

[導入事例]

DDoS攻撃に対する防御をサービス化 そのための機器としてCisco Guard XT 5650を採用

NTTコミュニケーションズ株式会社



“グローバルIPソリューションカンパニー”として国際的な大規模ネットワークを構築すると共に、多様な高付加価値サービスを開拓し続けているNTTコミュニケーションズ。ここではその一環として、2005年11月よりDDoS攻撃検知サービス「DDoSファインダー」を提供中だ。さらには2006年3月末までにDDoS攻撃に対する防御機能をサービス化し、「DDoSディフェンダー」として提供開始する計画になっている。このサービスを提供するための実現技術としてNTT持株研究所のR&D成果と共に中核に位置するのがCisco Guardだ。複数のベリフィケーションプロセスによる効率的なトラフィックのチェック機能や、ソフトウェアで実現されたきめ細かい処理、スイッチとの統合によって実現されたスケーラビリティなどが高く評価されている。NTTコミュニケーションズではDDoS攻撃防御を目玉サービスのひとつに位置づけ、グローバルに展開していく予定。また新たな攻撃にも対応できる仕組みを作り上げるため、シスコとの協業も強化していくという。

●導入の背景/課題

- ・DDoS攻撃への対応は、できるだけネットワークの上流で行う方が効率的であり、上流ISPとのリンク輻輳などお客様サイドでは対応が難しい点もあれば社内オペレーターから指摘されていた。
- ・調査会社を利用した調査によって、顧客のほとんどがDDoS攻撃の被害を経験していることがわかった。
- ・DDoS攻撃の防御に対する潜在的なニーズは高いと判断、サービス化に踏み切った。

●導入ソリューション

- ・シスコセキュリティソリューション
-Cisco Guard XT 5650

●導入効果(期待される導入効果)

- ・バックボーンネットワーク内で攻撃防御を行えるため、顧客側での対応負担を軽減できる。
- ・攻撃パケットをドロップできるのはもちろんのこと、顧客のアクセス回線に向かうパケット量のコントロールも行えるため、アクセス回線での輻輳を回避できる。
- ・NTTコミュニケーションズにとっても、新たな付加価値サービスによって競争力を高められるというメリットがある。

被害額が大きいDDoS攻撃 その対応をシスコ製品でサービス化

手法の高度化や影響範囲の拡大に伴い、年々その被害額が拡大しているセキュリティ脅威。その具体的な内容としては、システムへの不正アクセスやシステムの乗っ取り、フィッシング詐欺など様々なものがあるが、損害額から見て最も重大なもののひとつとして挙げるべきなのが、DoS攻撃(Denial of Service Attack)であろう。

DoS攻撃とは、インターネット上の各種サーバーに対して無意味なサービス接続要求を大量に送りつけ、サーバー負荷を高めることでサーバーダウンなどを引き起こすというもの。この攻撃を受けたサイトは“正当なユーザー”に対するサービスを継続できなくなることから、日本語では“サービス不能攻撃”や“サービス拒否攻撃”などと呼ばれている。また最近では1ヶ所からDoS攻撃を行うのではなく、複数ヶ所から同時に大量のサービス要求パケットを送りつけるDDoS(Distributed DoS)攻撃も増えている。近年、DDoS攻撃によく使われるコンピューターに“ゾンビPC”がある、現在では数十万台のゾンビPCが存在し、毎秒数百万パケットという膨大なトラフィックによる攻撃も可能だといわれているのだ。

米国における情報セキュリティ被害の統計として発表されている「CSI/FBI Computer Crime & Security Survey」の2004年版によれば、この種の攻撃による被害額は2600万ドルを超えていると指摘されている。もちろん日本企業にとっても“対岸の火事”ではありえない。インターネットには国境がないため、どこから攻撃を受けるかわからないからだ。最近のインターネットサイトは単なる情報発信の手段にとどまらず、ビジネスの基盤として重要な役割を果たしている。このようなサイトにDDoS攻撃をかけられれば、その間ビジネスが止まってしまう、莫大な機会損失が発生することになる。

