2004－ＣＳＥＣ－26　(17)
2004／7／20

Mobile IPv6 技術を応用した輻輳型 DoS 攻撃回避方式の提案

日下 貴義　角 将高　馬場 達也　稲田 勉

株式会社 NTT データ 技術開発本部

〒104-0033 東京都中央区新川 1-21-2 茅場町タワー

E-mail:　{ kusakat, babatt, kadom, inadat}@nttdata.co.jp

あらまし　モバイル IPv6 技術を応用することによって，回線を飽和させたりサーバ処理能力を飽和させたりするような輻輳型 DoS 攻撃から，インターネットにサービスを公開しているサイトを守る方法を提案し，試作によって動作を検証した結果を報告する．具体的提案内容は，モバイル IPv6 技術の IP アドレス変更機能と移動先 IP アドレス通知機能を使うことによって，輻輳型 DoS 攻撃を受けているサーバの IP アドレスを動的に変更し攻撃先から逃れ，さらに正規ユーザの接続は維持し続けることができる特徴を持つものである．

キーワード　DDoS 攻撃，モバイル IP，ネットワークセキュリティ

A Proposal of Congestion DoS Attack Avoidance System to which Mobile IPv6 Technology Applied

Takayoshi KUSAKA, Tatsuya BABA, Masataka KADO, and Tsutomu INADA

Research and Development Headquarters, NTT Data Corporation

Kayabacho Tower, 1-21-2, Shinkawa, Chuo-ku, Tokyo, 104-0033 Japan

E-mail:　{ kusakat, babatt, kadom, inadat }@nttdata.co.jp

Abstract　We propose how to protect a site of services to the public in the Internet from the congestion type DoS attack which saturates server management ability , and the result that a movement was verified by the trial production is reported. Concrete contents of a proposal change the IP address of the server which congestion type DoS attack is taken from dynamically by using the function which changes the IP address of the Mobile IPv6 technology, and the function which informs it of the movement point IP address. Furthermore as the characteristics, the connection of the legitimate user can be maintained.

Keyword　DDoS Attack, Mobile IP, Network security

1. はじめに

電子商取引や各種情報公開など，インターネットを利用したサービス提供が多様化するに伴い，インターネットの重要な社会基盤としての役割や影響力は高まっている．特に，インターネットを使っての決済処理，株取引，競売，資金移動などのサービスを提供している場合，一時的でもそのサービスの遅延や停止が与える影響は大きく，個人や企業に直接的な被害を与える可能性がある．そのため，インターネットにおけるシステムのセキュリティや堅牢性について，十分な対策を施す必要がある．本稿では，対策の中でも特に，インターネットに公開しているサービスが受ける不正行為を対象とし，その対策を考案する．

インターネットに公開しているサービスが受ける不正行為の代表的なものに，DoS 攻撃（Denial of Service Attack：サービス不能化攻撃）がある．DoS 攻撃の中でも，DDoS 攻撃（Distributed Denial of Service Attack：分散型サービス不能化攻撃）と呼ばれる輻輳型の DoS 攻撃は，乗っ取りに成功した多数のホストを利用して攻撃目標となるサイトに大量のパケットを送りつける攻撃であり，結果的に攻撃対象のサービスが大幅に遅延または停止する事態にまで至らしめることができる攻撃である．公開されている DDoS 攻撃の主な事例[1]では，米 SCO 社のウェブサイトが 2003 年中，断続的に DDoS 攻撃を受け続け，ウェブサイトが閲覧不能に陥ったことが良く知られている．また，非難を受けた報道機関系サイトや政府機関系のサイトは，社会的影響力の点から DDoS 攻撃の標的となることが多い．他に，オンライン決済プロバイダである英 WorldPay 社が大規模な DDoS 攻撃を受け，取引がほと

んど処理できなかったという事例は，DDoS 攻撃が企業の名声以外にも直接経済的な被害を与えることがあることを示しており，そのため金融機関やギャンブルサイトなどは，実際に DDoS 攻撃者の恐喝対象となっている．さらに最近では，ウイルスを利用して無差別に乗っ取ったホストが，特定サイトに DDoS 攻撃をしかけるなど，攻撃の効果は増大する傾向が見られる．以上のような事例から，インターネット上にサービスを提供している企業を中心に，DDoS 攻撃と呼ばれる輻輳型 DoS 攻撃に対して効果的な対策が，求められている．

輻輳型 DoS 攻撃への対策は主にネットワークプロバイダでなされることが効果的ではあるが，本稿では，インターネット上にサービスを提供しているシステムにおいて実施できうる対策に特化し，輻輳型 DoS 攻撃回避方式として提案，動作検証のためにプロトタイプを試作した．さらに，本方式の機能的な有効性について，一部検証を行った結果を報告する．

