 攻撃とは，図 3 に示すように，Web サーバに対して TCP プロトコルのウィンドウサイズを小さく通知し，HTTP 応答データを少しずつ送信させるよう制御することで時間をかけさせるという手法である．これにより，Web サーバ上のプロセス占有時間が長くなり，無駄なリソース消費が発生することになる．さらに，攻撃者は Web サーバの最大同時接続数(MaxClient 数)まで接続することで，Web サーバがほかの新しい接続を受け入れることができない状態を作り出す．

(3)スローHTTP ヘッダ攻撃

Slowloris 攻撃とも呼ばれる．図 4 に示すように Web サーバに，HTTP-GET 要求を少しずつ送信し時間をかけることで，Web サーバのプロセス占有時間を長くし，サーバに無駄なリソース消費を発生させる．

(4) Slow POST DoS 攻撃

Slow POST DoS 攻撃とは，図 5 に示すように HTTP POST 要求を少しずつ送信することで時間をかけさせる手法である．これにより，Web サーバ上のプロセスの占有時間を長くして無駄なリソース消費を発生させる．

Slow Read DoS 攻撃，Slowloris 攻撃，Slow POST DoS 攻撃のいずれも，少ないパケット数で Web サーバのリソースを消費させ，サービス不能にするものである．これらの攻撃コードは公開されていることから，ボットに組み込まれ DDoS 攻撃に使用される可能性も想定される．

2.2 L4 型 DoS/DDoS 攻撃対策

ネットワークレイヤ型 DoS/ DDoS 攻撃の主な対策として，パケットに対しての対策とネットワーク環境を改善する手法がある．パケットに対する対策としては，ソースアドレスが詐称されたパケットやブロードキャスト宛パケットをフィルタリングする．例えば，不必要な ICMP パケット，UDP パケットや SYN パケットなどがあれば，そのパケットを拒否したり帯域制限を行うようにする．また，ネットワーク機器がブロードキャスト宛パケットを受け取った場合は，受け取ったパケットやフレームを宛先情報に基づいて適切なポートへ送出することを禁止するようにする．

ネットワーク環境の改善としては，サーバやネットワークデバイスの処理能力を増強したり，回線・ネットワークデバイス・サーバの負荷分散機能を含めたシステムの再構成を行う．また，各種デーモンのチューニングを施すことによるレスポンス改善を行う．

2.2.1 ルータにおける対策

(1) トラフィック制限

外部からの不必要な ICMP や UDP トラフィックを制限する．公開サービスへの UDP Flood 攻撃に対して該当ポートに割り当てる帯域幅を制限する．また，SYN パケットの転送レートを制限する．特定の場所からの大量アクセス攻撃に対しては，ルータでアクセス別に拒否する．

（2）IP スプーフィング防止

到着したパケットインターフェースから送信元アドレスへの経路の中に CEF(Cisco Express Forwarding)テーブルが存在しない場合は破棄する.送信元アドレスにプライベートアドレスが設定された内向きのパケットは遮断する.送信元アドレスに自ドメインのアドレスが設定された内向きのパケット，又は，送信元アドレスに外部のアドレスが設定された外向きのパケットはドロップする.

（3）その他

DoS 攻撃に対する脆弱性の対処を行うか，ネットワーク機器の処理能力を増強する.ルータが攻撃対象にならないように不要なサービスを停止する.

2.2.2 ファイウォールにおける対策

ファイアウォールにおける対策としては,ファイアウォールの Account ログ，NBT パケット等のログはできる限り記録量を減らす．ルールの作成において，頻繁に使用されるルールをルールベース上に作成する．また，同じセキュリティ・ポリシーを持つサブネットマスク群は 1 つのネットワークとして定義したり,グループを使用したりして検知・遮断のルールの数を減らす．さらに，ドメイン・オブジェクトは使用しない．もし使用する場合は，ルールベースにおいて，アドレス変換ルール内で，アドレス範囲オブジェクトの代わりにネットワーク・オブジェクトを使用することで,ルールの作成においてファイアウォールに負担がかからないようにする.

