NEWS RELEASE

NTT

日本電信電話株式会社

2005年10月18日

インターネットのサイトを保護する
次世代DDoS対策システムの米国トライアルについて

～Moving Firewall技術の有効性を実地検証、年度内での実用化にめど～

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、データセンタや企業が設置するインターネット上のサイトをISP（※1）と連携して、DDoS攻撃（※2）から守る防御システム（以下、本システム）のトライアルを米国で実施しました。本システムは、DDoS攻撃をネットワーク全体で連携して自動的に防御するために、ＮＴＴ情報流通プラットフォーム研究所が開発している次世代のDDoS対策技術Moving Firewall（※3）を応用したものです。

DDoS攻撃を防御するためには、攻撃を受けている企業やデータセンタ側（以下、ユーザ側）がＩＳＰ側のネットワークと連携して対処することが重要です。本トライアルでは、ユーザ側が自主的にネットワーク側と連携して攻撃を防御する仕組みをMoving Firewallで実現し商用環境で確認しました。

DDoS攻撃が多発している米国のＷｅｂサイトにおける今回のトライアルは、既にDDoS攻撃対策で豊富な経験とノウハウを持っているNTTコミュニケーションズの米国子会社ヴェリオ社（http://www.verio.com/）の協力を得て実施しました。

＜トライアルの背景と結果＞

電子商店やインターネット銀行など、ネットワークを活用した便利なサービスが身近な存在になる一方で、インターネットの安心・安全を脅かす犯罪行為が多発しています。

中でも、悪意の大量パケットでネットワークやサーバの機能を麻痺させてサービス提供を不可能にするDDoS攻撃の被害は年々増加の一途をたどっており、例えば2004年には、蔓延したMyDoomワームが仕掛けたDDoS攻撃により米国のあるWebサイトがアクセス不能状態に陥りました。

現在、一般的なセキュリティ対策によく用いられているファイアウォールでは防御できないこうしたDDoS攻撃が、特に多発している米国においては、対策用の製品やサービスなどのDDoS対策関連市場が今後大きく伸びると予想されています。しかしこれらの製品は、攻撃の検出や対策など個々の機能はある程度実現しているものの、これらをお客様とISPが連携して実施するケースを

想定しておらず、オペレーションが複雑になってしまいます。さらに、攻撃元と攻撃先が同じＩＳＰ内や同じ国内に閉じるケースはまれで、複数事業者や国境をまたいだ攻撃が一般的になりつつあります。このような攻撃が多発化・日常化するにつれ、攻撃対処のオペレーションをできるだけ自動化・省力化したい、あるいは複数事業者間で連携して対処したい、という要求が今後高まってくると予想されます。

NTTでは、DDoS攻撃がまだ深刻な社会問題化する以前の段階から、ネットワーク全域で攻撃を防御するMoving Firewallのプロトタイプを開発し、その有効性を検証してきました。この度の米国トライアルでは、データセンタとネットワークそれぞれにプロトタイプを設置し、複数マシンから行われた数千規模のホスティングユーザに影響を与える攻撃への対処に成功するなど、データセンタのサーバ等への被害を効果的に軽減できることを確認しました。

また、本来データセンタや企業は、それぞれのポリシーに基づき、Ｆｉｒｅｗａｌｌや侵入検知システムなど各種対策システムを用いて、セキュリティ対策を行っています。DDoS攻撃への対処についても、最終的にはユーザ側の判断でその実施をコントロールできることが重要です。そこで本トライアルでは、ＩＳＰ側から対処策を提示し、ユーザ側で実施を選択するインタフェースをポータルで提供しました。

＜トライアルの概要＞

トライアルは以下の要領で実施しました。

（1）実施形態

Moving Firewall技術を利用した「DDoS対策システム」を、ヴェリオ社における日常のDDoS対策オペレーションと併用してもらい実用性を確認

（2）実施場所

米国内データセンタおよびネットワークで実施（計3システム配備）

（3）実施期間

2005年4月～同年7月

＜技術のポイント＞

DDoS攻撃の検知をユーザ側で、防御をISPの攻撃元に近い場所で、それぞれ連携して行うためには、ユーザ側とISP側（ときには複数事業者にまたがる）との間で、攻撃情報の共有、対策依頼の送受信、依頼の承認・妥当性の判断・通知、対策の実施・結果のフィードバック、といった一連の処理を行う必要があります。

本システムでは、構成する複数の攻撃検出装置および防御装置が連携動作することで、このような複数の組織や事業者にまたがる一連のDDoS対策処理をサポートします。特に、ユーザ側の攻撃検出装置とネットワーク側の防御装置が連携してユーザとISPネットワークを結ぶアクセス回線の輻輳を救済できることへの期待は大きく、他の市中技術と比べた場合の特徴となっています。

＜今後の展開＞

今回の米国トライアルは、NTTが提案する次世代DDoS対策システムの有効性と共に、ネットワークセキュリティに対して複数事業者が連携することの重要性を証明するものです。ＮＴＴでは今後、Moving Firewall技術の開発過程で培った事業者間連携・装置間連携のインタフェース規定・ノウハウをさらにブラッシュアップさせ、事業会社のサービスを通して、広く世の中に利用頂くための活動を進めていきます。

さらに、日本においても同様の脅威の増加傾向が見られることから、トライアルで実証された機能の一部（特に攻撃検出機能）をさらに低コストで実現できるよう改良し、今夏からNTTグループの商用ネットワークやデータセンタにおいて試験評価を開始しており、年度内での実用化を目指しております。

また今後の課題として、ウイルス・ワームなど各種セキュリティ脅威への対策やＷｅｂサーバの負荷監視など、より広義のセキュリティ対策技術と連携させることで、異常トラフィックやサーバ攻撃に対して高精度かつ迅速に対処する技術へ発展させていくための研究開発を行っていきます。

＜用語解説＞

※1　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。

※2　DDoS (Distributed Denial of Service)攻撃

分散サービス停止攻撃。ウィルスなどを使って乗っ取ったサーバを踏み台とし、標的とするサーバ（電子商店、インターネット銀行など）に大量のパケットを送りつけて、正常なサービスを行えないように妨害する攻撃。

※3　Moving Firewall

自動的に悪意の通信を検出して攻撃元を追跡することで、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、正規利用者の通信を保護することで、ネットワーク全体の“安心・安全”な運用を可能にするシステム。

・[別紙]　Moving Firewallを利用したDDoS対策オペレーションの実証実験

【本件に関するお問い合わせ】

日本電信電話株式会社
第三部門プロデュース担当

舘（たち）
電話：　03-5205-5390
E-mail: security-p@ml.hco.ntt.co.jp

NTT ニュースリリース