2. 攻撃と被害の分類

本章において，インターネットに公開しているサービス（以後、公開サービスと記述する）が，現状どのような脅威にさらされているかを分析する．そのために，まず公開サービスが受ける攻撃の種類について整理し，次に，その攻撃によって引き起こされる被害を分類する．これにより，我々が対処できる攻撃や被害はどのようなものであるかを把握する．

なお，公開サービスとは，いわゆる DMZ（DeMilitarized Zone）に配置されるサービスであり，例えば，公開ウェブサーバや外向けの DNS や外部とやりとりするメールサーバなどが存在する．

2.1. 攻撃の種類

公開サービスの受けうる攻撃の種類を，大きく以下の三つ（輻輳攻撃，脆弱性攻撃，侵入）に分類した．

（1） 輻輳攻撃

悪意のある大量アクセスであり，Syn Flood や UDP Flood などの Flood 系の攻撃や，DDoS 攻撃や DRDoS（Distributed Reflection DoS）攻撃がこれにあたる．F5 Attack（HTTP Reload Attack）など，大量のアクセスではあるがプロトコル的には異常ではないので，攻撃かどうかの区別がつきにくい．悪意のない単なる大量アクセスは Flash Crowd と呼ばれ，攻撃には分類されない．

（2） 脆弱性攻撃

プロトコル実装の脆弱性を狙った攻撃と，アプリケーションや OS，ミドルウェア実装の脆弱性を狙った攻撃がある．前者に関して，古くは Ping of Death，Tear Drop，Land Attack などがこれに相当する．後者に関して，バッファオーバフローや XSS（Cross Site Scripting）がこれに相当する．1～数回程度の少数のパケットによるアクセスで，サービスを停止させるなど不正行為を行うことが可能である．

（3） 侵入

脆弱性を突く攻撃は，システムへの侵入の手段にも利用され，侵入により不正なプログラムが実行されるという攻撃につながる．他に，正規の権限を持つ者が侵入して内部犯罪を引き起こすという攻撃も含まれる．

以上のような分類のうち，攻撃ではない（悪意のない）大量アクセスへの対処は，サーバのクラスタリングなど性能拡張などで行うべきものであり，セキュリティ上の問題ではない．また，正規の権限を持つ者の侵入による内部犯罪は，システム運用や利用の規約によって対処すべき運用上の問題であり，システム構築時におけるセキュリティ対策の対象から除外される．以上よりシステム構築者による対策が必要になるのは，輻輳攻撃，脆弱性攻撃，脆弱性を利用した侵入であり，これらの分類を図示すると図 1 のようになる．

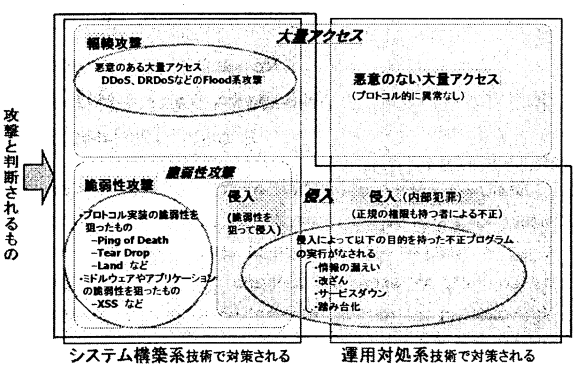

図1 公開サービスが受ける攻撃の種類

2.2. 被害の分類

前節で整理した攻撃によって，公開サービスが受ける被害の種類を，以下の四つに分類した．

（1） パフォーマンスダウン

想定された性能を凌駕する処理要求により，公開サービスが本来のレスポンスを維持できなくなるという被害になる．主な原因は，輻輳攻撃であり，ネットワーク帯域や攻撃対象ホストの処理能力を，無意味な通信で飽和させることによって，パフォーマンスダウンに至らしめる．

（2） サービスダウン

公開サービスで機能すべきサービスが提供できないという被害になる．主な原因は，輻輳攻撃や脆弱性攻撃であり，公開サービスに対して異常に

高い負荷を与えたり，脆弱性を利用して侵入後に不正なコマンドを実行したりする手段によって，サービスダウンに至らしめる．

（3） 情報漏えいや情報改ざん

公開サービスが本来提供すべきではない情報が外部に漏洩したり，提供している情報の内容が意図とは異なって改ざんされたりする被害になる．主な原因は，内部犯罪を含め侵入によるものであり，侵入後に不正なコマンドを実行し，情報漏えいや情報改ざんに至らしめる．

