NEWS RELEASE

NTT

日本電信電話株式会社

２００３年2月１８日

攻撃元にまで攻め上がりながらネットワーク全体を防御する DDoS攻撃対策システム「Moving Firewall」を開発

―攻撃を局所的に封じ込めて一般の利用者の通信を確保―

日本電信電話株式会社（以下ＮＴＴ、本社：東京都千代田区、代表取締役社長：和田紀夫）は、ネットワークに接続された複数のコンピュータを使い、特定のサーバあるいはネットワークをサービス不能状態に陥らせる、「分散サービス停止攻撃（DDoS攻撃*1）」からネットワーク全体を守るDDoS対策システム「Moving Firewall」（以下、MovingFW）の試作品を開発しました。

このMovingFWは、攻撃を“点”で防御する従来のDDoS対策ツールとは異なり、ひとたび攻撃を察知すると攻撃元（複数）にまで“攻め上り”ながら、ネットワークに侵入しようとするDDoS攻撃パケットを遮断し、ネットワーク全体の防衛を可能にするシステムです。

ＮＴＴでは、昨年１１月に「“光”新世代ビジョン：ブロードバンドでレゾナントコミュニケーションの世界へ」を策定し、その実現に向けた研究開発に積極的に取り組んでいるところです。今回開発したMovingFWも次世代ネットワークアーキテクチャ（Resonant Communication Network Architecture: RENA）の実現に向けた研究開発の一環です。

＜開発の背景と目的＞

DDoS攻撃による被害は年々増加の一途をたどっており、2002年10月にも全世界のインターネットの基幹システムをなす13台のドメインネームサービス(DNS)ルートサーバに対するDDoS攻撃が発生しました。また、本年１月下旬にはウィルスに起因した世界的規模でのインターネット障害の発生が確認されています。このようなサイバー攻撃は、インターネットが停止することにもつながりかねない重大な危険性をはらんでいます。しかし、現在一般的に利用されているファイアウォールを使った“点”での対策では、攻撃トラヒックによるネットワークの輻輳を防ぐことはできないため、このような大規模なDDoS攻撃を防ぐことは全くできません。

ＮＴＴ情報流通プラットフォーム研究所が新たに開発したMovingFWでは、

ネットワーク全体での“面”での防御と、詳細なトラヒック分析を行うことにより、“点”での防御では困難だった一般ユーザのための通信路（あるいは帯域）を確保し、DDoS攻撃を阻止することが可能になります。

こういった特徴から、MovingFW をISP*2などのネットワーク事業へ適用することにより、一般の利用者が安心してネットを利用できるようになります。さらに、様々なサービスを提供するビジネスWebサイトでは、安心してネットビジネスを展開できるようになると期待されます。

＜主な特徴＞

(1) ネットワーク全体の防御

MovingFWは、攻撃元近くの多地点へ攻撃防御機能を展開する“面”での防御により、攻撃対象のサーバだけではなく、ISP等のネットワーク全体を輻輳から守ることができます。DDoS攻撃では、送信元アドレスを偽装して攻撃元の分析を困難にする方法が多く用いられています。Moving FWは、このような方法に対しても攻撃元近くへ“攻め上がる”ことが可能です。

(2) 一般ユーザの保護

多地点へ展開したMovingFWは、各々詳細なトラヒック分析を行い、Webサイト運営者やサーバ管理者のサービスポリシーに応じて、攻撃パケットを正確に分離する仕組みとなっているため、従来の“点”での対策で発生してしまう「一般ユーザの遮断」を回避し、一般ユーザはサービスを使い続けることが可能になります。

(3) フレキシビリティに富んだ対策システム

アクティブネットワーク技術*3を採用しているため、新たな攻撃が登場した場合でも、MovingFWプログラムの書き換えが即座に行えるため、迅速な対応が可能です。

＜システム概要＞（別紙参照）

MovingFWのシステムは、Moving FW管理システム、Moving FWソフトウェア、MovingFW装置から構成され、それぞれの役割は以下のとおりです。

(1) MovingFW管理システム

MovingFW装置への設定、DDoS攻撃の状況や攻撃抑止の状態などを視覚的に表示します。

(2) MovingFWソフトウェア

防御対象のWebサイトやサーバに最も近いMoving FW装置にダウンロード

され、攻撃を監視します。攻撃検出や防御の基準は、サイト運営者等のサービスポリシーに応じて自由に設定できます。攻撃を検出した際には、自動的に攻撃の防御を開始すると共に、攻撃上流のMoving FW装置に向かって、攻撃パケット識別情報を含むプログラムコードを自動複製し送りつけます。この連続により、攻撃元にまで“攻め上って”、DDoS攻撃パケットを制圧することができます。

(3)　Moving FW装置

アクティブネットワーク技術を採用し、MovingFWソフトウェアを実行するブリッジ装置*4です。

＜今後の予定＞

現在、試作品で効果を確認しておりますが、今後は2005年を目途にレゾナントコミュニケーション環境の実現に向けて必要となる次世代ネットワークアーキテクチャ（RENA）に適用することを狙いとして継続的に研究を進めていく予定です。当面は、攻撃手法とネットワーク構成により様々な挙動を見せるDDoS攻撃の防御の効果を、実証実験を通して、実ネットワークで検証して行く予定です。

【用語解説】

*1：DDoS攻撃 (Distributed Denial of Service)

ウィルスなどを使って乗っ取った多数のコンピュータを踏み台として、標的とするコンピュータに大量のパケットを送りつけて、サービスを停止させてしまう攻撃。

*2：ISP (Internet Service Provider)

インターネット接続事業者。電話回線やADSL回線、データ通信専用回線などを通じて、顧客である企業や家庭のコンピュータをインターネットに接続するサービスを提供する。

*3：アクティブネットワーク技術

ネットワークのサービスを柔軟に変更するための技術であり、ルータ等のネットワーク機器上でプログラムを走行させるミドルウェアと、プログラムを移動させるためのプロトコルで構成される。

*4：ブリッジ装置

ネットワークでパケットを中継する機器。OSI参照モデルでいうデータリン

ク層(第2層)の中継機器であり、ネットワーク層(第3層)のルーティングには影響を及ぼさない。

・（別紙）Moving Firewallシステムの概要

【本件に関するお問い合わせ】
ＮＴＴ情報流通基盤総合研究所
企画部　広報担当　飯塚、佐野、池田
TEL：0422-59-3663
E-mail：koho@mail.rdc.ntt.co.jp

NTT ニュースリリース

Copyright(c) 2003 日本電信電話株式会社