2.2.3 サーバにおける対策

サーバにおける対策としては,そのサーバに必要なサービス関連以外のポートは塞ぐか,各種デーモンでロギングの際にリクエスト元の名前解決を行うことを禁止する.特に，SYN Flood 攻撃の対策として 3way ハンドシェイク時のタイムアウトを短くするか，SYN Flood 攻撃に対するプロテクション機能を有する OS を導入し，機能を有効にする．また，ハーフコネクション要求を受け付けるキューを大きくする．さらに，サーバ処理を増強するため，Web サーバの負荷分散を行ったり,ネットワーク構成を再考したり，サーバの構成を見直すのも対策として有効である.

2.3 L7 型 DoS/DDoS 攻撃対策

2.3.1　HTTP-GET Flood 攻撃対策

HTTP-GET Flood 攻撃は元々正常な通信を大量に行うことで攻撃しているため,ファイアウォールや IDS 等のセキュリティ製品での検知ができず，攻撃を意図した通信か，否かの判断が難しい．そこで“攻撃”とは，サーバ管理者にとって不都合なアクセスとし，同一 IP アドレスから一定頻度以上のアクセスがあった場合に攻撃者と判断する.そこで,この攻撃に対して一般利用者の通信をできるだけ生かしつつ,対策を行っていることが攻撃者に気づかれにくくなるよう Web サービス提供側で可能な対策の研究が行っている[2,3]．ここでは，仮想化技術を使って 1 台の物理マシン上に複数台の仮想マシンを導入することで,攻撃者と一般利用者が利用できる資源（CPU,メモリ，ディスク，回線帯域など）を分離する．具体的には，仮想化ソフトウェア Xen を使って,ハードウェアの制御や管理を行う特権をもつドメインである Domain 0 と，その他のオペレーティングシステムが動作し特権をもたないドメインである Domain U から成る仮想化システムを構成することで，Domain 0 でユーザのアクセスが攻撃であるかの判断を行い，攻撃と判断した IP アドレスからのアクセスを Domain U へ振り分ける．また，Domain 0 は Domain U のリソース制御を行うことで,処理時間がかかる状態すなわちサーバの不能状態を作り出すことができる.

この提案においては,攻撃者が利用する資源の操作を行うことで,攻撃者に攻撃が成功しつつあるかのように見せるが,実際に攻撃者に攻撃行為を止める対策が行われていない．たとえ，成功しつつあるかのように見せることに成功しても，攻撃が停止することに等しくはないので，ネットワークのリソースや帯域が圧迫される．また，最近の DoS/DDoS 攻撃の攻撃目的が政治化，思想化していることにより,一般利用者が攻撃者になることが多いと考えられる．そこで一般利用者に攻撃成功を見せても，専門知識がないため，効果が得られない問題点がある.

3. マルチ手法による HTTP 攻撃対策

本研究では，アプリケーションレイヤ型の DoS/DDoS 攻撃である，HTTP-GET Flood 攻撃対策手法について検討する.

3.1 サーバ側とクライアント側とのマルチ手法

高度化したアプリケーションレイヤ型の DoS 攻撃である，HTTP-GET Flood 攻撃は，攻撃時に TCP セッションを確立しなければならないため,送信元を詐称することが難しい．また一定量送信しないと攻撃にならない．そこでセッションの確立時間と更新時間の間隔を記録し,攻撃として判断した場合,攻撃端末(ホスト)にエラーページを表示させ，クライアント側で送信を制御するようにする．そして，サーバ側でエラーページをアクセスした IP アドレスを記録し，連続アクセスした場合は通信を遮断する．これで，サーバ側とクライアント側とのマルチ手法による HTTP 攻撃を防御する方法を提案する.