（4） 踏み台化による信用失墜

公開サービスそのものへの被害は無いが，公開サービスが他の公開サービスへ攻撃するための踏み台となることで，攻撃の共犯者にさせられるという被害になる．DDoS 攻撃を実行するためのエージェント化がこれにあたる．踏み台化されることにより，その公開サービス運営者や組織の信用や評判が失墜する．

以上を整理したものを，表１に示す．

表1 被害の種類

	直接的な被害 直接にサービス運用が妨害される		間接的な被害 サービス運用妨害の加担者に仕立て上げられ、社会的信用が失墜する
攻撃種類	・輻輳攻撃	・脆弱性攻撃 ・侵入（脆弱性を狙って）	・侵入 ・脆弱性を狙って侵入 ・内部犯罪としての侵入 ・脆弱性攻撃
被害内容	・ネットワーク高負荷 ・ホスト＋サービス高負荷 ・パフォーマンスダウン ・サービスダウン	・脆弱性を狙った攻撃 ・サービスダウン ・侵入 ・不正コマンドの実行 ・情報漏えい ・改ざん ・サービスダウン	・侵入（脆弱性を狙う、内部犯罪） ・脆弱なプログラムの想定外利用（SMTP フォワードなど） ・攻撃基エージェント化 ・攻撃中継エージェント化

一般的なDoS攻撃の範囲

3. 既存技術

本章では，第二章で分析された公開サービスの脅威を受けて，現状では技術的にどのような対処がなされているかを調査した．その結果，現状の対策では十分対応できていない課題について明らかにした．

3.1. 既存技術による対策

既存技術による各種攻撃からの対策は，対策実施者の立場によって，大きく二つに整理できる．ひとつは公開サービス提供側が実施できるものであり，もうひとつは ISP（Internet Service Provider）といったネットワークプロバイダが実施するものである．それら立場による具体的な対策内容を，以下に整理する．

（1） 公開サービス提供側による対策

一般的には，ファイアウォールや IDS（Intrusion Detection System），IDP（Intrusion Detection and Prevention）を使ったシステムである．外部インターネットと公開サービスの間に配置され，攻撃のパターンなどをシグネチャで定義したり（シグネチャベース型）通信の異常性を捕捉したり（プロトコルアノーマリィ型）するなど，通過するパケットの挙動を観察することにより攻撃を検知し，攻撃と種別された通信のフィルタを行う．脆弱性攻撃や進入に対しての通信のフィルタは，主にパケットの遮断を実施するが，輻輳型攻撃に対してはさらに帯域制御や回線増強，サーバクラスタ化が実施される．その他，syncookies やコネクションキュー制限など，攻撃対象ホストそのものに対して直接対策を施すものがある．

（2） ネットワークプロバイダ側による対策

ネットワークプロバイダが実施する対策の手法については，研究開発段階のものから，実際に提供されて ISP のサービスメニュになっているものまで各種存在する[2][3][4][5][6][7]．共通する特徴としては，ネットワーク機器そのものあるいはネットワークにアタッチされた専用機器によって攻撃を検知し，広域分散されたネットワーク機器が連動してネットワークへ流入する攻撃パケットを遮断，あるいは帯域制御するものである．攻撃検知の手法は，一般の IDS と同様のものを使うことが多いが，多地点に及ぶトラフィックの挙動を観察したデータが共有できることから，公開サービス提供側のみで行う検知よりも，より精度の高い検知が可能になる．特に，広域分散されたホストからの DDoS 攻撃に対する効果が期待できる．

3.2. 既存技術の課題

未知の脆弱性をついた攻撃や，その脆弱性を利用した侵入は，公開サービス提供側でもネットワークプロバイダ側でも，シグネチャが作成されていないため攻撃を検知できず，正規のアクセスとして区別される．対策として，早急なシグネチャの作成と適用が求められるが，シグネチャが適用されるまでの間は無防備な状態である．

輻輳攻撃においては，公開サービス提供者やネットワークプロバイダが帯域制御を行うことによって輻輳を緩和しシステムを守る対処がなされるが，リロード攻撃などは正規の手順によりアクセスする攻撃であるため，無作為な帯域制御は本来の正規アクセスまで同時にパフォーマンス低下を引き起こすという弊害がある．特に，公開サービス提供側による帯域制御は，DMZ などファイアウォール内部のホストへの攻撃は緩和できるが，ファイアウォールと外部ネットワークの接点における輻輳は回避しにくいものとなっている．その点，ネットワークプロバイダ側で実施する輻輳攻撃対策は，パケットを中継するホップ数から見て攻撃ホストに近い位置でトラフィックの遮断あるいは帯域制御

