ミッションクリティカルなサーバを DDOS 攻撃から保護する

DDoS 攻撃、SYN フラッド攻撃、ICMP 攻撃を受けても機能する E コマースサーバ

シスコシステムズ®では、様々なタイプのネットワーク攻撃に対処するため、複数のテクノロジーを利用しています。例えば、限られた範囲のソースアドレスからの攻撃に対処するために、ネットワークのエッジ部分にはアクセス コントロール リスト（ACL）を配置しています。この手法をブラックホーリングと呼んでいます。

ビジネス上の利点

- **事業継続性の保証を支援**
- **ミッションクリティカルなサーバを保護**
- **攻撃に自動対応**
- **攻撃中も適正トラフィックは通過**

「我々のセキュリティ戦略は、低帯域幅からの DoS 攻撃の脅威に対しては脆弱でした。攻撃はそうしばしば行われるわけではないものの、受けた場合のリスクは重大です。ですから、私たちには、特に業務価値の高いサーバを保護するソリューションが必要だったのです」—John Banner, Network Engineer, Cisco Systems

しかし、2003 年頃から、シスコは新たな脅威にさらされるようになりました。それは、広範な偽装アドレスからの低帯域幅サービス拒否（DoS）攻撃です。このタイプの攻撃では、大量のソースアドレスが使われるため、ACL は無力です。ACL では、悪意あるトラフィックと共に適正トラフィックをも遮断してしまいます。シスコ IT はこれらのトラフィックを区別し、悪意あるトラフィックだけを遮断するソリューションを求めてきました。

そこで、シスコ IT が投入したのが Cisco Guard です。これにより、シスコのミッションクリティカルなサーバへの攻撃を軽減することに成功しました。Cisco Guard はサービスプロバイダー拠点と、全世界のシスコ インターネット アクセスポイント (POP) 上に展開されました。シスコ IT では、差し迫った脅威が認められると、Cisco Guard を使うか他のテクノロジーを使うかを選択します。

Cisco Guard は悪意あるトラフィックを排除し、適正トラフィックを通過させます。洗練されたアルゴリズムにより、トラフィックを、通常時に学習させた正常なプロファイルと比較します。

シスコのネットワークでは、Cisco Guard の保護システムが作動中でもパフォーマンスが低下したことはありません。攻撃を受けている間も、クライアントはシスコのネットワークリソースを通常通り利用し続けることができます。

Cisco Guard をサービスプロバイダーネットワーク上に展開することで、アップストリーム帯域幅を保護します。悪意あるトラフィックはシスコのネットワークに到達する前に途中で検出され、排除されます。

Cisco Guard は業務価値の高いサーバ資産にさらなる保護を提供します。

その他、各ビジネスソリューションに対する Cisco IT の事例研究は、
Cisco IT @ Work をご覧ください

http://www.cisco.com/jp (シスコシステムズ→Cisco IT@ Work)

付記

この文書に記載されている事例は、シスコが自社製品の展開によって得たものであり、この結果には様々な要因が関連していると考えられるため、同様の結果を別の事例で得られることを保証するものではありません。

この文書は、明示、黙示に関わらず、商品性の保証や特定用途への適合性を含む、いかなる保証をも与えるものではありません。
司法権によっては、明示、黙示に関わらず上記免責を認めない場合があります。その場合、この免責事項は適用されないことがあります。

シスコシステムズ株式会社

〒107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館
http://www.cisco.com/jp

お問合せ先(シスココンタクトセンター)
http://www.cisco.com/jp/service/contactcenter
0120-933-122(通話料無料)、03-6670-2992(携帯電話、PHS)
電話受付時間:平日 10:00～12:00 、13:00～17:00