3.2　攻撃の判断手法

通常利用者の正常利用を最大限度に配慮するため,本研究での“攻撃”とは，同一 IP アドレスから 3 秒間 5 回以上のアクセスがあった場合に攻撃者と判断する.その理由

Table 1.Number of Count F5 Key

累計実験者数	16 名
実験時間	1 秒間
最大押下回数	12 回
最低押下回数	6 回
平均押下回数	9.31 回

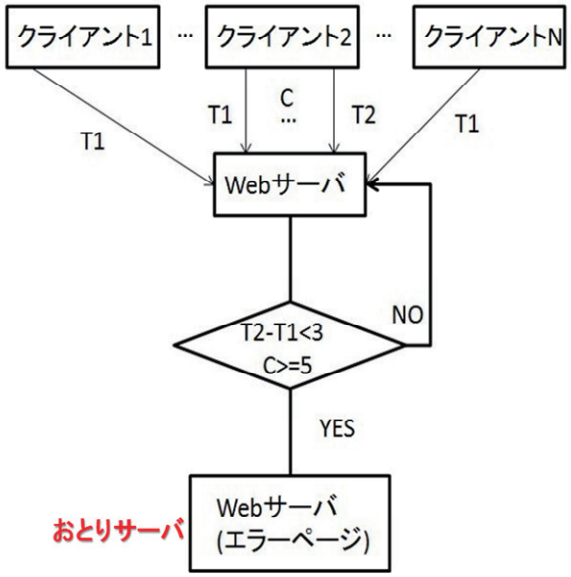

Fig.6 Attack judge Method

としては，実験結果から一般ユーザが更新キー（F5 キー）を連続的に押下する回数は表 1 に示すように，1 秒間 8,9 回程度となることが分かったからである．また，代表的な HTTP GET Flood 攻撃を行うウイルスは約 0.03 秒で GET 要求を行うため，はるかに攻撃判断基準を超えているので，それらに対する遮断効果もある．具体的に，初めて確立したセッションの時間を T1 で記録し，その後の利用者によるセッションの更新時間を T2 で記録するとする．その T2 と T1 間に何回セッションを更新したか，更新回数を C(Counter)で記録する．

図 6 に本研究でのサーバ側で攻撃判断制御手法を示す．ここで，攻撃と判断した Web サーバ側では，その HTTP リクエストのクライアントをおとりサーバ側へ転送する．おとりサーバ側では，そのクライアントへエラーページを表示する．

3.3 実験環境

提案手法の効果を解析するために図 7 に示すような実験環境を構築した．ここでは，サーバマシン 1 台に仮想化ソフトウェアにより仮想 Web サーバを 2 台作成し，エラーページ表示するサーバを Web Server2 に設置する．図 6 で示した攻撃判断によって，攻撃判断されたリクエストをエラーページに転送する．また，外部攻撃マシンと内部サーバマシンとの間にロードバランサを設置し，ロードバランサによって各クライアントからのアクセスを振り分けるようにする．すなわち，ロードバランサで攻撃と判定されたアクセスは，エラーページを表示するように設定された Web Server2 に転送される．各マシンの構成を表 2～表 5 に示す．ロードバランサの OS としては BIGIP-10.1.0.3341.1084 を使った．

3.4 実験手法

2 台のホストマシンに仮想マシンを各 10 台用意，合計

Table 2. Web Server Spec.

OS	Windwns7 Professional Service Pace 1 (x86)
CPU	Inter Core Quad Q9650(3.00GHz)
Memory	4 GByte
仮想計算機	VMware Player 5.0.0 build-812388

Table 3. Attack Server Spec.

OS	Windwns7 Home Premium (x64)
CPU	Inter Core I5-3470(3.20GHz)
Memory	16 GByte
仮想計算機	VMware Player 5. 0. 0 build-812388

Table 4. Web Server

OS	Ubuntu
CPU	1 Unit
Memory	256 MByte
Web Server	Apache 2.2.15

Table 5. Attack Server

OS	Windwns7 Professional SP1 (x86)
CPU	1 Unit
Memory	1 GByte
テストツール	Apache JMeter

20 台の仮想マシンに IP アドレスを割り振る．Web サーバは，仮想マシン VM1～VM2 をそれぞれ Web サーバ WebServer1～WebServer2 として動作させる．また，エラーページは WebServer2 に設置する．WebServer1～WebServer2 は同一の Web サービスを提供するものとする．実験の評価としては，クライアントマシンからリクエスト発行したときから遮断までの時間を計測するとする．そこで，攻撃マシンを 20 台とし，一般ユーザによるリロード攻撃に似ている攻撃頻度で，スレッド遅延間隔を 4000, 2000, 1000, 800, 600, 400, 200 に変更して，各攻撃マシンのスレッド数が 1 として遮断時間を測定する．