を試みることができるため，効果的である．ただし，広域にわたる攻撃検知は研究段階にあるものも多く，実際にはISPのサービスとして提供されていない場合が多い．また，ISPが異なると攻撃の検知や遮断といった動作の連携がされず，協調して動作する機能を多くのネットワークノードで導入しなければ効果が薄いため，コストが高くなる．

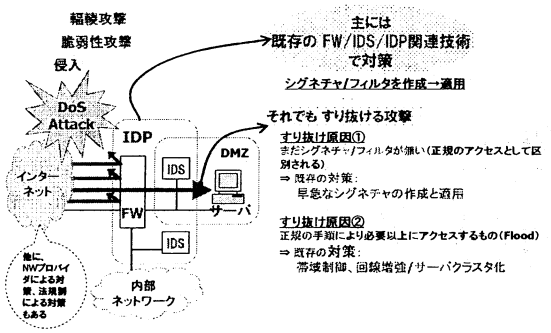

図2 公開サービス提供者の既存技術による対策

以上から，大別すると以下の二点が既存技術の課題と考えられる．

（1） 未知の脆弱性をついた攻撃や侵入に関して

シグネチャの適用が完了するまでの間，効果的な対策がない．

（2） 輻輳攻撃に関して

協調動作の点で課題があるものの，ISPによる効果的な対策は期待できるが，公開サービス提供側のみによる効果的な対策はない．

これら二つのうち，本稿では，特に公開サービス提供側のシステム構築者の立場から，まずは輻輳攻撃に対する対策を課題として設定し，公開サービス提供側のシステムのみで実施できる輻輳攻撃に対する仕組みを，輻輳型DoS攻撃回避方式として提案した．

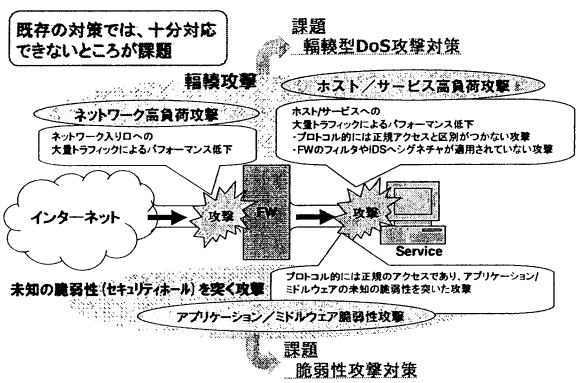

図3 既存技術の課題

4. 輻輳型DoS攻撃回避方式

本稿が提案する輻輳型DoS攻撃回避方式は，公開サービスを提供しているシステム側のみで実施できることが特徴である．これにより，ネットワークプロバイダが，輻輳型DoS攻撃への有効な対策を施せない場合にも対処できる．

4.1. 輻輳型DoS攻撃回避方式の基本概念

公開サービスを提供しているサイトは，公開されたグローバルIPアドレスを持っており，インターネット上からアクセス可能な状態である．これらの公開サービスに対して攻撃パケットを送りつけることは容易であり，悪意を持ったパケットでもISPがそれを検知しフィルタをかけない限り，グローバルIPアドレスすなわち公開サービスへパケットが到達することを防ぐことができない．そこで，公開サービスのグローバルIPアドレスを不定にし，そもそも攻撃先のIPアドレスを分からないようにして攻撃が来ないようにするという対策案がある．

この対策案の具体的手法の例として，IPv6のPrivacy Extensions[8]や，製品として米Invicta社のInvisiLAN[9]，類似の手法としてはDynamic DNS[10]などがある．IPv6 Privacy Extensionsでは，グローバルIPアドレスごと変更されるもので，IPアドレスは不定であるが，公開サービスへの新規接続要求者にとって不定であるだけで，既に接続されているコネクションは切断されるまで接続に使ったIPアドレスを変更せずに維持するものとなっている．したがって，一度接続してグローバルIPアドレスを得た攻撃者は，引き続きそのアドレスを使用して攻撃を継続することができるものとなっている．また，InvisiLANにおいては，専用のハードウェアを使い，VPN接続に使用しているIPアドレスを不定にすることが主な目的であり，公開サービスを守るための対策となっていない．Dynamic DNSは，IPv6 Private Extensionsと同様，公開しているグローバルIPアドレス（以後公開IPアドレス，またはPIPアドレス，またはPIPと記述する）ごと変更されるもので，新規接続要求者にとって不定になっている．さらに，Dynamic DNSでは公開IPアドレスが変更になると，接続していたコネクションは維持できない．

