

## ホスティングサービスへの導入事例 Rackspace Managed Hosting 社

### ユーザプロフィール

**企業名**

Rackspace Managed Hosting 社

**業種**

マネージド ホスティング サービス

**本社**

米国テキサス州サンアントニオ

**所在地**テキサス州サンアントニオ、  
バージニア州ハーンドン、ロンドン**導入規模**現在、Rackspace 社では、Cisco Guards  
をサンアントニオとハーンドンのデー  
タセンターに導入しており、ロンドンのデー  
タセンターへの導入も計画中である**背景**

Rackspace Managed Hosting 社（米国テキサス州サンアントニオ）は、顧客に対して「熱心なサポート」を提供することを第一としています。Rackspace 社では、顧客が悪質な Distributed Denial of Service (DDoS; 分散型サービス拒否) 攻撃の標的となっていることが判明し、シスコシステムズ製品を導入することで、被害を軽減して業務の継続性を回復することに成功しました。

**課題**

DDoS 攻撃が急激に増加し、Rackspace 社の顧客の Web サイトに被害が出始めたのは、2002 年初頭のことでした。

「これらの攻撃により、当社のファイアウォールの防御能力を超えるトラフィックが発生したため、お客様のサーバがダウンしてしまいました。」と Rackspace 社のネットワーク技術者である Jeff Nelson 氏は説明します。「そうなると、攻撃されているサーバの周囲にある他のデバイスに被害を出すわけにはいかないので、ネットワーク エッジで攻撃を受けたサーバに到達するためのルートを無効にして、攻撃がおさまるのを待つしかありませんでした。それには何時間かかるのか、何日かかるのか、予測もつきませんでした。」その間に、被害を受けた顧客はビジネスチャンスを逃したために数千ドルの損害を受けていました。

これは Rackspace 社にとって見過ごすことのできない出来事であり、早急に解決策を見つける必要がありました。「その頃、ちょうど登場した DDoS 攻撃をブロックする技術は、まったく目新しいものでした。」と Nelson 氏は言います。仕事の関係者から Riverhead Networks という会社（2004 年 3 月にシスコが買収）を勧められ、Nelson 氏はそのスタッフをサンアントニオに招きました。

「彼らのデモは非常にすばらしいものでした。」と Nelson 氏は思い返します。「彼らは、当社のお客様が受けていた各種の攻撃をブロックする機能を示しました。そこで我々は、トライアルを実施して現場環境でその機能を確認することに合意したのです。」

トライアルは、サンアントニオにある Rackspace 社のデータセンターの 1 つに Cisco Guard DDoS 軽減対策アプライアンスを設置して行われました。Cisco Guard はオフラインで設置され、攻撃フローをルート変更して分析とブロックを実行するようにしました。そのため Rackspace 社は、ネットワークを混乱させずに必要に応じてソリューションを展開し、テストすることができました。最初に被害を受けたサーバ以外の顧客にも攻撃の影響が出始めた時点で、Rackspace 社は、サーバへのルートを無効にしてオフラインにするか、攻撃されているサーバ宛でのトラフィックを Cisco Guard によりルート変更して攻撃を抑制するか、という選択肢を顧客に提示しました。「Cisco Guard を辞退したお客様はいませんでした。」と Nelson 氏は言います。「お客様にとってのリスクは何もないですからね。」

このデバイスの有効性はすぐに証明されました。最初に仕掛けられた攻撃は 10,000 pps（パケット / 秒）の単純な SYN Flood 攻撃で、ほんの数秒で撃退できました。「それは見事に機能しました。」と Nelson 氏は述べています。

しかし、さらに手ごわい攻撃が待ち構えていたため、Nelson 氏のチームは引き続き Cisco Guard を使用して設定の調整と新しいポリシーの定義を行い、Rackspace 社の顧客が受けていた複合型や変形型などのさまざまな大規模攻撃を撃退しました。トライアルは大成功でした。