4. 実験結果と考察

4.1 実験結果

図 7 での実験環境で行った実験結果を以下で示す．

図 8 に，各攻撃マシンの攻撃スレッドを 1 とし，スレッド遅延間隔を変化させた場合の，20 台攻撃マシンの通信遮断までの平均所要時間を示す．

本研究での遮断基準値は 3 秒で 5 回になっているので，即ち 600ms で 1 回攻撃が来る場合，エラーページに転送する．連続エラーページをアクセスした場合は通信を遮断することになっている．スレッド遅延間隔が 600～200ms のときは，基準値に超えている攻撃頻度なので，それぞれ通信を遮断した．4000～800ms のときは，基準値に達してな

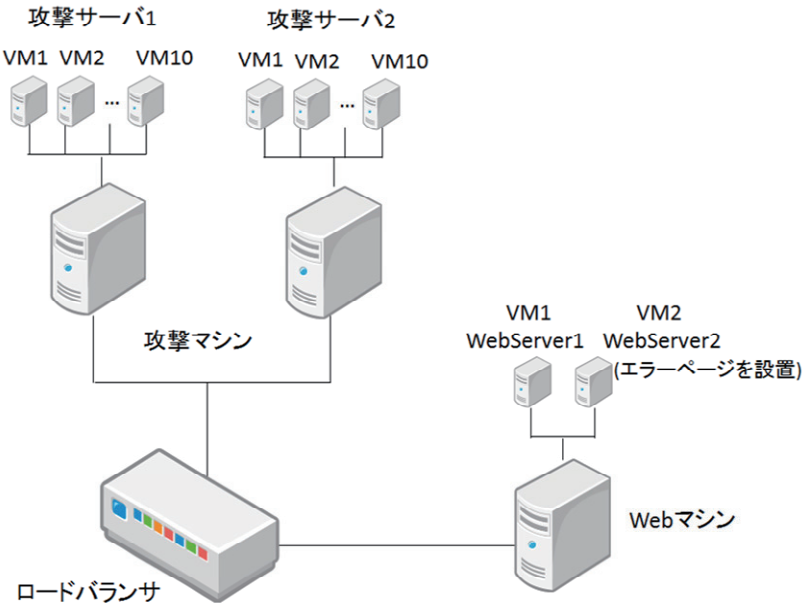

Fig.7 Experiment Environment

いので，通信を遮断することは確認できなかった．

図 9 に，各遅延間隔での攻撃時の Web サーバの CPU 使用率 MAX 値を示す．600～200ms のときは，27～45%になっている．これに対して，短時間で通信を遮断した 4000～800ms のときは，CPU 使用率 MAX 値が 15～24%という極めて低い水準なので，サーバでの通常処理に問題ないと思われる．

以上から，提案手法の基準に達したものは正常に遮断することを確認できた．

4.2 考察

本提案手法では，仮想マシンより同一のサービスを提供する複数台の Web サービスを用意し，その中 1 台の Web サーバにエラーページを表示するように設置している．そこで，複数台の Web サーバを利用するため，クライアントと Web サーバの間にロードバランサを導入している．また，攻撃の判断条件はシステム本来のセッション機能を利用するため，別の分析ソフトウェアを用意する必要するがない．以上のことから，本提案手法は既存のシステムへの導入が容易であるといえる．

本研究では，HTTP 攻撃に焦点を当て，同一 IP アドレスからの過剰アクセスに対して，主動的にエラーページを表示している．そこで，攻撃の呼びかけに応じて攻撃協力者になる一般利用者にこの行為は明確な違法性があることを示し，攻撃を止めさせることができる．従って本提案手法は DoS/DDoS 攻撃によるサーバの負荷を軽減する効果があると考えられる．

5. まとめ

現在，Web サービスは広く一般に利用され，日常生活を行う上で欠かせないものとなっている．それに伴い，Web サービスが停止した際の社会的影響も大きくなっている．一方，DDoS 攻撃の傾向は過去のサービス停止が甚大な損失につながるオンラインゲームサイトなどを対象とした恐喝の手段に用いられることから，Anonymous の攻撃に代表されるような，政治的・思想的主張によるものに変わりつつある．これによって，一般利用者が攻撃に参加することが多くなっている．本研究ではこの点に着目し，一般利用者が攻撃しやすい HTTP 攻撃に焦点を当て，主動的にエ