本稿で提案する輻輳型DoS攻撃回避方式では，公開サービスのIPアドレスを不定にする手法にMobile IPv6[11]の技術を応用している．公開サービスを提供しているサーバがMobile IPv6を改造したプロトコル実装を搭載したものになっており，公開IPアドレスは一定でも，実際にアクセスできるアドレスが任意のアドレスに可変であるという基本的な概念を持つ．つまり，公開IPアドレスは，モバイルIP技術のCoA（Care of Address：気付アドレス）に相当し，PIPを持つHA（Home Agent，Mobile IPを構成する機能のひとつ）によってインターネット上に公開されるが，実際にアク

セスするために必要な移動 IP アドレス（以後 MIP アドレス，または MIP と記述する）は，物理的な移動を伴わずともサーバ側で任意に設定できるようにするものである．任意に変更されるサーバのアドレスは，Mobile IPv6 で規定されている Binding Update(以後 BU と記述する）という仕様により，IP 層のプロトコルで接続要求者や既接続者に通知される．これにより，初期の接続要求者のみならず，既にコネクションが確立されているユーザと公開サービスとの間の通信も自動的に維持できるようになる．さらに，IP 層のプロトコルであるため，上位のプロトコルやアプリケーションは，公開 IP アドレスにアクセスしているのとまったく同じ動作で良く，クライアントは基本的に Mobile IPv6 に対応するのみで良いという利点がある．特に，BU を利用することにより，送信元 IP アドレスが実際の送信元ノードのアドレスと異なる場合，BU の通知が到達しないため，送信元アドレスを偽った攻撃者からのパケットは確実に回避することができる．

また，BU に伴う Return Routability（以後 RR と記述する）という Mobile IPv6 標準の簡易認証方式を利用することにより，むやみに BU されることを防ぐ手段も用意されている．さらに，ユーザ端末は Mobile IPv6 に対応するのみで，既存システムへの改造は公開サービス提供側のみで実現できるように配慮した．

他に，公開サービスそのものが擬似移動体として BU を行う以外，公開サービスの代わりに BU や RR を実施する機器を Binding Update Agent（以後 BUA と記述する）として設ける．これにより，既存の公開サービスに手を加える必要がないといったメリットがある．

以上のような輻輳型 DoS 回避方式を，公開サービス提供側のシステムに組み込むことにより，輻輳型 DoS 攻撃を行うノードの送出パケットが，公開サービス提供側サイトに到達しなくなり，輻輳型 DoS 攻撃を効果的に緩和することができると考えられる．

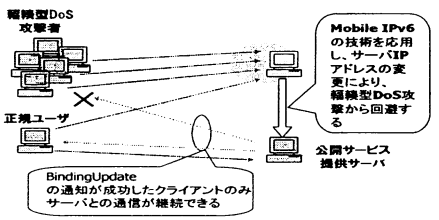

図4 輻輳型 DoS 回避方式基本概念

4.2. 機能構成と機能間の動作関連

輻輳型DoS攻撃回避方式を実現するための機能構成を，図5に示す．機能間の動作関連を，図6と図7に示す．図6では公開 IP アドレスへのアクセスに対して，図7では移動 IP アドレスへのアクセスに対して，それぞれ関連する動作を示している．