## ソリューション

次の数カ月間に、Rackspace 社は Cisco Guard を使用して多数の DDoS 攻撃を撃退しました。攻撃の可能性が検出されると、トラフィックのルートを手動で Cisco Guard 経由に変更しました。そこでは特許を取得した Multiverification Process (MVP) アーキテクチャによって、不正の可能性のあるフローに対して最高レベルの分析が行われ、不正パケットを識別して除去しながら、適正なトランザクションについては通常どおりに伝送できます。

最終的に、攻撃が相当な強度で頻繁に仕掛けられたため、Rackspace 社はオンデマンドの DDoS 保護ソリューションでは長期的に持ちこたえられないと結論しました。「同じやり方を続けるのは不可能でした。」と Nelson 氏は振り返ります。「当社には、最大規模の企業顧客を保護できるような、スケーラブルで管理性の高いアプローチが必要でした。」

その結果、業界初の管理型付加価値 DDoS 保護サービスである PrevenTier™ が生まれました。2003 年 8 月に登場した PrevenTier は、攻撃の存在を検出する Rackspace 社が独自に開発したソリューションがベースになっています。攻撃が検出されると、攻撃対象となっているサーバへ向かうトラフィックのみがすべて Cisco Guard を経由するようにルート変更され、検査とブロックが行われます。他のトラフィックは中断されることなく伝送されるので、他の顧客への影響はありません。攻撃フローが除去されると、適正なトラフィックは Cisco Guard によってネットワークに戻されるため、ビジネスクリティカルなトランザクションが失われることはありません。

PrevenTier が提供する保護レベルは顧客から高い好評を得られたため、Rackspace 社は新しい顧客を競合他社から獲得することさえできました。この成功は、PrevenTier がすでに相当な収益を生み出しており、Rackspace 社が初期投資から収益をすみやかに回収していることを示しています。

PrevenTier に感銘を受けたのは顧客だけではなく、2003 年 11 月、PrevenTier のおかげで Rackspace 社は InfoWorld 100 リストに選出され、テクノロジーを最も有効に活用して事業を強化した企業として認められました。

## 結果

シスコのソリューションは、絶えず巧妙化している攻撃からユーザを保護します。Nelson 氏によると、Cisco Guard を使用すれば、攻撃の 95% は容易にブロックできます。残りの 5% は最も強力な最新の攻撃となるため、若干の調整が必要となりますが、それでも問題なく撃退できます。「ハッカーたちがこうした攻撃を仕掛けるためにそれなりの時間を費やしていることを理解する必要があります。」と Nelson 氏は言います。「攻撃は、防御システムを突破するように設計されています。それをブロックするために多少の調整が必要になるのは、ごく当たり前のことです。」

また Nelson 氏は、シスコのソリューションは課題を達成するのに十分な柔軟性を持っていると述べています。「テクノロジーが成熟し、攻撃がより高度になるにつれて、増大する脅威に対応するソリューションの発展する速度にいつも驚かされます。」と彼は言います。

現在の最大の脅威は、脆弱化されたホスト コンピュータである「ゾンビ」の大群による攻撃だと Nelson 氏は言います。この攻撃では、1 台の「マスター」からたった 1 つのコマンドを発行するだけで、世界中に存在する「ゾンビ」から無防備な標的にトラフィックの洪水を浴びせることができます。

「ゴミ パケットなら、スクリプト ベースの排除リストで簡単にフィルタリングできます。問題なのは、膨大な量の要求なのです。送信元 IP あたりの要求は 1 秒間に 1 つ程度ではありますが、それがあらゆる場所から押し寄せてきます。」と Nelson 氏は説明します。

こうした攻撃をブロックするには、最高レベルの分析および軽減機能を備えた柔軟性のあるソリューションが必要です。「当社は Cisco Guard がそのソリューションであると確信しました。Cisco Guard では、1 秒間に 100 万を超えるパケットをフィルタリングしながら、遅延は 1 ミリ秒も増加しません。」と Nelson 氏は述べています。「シスコ製品は、かつて見たどんな DDoS ソリューションよりも、はるかに優れています。」

©2004 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。  
この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。  
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

お問合せ先