この問題に対応するため、シスコソリューションを活用したサービスの提供を決定したのがNTTコミュニケーションズである。同社は企業ユーザーや個人ユーザーに対してIP-VPNやOCN等のネットワークサービスを提供する、日本を代表するネットワークサービスプロバイダー。また日米間で49Gbps、アジア域内27Gbpsという世界最大規模のインターネットバックボーンを有する等、国際的なビジネス展開も積極的に展開している。2003年3月には“グローバルIPソリューションカンパニー”という事業ビジョンを発表。顧客にとって価値あるサービスを開拓することで、新たなマーケットを創造し続けているのだ。

DDoS攻撃に対する防御をサービス化
そのための機器としてCisco Guard XT 5650を採用
NTTコミュニケーションズ株式会社



「ネットワークを水道にたとえれば、これまでのDDoS攻撃への対応方法は各家庭で浄水するようなもの。しかしこれからは上流で浄水するのが必然的な流れになるはずです」

NTTコミュニケーションズ株式会社
グローバル事業本部
グローバルIPネットワーク営業部長
森林 正彰 氏



「日本では多くの企業が被害を申告せず、泣き寝入りをしている状況です。だからこそDDoS攻撃の防御をサービスとして提供しようと考えたのです」

NTTコミュニケーションズ株式会社
グローバル事業本部
新規事業開発部
グローバルインキュベーション担当課長
大和田 英俊 氏

「当社のネットワークには数多くのISPが接続されており、かなり大規模なものになっています」というのは、NTTコミュニケーションズ グローバル事業本部でグローバルIPネットワーク営業部の部長を務める森林氏。以前はこのネットワーク上で“トラフィックを確実に流す”ことを最重要課題としてきたが、ここ数年はいかに付加価値を高めていくかを重視するようになってきているという。たとえばIPv6とIPv4の両方に対応した“IPv6/IPv4デュアルサービス”を、2004年に世界で初めてグローバルに提供したのはその一例だと説明。またセキュリティの強化にも継続的に取り組んでおり、ファイアウォールやIDS（不正侵入検知）、SPAMフィルターなどのソリューションも他事業部で既に提供しているという。DDoS攻撃への対応サービスの実現も、その一環として進められているのである。



今回導入された Cisco Guard XT 5650

ほとんどの法人顧客が被害を経験 上流での攻撃阻止の必要性を確信

NTTコミュニケーションズが、DDoS攻撃への対応を検討し始めたのは2004年7月。そのきっかけになったのは、NTTコミュニケーションズ社内でネットワークオペレーションを担当しているスタッフからの指摘だったという。

「現在はDDoS攻撃への対応を各サイトが行っていますが、できるだけネットワークの上流で阻止した方がロスが少なくなります」と指摘内容を説明するのは、NTTコミュニケーションズ グローバル事業本部でグローバルネットワーク部 主査を務める水口氏。ネットワークの下流で阻止しようとしても、上流とのリンクのリソースは消費しているため、結局はその上流での対応が必要となる。「攻撃パケットを早い段階で食い止めれば、影響範囲も限定できるので対応が容易になります。また各サイトでの作業も不要になるため、必要な労力も削減できるのです」

しかしこの時点ですぐに、DDoS攻撃への対応をサービス化するという決断が下されたわけではない。NTTコミュニケーションズ グローバル事業本部で新規事業開発部 グローバルインキュベーション担当課長を務める大和田氏は「これまで存在しないサービスなので、本当に市場ニーズがあるのか、当初は確信がもてませんでした」と振り返る。また日本ではDDoS攻撃に関する被害報告が、米国に比べてそれほど多くなかったことも、サービス化を躊躇する要因のひとつだったという。しかし2005年2月にこの空気は一転する。調査会社を使って実施したマーケティング調査の結果、ほとんどの法人顧客がDDoS攻撃を受けた経験を持つことが判明したからだ。「日本では多くの企業が被害を申告せず、泣

**DDoS攻撃に対する防御をサービス化
そのための機器としてCisco Guard XT 5650を採用
NTTコミュニケーションズ株式会社**

き寝入りをしている状況だということがわかりました。それならばぜひサービス化に踏み切るべきだと判断したのです」

NTTコミュニケーションズが提供を予定しているDDoS攻撃対応サービスは「セキュアトランジット」と呼ばれているが、「これは大きく2種類の機能から構成されています」と、NTTコミュニケーションズグローバル事業本部でグローバルIPネットワーク営業部 課長を務める西田氏は説明する。ひとつはDDoS攻撃検知機能であり、これは2005年11月1日に「DDoSファインダー」としてリリース。もうひとつはCisco Guardを活用したDDoS攻撃防御機能であり、これに関しても2006年3月までに「DDoSディフェンダー」として提供する計画になっているという。