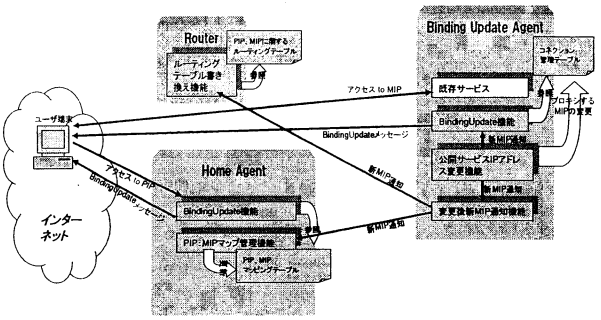

図5 機能構成

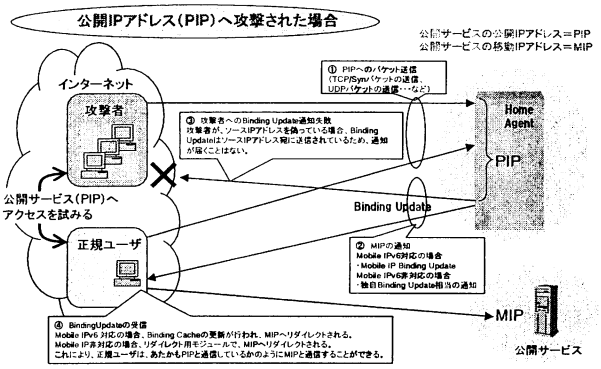

図6 公開 IP アドレスへのアクセス時

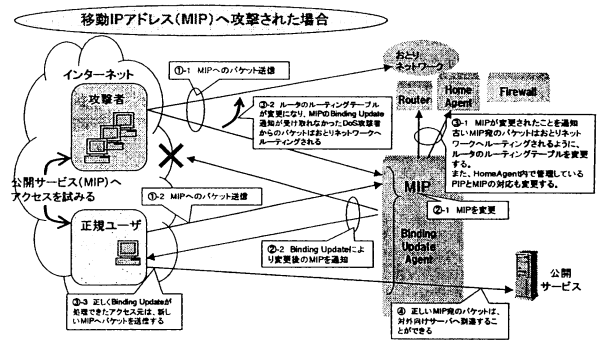

図7 移動 IP アドレスへのアクセス時

4.3. 基本動作

輻輳型 DoS 攻撃回避方式の基本的な動作フローを，図8と図9に示す．図8では，ユーザ端末と HA 間，図9ではユーザ端末と BUA の間の動作を記述する．

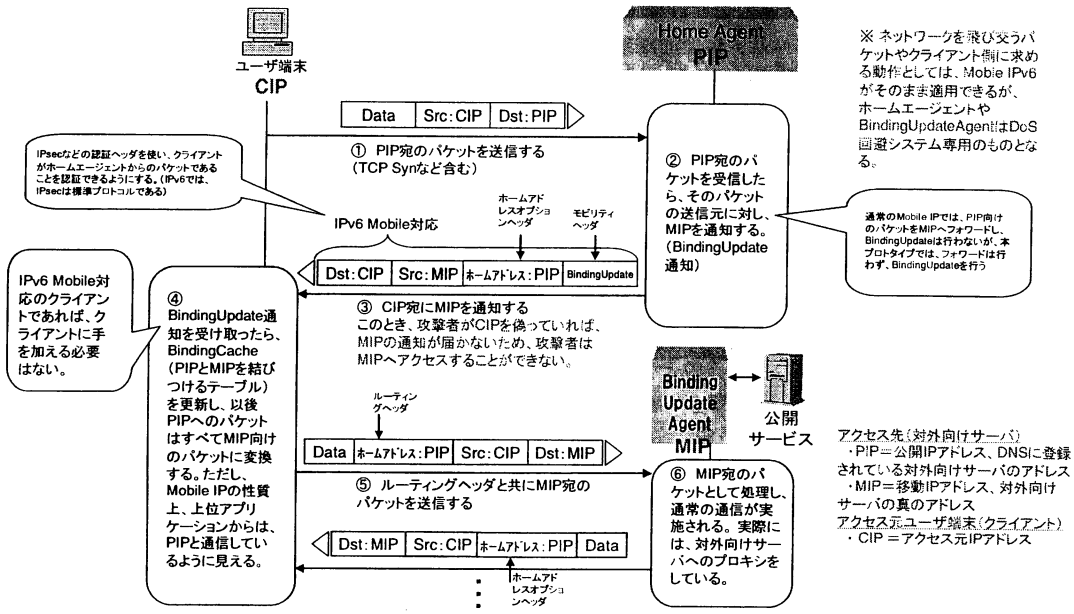

図8 ユーザ端末-HA 間 動作フロー

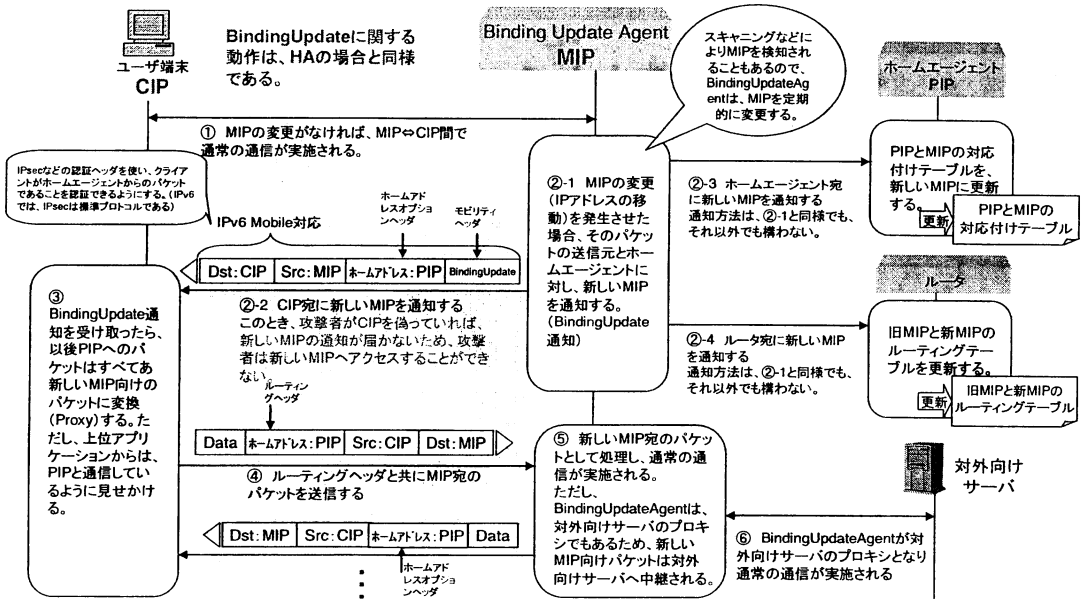

図9 ユーザ端末-BUA 間 動作フロー

5. 輻輳型 DoS 攻撃回避方式の動作検証

第四章にしたがって本方式のプロトタイプを作成し，動作検証を行った．

5.1. 動作検証項目

動作検証項目は，大きく以下の三項目を確認することとした．なお，以下の正規ユーザとは，BU を受信して正しく処理できる Mobile IPv6 に対応した機器のことをいうものとする．

（1） 正規ユーザであれば PIP から MIP へ接続が誘導されることの確認

ユーザ端末が PIP へアクセスすると，BU によって自動的に MIP へ送信パケットが誘導され，MIP と接続される．正規ユーザのアプリケーションでは PIP と接続していると認識されており，MIP と接続されていることは意識されない．

（2） MIP を変更しても変更先の MIP と通信が維持されることの確認

MIP を任意のタイミングで変更しても，正規ユーザ端末は変更後の MIP と自動的に再接続され，コネクションが維持される．正規ユーザのアプリケーションは，MIP が変更されたことを意識せず，通信は継続される．

（3） 非正規ユーザからのアクセスは回避できることの確認

非正規ユーザ（攻撃者）は，PIP へアクセスしても MIP に接続することができない，あるいは，MIP へアクセスしても MIP が変更されると変更された MIP へ接続できない．MIP を持つ公開サービスが，正規ユーザと非正規ユーザから同時に連続してパケットを受信しているとき，MIP を変更すると，正規ユーザのみ接続が維持できる．

5.2. 検証環境