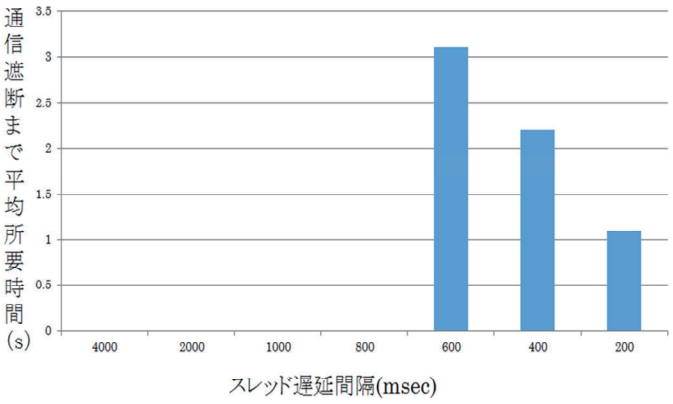

Fig.8 Average Time of Traffic Interception

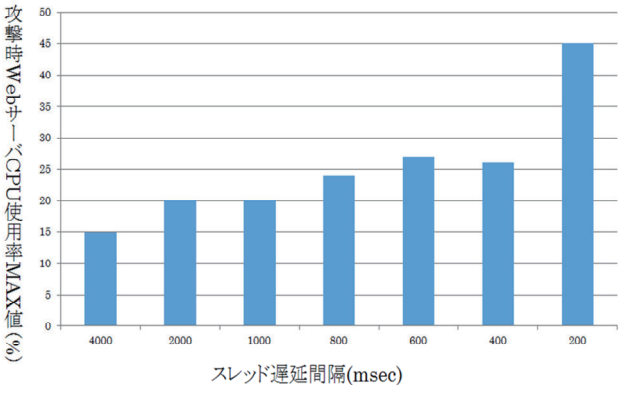

Fig.9 CPU MAX Value of Web Server

ラーページを見せる手法を提案した．その結果，この行為は明確な違法性があることを示して，攻撃を止めさせることができると．

更に本研究では，提案手法の有効性を確かめるために，Web サーバからエラーページ表示できる実験を行った．その結果，本提案手法によって攻撃として判断したアクセスにエラーページを表示し，エラーページを連続アクセスした IP アドレスの通信を遮断することができたことを確認した．

今後の課題として，攻撃制御基準の柔軟性が低い点を改善することが挙げられる．

参考文献

[1] 寺田真敏，“DoS/DDoS 攻撃とは”，情報処理，Vol.54 No.5,pp.428-435，May 2013.

[2] 高橋 朝英，田口 元貴，小林 良太郎，加藤 雅彦：仮想計算機のリソース制御による HTTP-GET Flood 攻撃対策，電子情報通信学会論文誌 D vol.J94-D,no.12,pp.2058-2068，2011.

[3] 吉田 祥真，三上 烈史，小林 良太郎，金岡 晃，加藤 雅彦：複数台のおとりマシンによる HTTP-GET Flood 攻撃対策，第 11 回情報科学技術フォーラム，第 4 分冊，L-032,2012.

[4] 倉上 弘，“DoS/DDoS 攻撃対策(2)～高度化する DDoS 攻撃と対策サイトの視点から～，”情報処理，Vol.54 No.5,pp.475-480，May 2013.

[5] キーマンズネット，“安心安全な Web サイトのつくり方～スロークライアントアタック～”，http://www.keyman.or.jp/kc/sec/firewall/30006788/, 2013.

[6] 朴，岩井，田中，黒川“Web サーバの Slow Read Dos 攻撃に関する考察”SCIS2014.pp.907-919，2014.

[7] みやたひろし：「サーバ負荷分散入門」，SoftBank Creative 2012 年 6 月

[8] 鶴長 鎮一：「サーバ構築の実際がわかる Apache[実践]運用／管理」，株式会社技術評論社 2012 年 4 月