セキュアトランジットサービスのDDoS攻撃防御機能のメカニズムを示したのが図1である。まずDDoSの攻撃を受けているか否かをデテクション機能によって判別。攻撃を受けていると判断された場合には、その情報を顧客収容ルータ群とCisco Guardに伝達し、攻撃対象（ターゲット）に向かうパケットをCisco Guardへリダイレクトする。Cisco Guardにリダイレクトされたパケットは複数のベリフィケーション（検査）プロセスによってチェックされる。そして正しいパケットだけがターゲットに送り込まれるのである。

CiscoGuardで5種類の検査を実施 パケットの絞り込みで効率的に処理

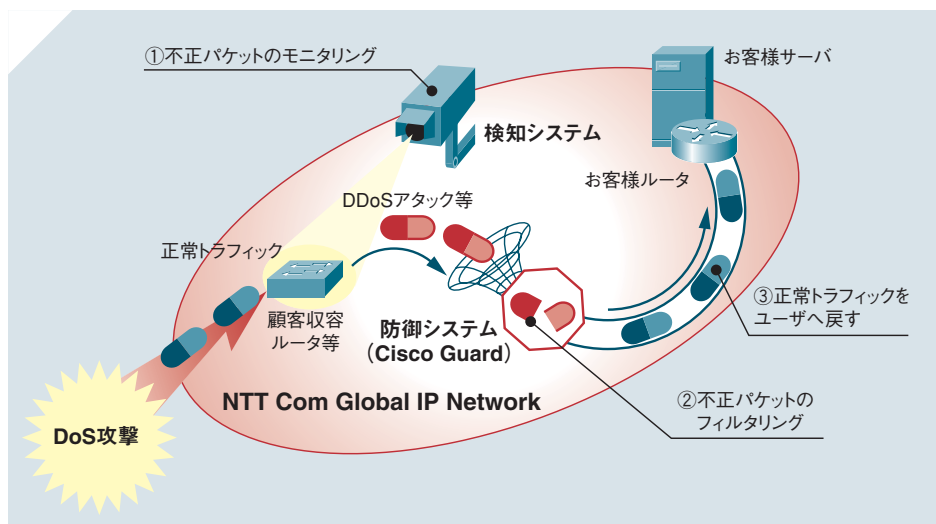
それではCisco Guardではどのようなチェックが行われるのか。大きく5つのベリフィケーションプロセスが用意されている。

まず第1のプロセスは“Static Packet Filtering”であり、事前に定義されたルールに一致したパケットをドロップする。第2が“Dynamic Packet Filtering”であり、ここではフローやプロトコル、ソースアドレス毎のフィルタリングを行う。第3のプロセスは“Anti-Spoofing Mechanism”であり、偽の送信元IPアドレスを持った（スプーフィングされた）パケットをドロップ。第4が“Statistical Inspection”であり、ここではフロー毎のアノマリートラフィック（異常にトラフィック量が大きくなるなどの通常とは異なった挙動）をチェックし、その内容を“Dynamic Packet Filtering”や、この後に来る“Rate-limiting”に伝達する。そして第5のプロセスが“Rate-limiting”であり、ここではターゲットに向かうトラフィック量の最終的なコントロールを行う。

「Cisco Guardによるベリフィケーションプロセスの最大の特徴は、全てのトラフィックをチェックするのではなく、ターゲットに向かうトラフィックだけを選別した上で、パケットを段階的に絞り込んでチェックできる点にあります」と水口氏。そのため大量のトラフィックが集中しても対応しやすいのだと説明する。また複数のCisco Guardをシスコスイッチに統合できる点も、Cisco Guardが持つメリットのひとつであると指摘。Cisco Guardには1Gbpsのインターフェースが装備されているが、これをスイッチ内に複数格納することで負荷分散が可能になり、スケーラビリティが確保しやすくなるという。

ネットワークに“インライン”で設置する必要がない点も、製品採用の重要なポイントになった。インラインで設置するというのは、トラフィックの経路上に機器を“直列”に接続すること。このような接続が要求される機器では、接続の際にルータ間の接続を切り離す必要があるため、サービスを継続したまま設置することは困難だ。また万一機器障害が発生した場合も、インラインの設置では対応が難しいのである。「効