正規ユーザ端末と非正規ユーザ端末が，PIP あるいは MIP へパケットを送信できるようなネットワーク環境を構築し，正規ユーザは FTP により PIP に対して継続的にファイル転送を行うようにする．このとき，公開サービス提供側では，BUA による MIP の変更が任意に行えるものとする．非正規ユーザは，FTP または UDP パケットの一方的な送信を，PIP または MIP に対して行えるようにする．以上のような検証環境を構築した。

5.3. 検証結果

先の検証方法に基づき，動作検証項目を確認した結果，第四章で考案した輻輳型 DoS 攻撃回避方式は，検証項目すべてが期待どおり動作できるものであることを確認した．

ただし，正規ユーザによる PIP へのアクセスから MIP への接続までのシークエンスは，TCP など上位プロトコルの再送や継続的なアクセスに依存するものとのなっており，最初のパケット（TCP の SYN パケットなど）は必ず欠落するものとなっている．つまり，HA が受信する最初のパケットは BU によって誘導するためのトリガとなって廃棄され，BU が成功すればその後のパケットから MIP へアクセスできる動作となっている．これは，ユーザ端末が Mobile IPv6 標準の動作に従うだけで対応できるようにしたことと，最初のパケットは攻撃であると仮定した性悪説的な対処としたことによるが，SYN Flood のような攻撃を想定するとやむを得ない動作と考える．そのため，TCP の初期の接続において，再送を見込んだ接続遅延（Linux FedoraCore1 における実測で約 3 秒程度）が発生する．

また，MIP アドレス変更の仕組みに伴って，IPv6 アドレスの自動構成機能をそのまま使用している．これにより，MIP を任意に変更しても，IPv6 アドレス自動付与に伴う一連の動作が実施されるなど，ユーザ端末に変更後 MIP が通知されるまでのシークエンスは多くなっている．このため，MIP 変更後の再接続には，実測で約 6〜8 秒程度の時間がかかっている．なお，再接続には，Router Advertisement や Neighbor Discovery など Mobile IPv6 以外に必要なプロトコルの動作も含まれており，特に，MIP を持つ BUA が擬似的にセグメントを移動するためにルータの再設定を行う手順や，Router Advertisement の送出間隔が，再接続に要する時間を引き延ばしている原因と予想される．

6. 今後の課題

機能面を中心に，プロトタイプの動作検証を行い，機能的には輻輳型 DoS 攻撃回避方式が動作可能であることを確認できたが，以下の三つの項目において，課題があると考えられる．

（1） 性能向上

Mobile IPv6 では，BU に必要な認証プロトコルとして RR が標準で動作する．このとき，HA が輻輳型 DoS 攻撃を受けている最中，RR 用のパケット（HOT：Home Test と，COT：Care-of Test）が輻輳状態の回線を通らなければならないことがある．BU に必要なパケットが輻輳状態の回線を通ってしまうと，BU 自体が大幅に遅延することが懸念される．これは，再接続に大幅な時間がかかる可能性があることを意味する．ただし，動作検証においては，公開サービスへのアクセスに遅延が発生するほど効果的な輻輳型 DoS 攻撃を実施することができなかったため，BU の遅延現象は確認できなかった．以上のような予想される性能低下を防ぐために，BU や RR は，HA とは別のセグメント（攻撃を受けていないセグメント）から実

施するという対策案が考えられる．特に，HA は PIP を扱っている関係上，輻輳型 DoS 攻撃を受け続けることになるが，BUA は回避機能があるので，HA の実施する BU や RR もすべて BUA が実施するという方法が，改良案の候補として考えられる．

（2） 認証高度化

現状，BU を行うユーザ端末を認証するのに，RR を利用している．この RR は，ユーザ端末やサーバのソースアドレスを保証するための簡易認証方式であるが，これによって，悪意を持った BU 送信者によってユーザ端末の接続先が強制変更されてしまったり，不正に BU を受信することによって公開サーバの回避先が知れてしまったりする，セキュリティ面の危険性を払拭することはできないものとなっている．そこで，今後の課題として，Mobile IPv6 の仕様とは別に，IPsec などを使って，ユーザ端末と公開サービス間の相互認証に関する高度化が必要になるものと考える．

（3） 実用性向上

BU は，Mobile IPv6 では必須の機能となっているが，IPv4 には存在しない．将来 IPv6 に移行することが見込まれているが，実用面を考慮すると，現状の IPv4 にも対応させる必要がある．しかし，Mobile IPv4 では BU に相当するプロトコルが存在しないため，本稿で考案した方式の適用は困難である．そこで，今後の課題として，BU と同様の機能を IPv4 に実装し，かつ JAVA アプレット化や Plug-In ツール化など，ユーザ端末で簡便に利用できる仕組みを考案することが実用上必要になるものと考える．

7. まとめ

本稿では，公開サービスが受ける脅威を整理し，既存技術で対応できるところと対応が不十分なところを整理した．さらに，対応が不十分な輻輳型 DoS 攻撃について，Mobile IPv6 を応用した回避方式を提案し，プロトタイプを作成した．プロトタイプでは，BU が受信できない攻撃端末からのアクセスを回避し，正規ユーザからの接続は回避動作後も維持できることを，動作検証にて確認した．ただしその検証において，性能面，セキュリティ面において課題が見出された．

今後は，新たに提起された課題について，対処案を考案，さらに検証し，本方式がより効果的になる方策を検討したいと考える．

参考文献

[1] Cyber Defense 社，“CyberNotice Intelligence Reports”，iDEFENCE，2003-2004

[2] 田村直弘 他，“DDoS 攻撃回避システムの開発”，IPSJ SIG Technical Report 2004-CSEC-24，pp.133-138，（社）情報処理学会，Mar.2004

[3] “Moving Firewal”，http://www.ntt.co.jp/news/news03/0302/030218.html，

[4] Ratul Mahajan, Steven M. Bellovin, Sally Floyd, John Ioannidis, Vern Paxson, and Scott Shenker. “Controlling high bandwidth aggregates in the network.” Technical Report, AT&T Center for Internet Research at ICSI, July 2001.

[5] David K.Y. Yau, John C.S. Lui, and Feng Liang. “Defending against distributed denial-of-service attacks with max-min fair server-centric router throttles.” In Proc. Of the IEEE International Workshop on Quality of Service, p35-44, May 2002.

[6] Kalman K.K. Wan and Rocky K. C. Chang. “Engineering of a global defense infrastructure for DDoS attacks.” In Proc. of the IEEE Symposium on Security and Privacy, May 2003.

[7] “AT&T DDoS Defense”, AT&T Internet Protect, http://www.att.com/news/item/0,1847,13096,00.html

[8] “Privacy Extensions for Stateless Address Autoconfiguration in IPv6”, IETF RFC 3041, January 2001

[9] InvictaNetworksInc., “InvisiLAN”, http://www.invictanetworks.com/invisilan.html

[10] “Secure Domain Name System (DNS) Dynamic Update ”, IETF RFC3007, November 2000

[11] “Mobility for IPv6”, http://www.ietf.org/html.charters/mip6-charter.html