図1 セキュアトランジットサービス概念図





「Cisco Guardなら効率よくガードできるのはもちろんのこと、
将来の新しい攻撃にも対応可能。
この条件を満たす機器は他に存在しません」

NTTコミュニケーションズ株式会社
グローバル事業本部
グローバルネットワーク部 主査
水口 孝則 氏

率的な処理とスケーラビリティ、インライン不要という条件を全て満たす製品は、Cisco Guard以外には存在しません」

さらに水口氏は「フィルタリングの機能も優れている」と指摘。DDoS攻撃ではICMPパケットやSYNパケットを大量に送りつける手法が一般的だが、この種のパケットに対してプロキシとしてレスポンスを返す等、処理内容を細かく設定できるのだという。これによって単独のパケットだけでは判別しきれない攻撃も、高い精度で判別できるようになる。このようなことが可能なのは、Cisco Guardがソフトウェアによって機能を実装しているからだ。このような機能を実現しているのはCisco Guardしかないという。また攻撃と判断したときにそのソースアドレスやポート番号をブラックリストに登録したり、逆に正常なパケットのやり取りを行ったソースアドレスやポート番号をホワイトリストに登録するといった機能も装備。「Cisco Guardなら将来の新しい攻撃にも対応しやすい。これもDDoS攻撃をガードする上で欠かせない条件です」

すでにDDoSファインダーの社内トライアルもスタート。DDoSディフェンダーで攻撃と判断されたパケットを、Cisco Guardによって間違いなくフィルタリングできることが確認されているという。

セキュリティ機能のサービス化は 今後の大きなトレンドに

「ネットワークを水道にたとえれば、これまでのDDoS攻撃への対応は各家庭にフィルターを装着して浄水するようなものでした」と森林氏。しかし水道では家庭に水を送る前に浄水を行っている。これと同じことをネットワークサービスプロバイダーが行うのは、必然的な流れだという。また西田氏も「セキュリティ機能をサービスとして提供することは、ユーザにとって運用管理稼働の削減面からも今後大きなトレンドになるはず」だと指摘。日々アップデートされるセキュリティ機器を適切に運用するには高度なノウハウが必要になるため、各ユーザーが導入しても検証に時間がかかったり、うまく使いこなせない危険性があるからだ。「セキュリティに関するアウトソースのニーズは間違いなく高いはずです」

インターネットに接続されている限り、どのサイトもDDoSの攻撃対象になる危険性を抱えている。そして攻撃を受けた場合の損害額も非常に大きい。これを適切な形で阻止することは、ネットワークを安心して使うための前提条件である。「シスコはそのためのコアになる技術を持っています」と森林氏。「これからもシスコと協力しあいながら、新しい攻撃に対応できる体制を作り上げていきたいと考えています」

Profile

NTTコミュニケーションズ株式会社

本 社：東京都千代田区内幸町1-1-6
営業開始日：1999年7月1日
資 本 金：2116億5000万円
(2005年3月31日現在)
従業員数：約7,700人
(2005年3月31日現在)

企業ユーザーや個人ユーザーに対してIP-VPNやOCN等のサービス提供する、日本を代表するネットワークサービスプロバイダー。また日米間で49Gbpsという世界最大規模の帯域のバックボーン(www.ntt.net/ja_JP/about/)を有する等、国際的なビジネス展開も積極的に展開している。2003年3月には「グローバルIPソリューションカンパニー」という事業ビジョンを発表。顧客にとって価値あるサービスを開拓することで、新たな市場を創造し続けている。
<http://www.ntt.com/>

©2006 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems, および Cisco ロゴは米国およびその他の国における Cisco Systems, Inc. の商標または登録商標です。

その他、記載されている会社名、製品名は各社の商標、登録商標または登録サービスマークです。

この資料の記載内容は2006年3月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社
URL: <http://www.cisco.com/jp/>
問合せURL: <http://www.cisco.com/jp/go/contactcenter>
〒107-0052 東京都港区赤坂2-14-27 国際新赤坂ビル東館
TEL: 03-6670-2992
電話でのお問合せは、以下の時間帯で受付けております。
平日 10:00~12:00 および 13:00~17:00

お問い合わせ先